СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(16–30.06)

2014 № 12

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(16–30.06)
№ 12

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

Головний редактор
В. Горовий, д-р іст. наук, проф.

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Соціальна мережа Facebook не повинна перейматися рівнем своєї популярності серед підлітків. Про це свідчать результати нещодавнього дослідження, пише mashable.com.

У рамках дослідження Forrester опитали понад 4,5 тис. підлітків у Сполучених Штатах Америки стосовно їхніх уподобань у соціальних медіа. З'ясувалося, що популярність Facebook дуже велика.

«Понад три чверті молоді використовують Facebook – це вдвічі більше, ніж Pinterest, Tumblr чи Snapchat, а також більше, ніж Instagram та WhatApp разом узяті, – пише аналітик Forrester Нейт Еліот (Nate Elliott) у підсумковому повідомленні щодо результатів дослідження. – І 28 % юних користувачів Facebook сказали, що використовують його "увесь час". Серед усіх соцмереж це найбільший відсоток користувачів, які так висловилися».

Популярність Facebook зростає і серед наймолодшої категорії юних користувачів, 12–13-річних. Серед половини з них спостерігається більш активне користування цією соцережею. Forrester також передбачає, що висхідний тренд у придбанні підлітками смартфонів лише допомагатиме зростанню популярності Facebook у цій віковій групі.

Торік Facebook заявляв про зменшення кількості користувачів серед підліткової аудиторії. Це також демонстрували різні дослідження популярності соцмереж ***(Facebook має велику популярність серед підліткової аудиторії США – опитування // Громадська організація «Телекритика» (http://osvita.mediasapiens.ua/material/32010). – 2014. – 25.06).***

***

Некоторое время служба микроблогов Twitter проводила испытание применения автоматического переводчика. Впервые Bing Translator начал использоваться в приложении для Windows Phone и на сайте Twitter в режиме детализированного отображения сообщений.

Теперь эта функция становится доступна более широкому кругу пользователей. Компания встроила в приложение для iOS функцию автоматического перевода с помощью службы Microsoft.

Эту же возможность Twitter интегрировала в веб-клиент: рядом с сообщения на иностранных языках появилась кнопка в виде земного шара. Конечно, для эффективной работы необходимо правильное написание текста и отсутствие редких сокращений, не говоря уже о том, что сегодня машинный перевод далёк от совершенства.

Широкое внедрение новой функциональности предоставит пользователям больше возможностей для общения и подписок на иностранные каналы, например, посвящённые чемпионату мира по футболу

FIFA 2014 ***(Twitter расширяет использование Bing-переводчика // InternetUA (http://internetua.com/Twitter-rasshiryaet-ispolzovanie-Bing-perevodcsika). – 2014. – 16.06).***

***

Спустя неделю после непреднамеренного запуска компания Facebook официально анонсировала приложение для обмена фотографиями и видео Slingshot. Об этом сообщила пресс-служба компании.

10 июня Facebook преждевременно выпустил Slingshot в App Store: приложение успело появиться сразу в нескольких странах, однако через короткий промежуток времени исчезло из магазинов. На этот раз релиз состоялся официально.

С помощью Slingshot – как с помощью практически любого современного мессенджера, в том числе Facebook – можно отправлять друзьям фотографии и видеоролики. Однако Slingshot играет на любопытстве пользователей: присланный другом снимок или ролик нельзя посмотреть до тех пор, пока не отправишь ему что-нибудь в ответ.

В отличие от многих других приложений, использующих камеру, Slingshot сразу использует фронтальную, а не заднюю: этот режим в приложении называется Selfie. Зажав кнопку, можно снять короткое видео.

На картинку или ролик можно нанести надпись: текстом или при помощи инструмента кисти. Толщину и цвет кисти можно выбрать при помощи интуитивно понятного слайдера, а в процессе рисования играет приятная музыка.

Slingshot продолжил традицию современных мессенджеров не требовать никаких дополнительных данных для регистрации, кроме номера телефона. По желанию в приложении можно просканировать записную книжку в поиске друзей или добавить их из Facebook.

Авторитетный в Кремниевой долине венчурный инвестор Э. Д. Сиглер уже предрёк приложению скорое забвение.

Мессенджер позаимствовал свои функции сразу у нескольких приложений: 15-секундная длина роликов взята из Instagram, зацикленность видео – фирменная карточка Vine, а эфемерность и общая концепция общения – у Snapchat или Taptalk. Под эфемерностью подразумевается то, что изображения и видео посылаются не с целью их дальнейшего сохранения: после просмотра они больше не доступны.

Приложение бесплатно доступно в App Store и Google Play, однако, по всей видимости, Россия пока не входит в число стран, где уже можно воспользоваться Slingshot. Тем не менее, пользователи с американским аккаунтом могут скачать Slingshot из App Store ***(Facebook официально выпустил эфемерный мессенджер Slingshot // IT Expert (http://itexpert.org.ua/rubrikator/item/36425-facebook-ofitsialno-vypustil-efemernyj-messendzher-slingshot.html). – 2014. – 18.06).***

***

Facebook сделала приложение Slingshot доступным для пользователей всего мира. В настоящее время сервис доступен для всех остальных стран. Для того чтобы оценить возможности потенциального конкурента Snapchat, потребуется немногое. Нужно лишь иметь устройство на базе iOS или Android и круг друзей, кому взаимообмен исчезающих сообщений (фото, видео) будет интересен.

Slingshot не позволит пользователю участвовать в обмене материалами до того момента, пока он сам чем-нибудь не поделится с друзьями. Данное приложение распространяется отдельно – никакой привязки к Facebook делать не нужно. То есть для начала провокационной конференции потребуется лишь сам смартфон и привязанный к нему номер мобильного телефона ***(Facebook сделала приложение Slingshot доступным для пользователей всего мира // InternetUA (http://internetua.com/Facebook-sdelala-prilojenie-Slingshot-dostupnim-dlya-polzovatelei-vsego-mira). – 2014. – 28.06).***

***

Крупнейшая мировая социальная сеть Facebook 19 июня презентовала открытую модель программного сетевого коммутатора, способного управлять серверами в масштабах датацентра. Новая концепция потенциально может угрожать бизнесу таких гигантов, как Cisco Systems или Juniper Networks, так как затраты на поддержку софтверного роутера значительно ниже, чем на содержание аппаратного парка.

Как рассказали в Facebook, их роутер может управлять потоками трафика, причем он изначально оптимизирован для работы с крупными интернет-проектами, которым нужна система веб-балансировки нагрузки, изощренная маршрутизация и другие особенности. В Facebook говорят, что столкнулись с необходимостью создания собственного программного маршрутизатора, после того как компания возросла до тех масштабов, что работать с обычными коммутаторами стало уже неудобно.

Коммутаторы открытого дизайна – это последний шаг крупнейшей социальной сети по созданию инфраструктурных сетевых решений. С 2011 г. Facebook совместно с партнерами работает над разработкой более эффективных и экономичных решений. Соцсеть обменивается инициативами в рамках ранее созданного проекта Open Compute Project. Данный проект имеет своей целью обмен технологиями и идеями относительно программно-аппаратных компонентов датацентров и высокоскоротных сетей. Здесь партнеры занимаются созданием серверов, систем хранения и сетевых продуктов кастомизированного дизайна.

Ранее Facebook заявляла, что за счет разработок, созданных в недрах Open Compute Project ей удалось сэкономить 1,2 млрд дол. на инфраструктуре. В прошлом году Facebook инвестировала 1,36 млрд дол. в создание собственных серверов. За 2013 г. объем инвестиций возрос вдвое. В

Facebook покупают серверы по кастомизированным проектам у таких компаний, как Quanta Computer, вместо того, чтобы покупать оборудование у мировых брендов, таких как HP, IBM или Dell ***(Facebook анонсировала программный коммутатор // InternetUA (http://internetua.com/Facebook-anonsirovala-programmnii-kommutator). – 2014. – 19.06).***

***

Сайт twitter.com, а также официальные приложения Twitter для Android и iOS теперь поддерживают формат анимированных картинок GIF. Вообще-то анимацию можно было публиковать в Twitter и раньше, но для этого требовалась сокращалка URL-адресов Giphy.

В API сервиса также добавлена поддержка GIF, поэтому стоит ожидать, что сторонние приложения в скором времени тоже смогут загружать и показывать анимацию. В официальных приложениях Twitter для Mac и Windows Phone, а также в веб-версии TweetDeck поддержки GIF пока нет ***(В приложениях Twitter появилась поддержка картинок в формате GIF // InternetUA (http://internetua.com/v-prilojeniyah-Twitter-poyavilas-podderjka-kartinok-v-formate-GIF). – 2014. – 19.06).***

***

The Washington Post, The New York Times і Mozilla об’єднаються, щоб розробити нову систему комунікації на веб-сайтах. З її допомогою читачам буде легше писати коментарі, додавати фотографії, а також спілкуватися (як читачам із журналістами, так і медійникам між собою). Про це повідомляє The Washington Post.

Кошти на дворічну роботу над проектом виділить Knight Foundation, благодійна організація, що спеціалізується на медіа та мистецтві і базується у Маямі. Конкретно йдеться про суму в 3,89 млн дол.

Як описують проект розробники, система об’єднає і стандартизує різні технології «залучення суспільства», що нині використовуються веб-сайтами.

Найбільш амбітною метою проекту є створення такого набору функцій, який би виділяв найбільш релевантні до контенту коментарі читачів. Планується також, що коментатори категоризуватимуться відповідно до попередніх дописів.

На думку директора цифрових проектів The Washington Post Г. Барбера, ці функції не зможуть усунути «тролів», але допоможуть їх трохи «притишити» і виховати спільноту коментаторів. Він також зазначив, що нові можливості дозволять журналістам більш ефективно працювати з аудиторією.

The Washington Post та The New York Times заявляють, що не обмежуватимуть використання майбутньої системи своїми сайтами і готові поділитися нею з іншими виданнями та блог-платформами ***(The Washington Post, The New York Times і Mozilla спільно розроблять нову систему для***

коментування сайтів // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/31872). – 2014. – 21.06).

***

Программист А. Стегно и дизайнер И. Дмитрук запустили социальную сеть полезных контактов Cardsaround. Сервис поможет интернет-пользователям в поиске партнеров по бизнесу и специалистов в определенной области. А. Стегно уверен, что ни одна существующая соцсеть не решает эту проблему напрямую и в ближайшее время планирует выход на международный рынок, пишет AIN.UA (http://ain.ua/2014/06/23/529634).

Главный принцип новой соцсети заключается в том, что пользователь создает визитную карточку с указанием, как и по каким вопросам к нему можно обращаться, а другие находит его именно по этим ключевым словам. Например, чтобы найти партнера для тенниса нужно в поиске набрать #теннис и в результатах поиска сразу появятся профили людей, которые увлекаются этим видом спорта. Основной функционал сети бесплатен, но в дальнейшем там появятся платные функции: например, закрепление профиля в топе, поиск по городам и привязка аккаунта к собственному домену.

А. Стегно рассказал AIN.UA, что ради работы над новым проектом они с И. Дмитруком уволились с предыдущей работы в IT-компании DAXX и последние несколько месяцев занимаются исключительно развитием Cardsaround.

В новой сети будут действовать строгие правила, которые исключат общение не по делу. «Обращаться к пользователю можно только по указанной теме, – говорит А. Стегно. – К примеру если я написал – обращаться по поводу #футбола, а мне написали по поводу работы – я нажимаю REPORT SPAM и пользователь на другой стороне получает уведомление о нарушении правил».

Создатель соцсети считает, что Cardsaround – это не очередная социальная сеть, а проект который решает проблему поиска людей и быстрого поиска по хештегам. При этом, шаблон соцсети используется потому, что он наиболее удобен для данного сервиса.

Это не первый проект киевского программиста. Несколькими месяцами ранее он запустил социальный рейтинг кандидатов в президенты ***(Киевляне запустили социальную сеть полезных контактов Cardsaround // AIN.UA (http://ain.ua/2014/06/23/529634). – 2014. – 23.06).***

***

В Twitter тестируют новые варианты комментариев

Тестовая выборка пользователей Twitter сегодня обнаружила в своих микроблогах новую возможность: они могут выбрать не только простой ретвит чужой записи, но и ее ретвит с комментарием. Во втором случае запись отображается в виде ссылки, оставляя, тем самым, больше свободных символов для комментария к ней.

При этом в результате другие пользователи видят цитируемый твит не как ссылку, но как карточку – подобно приложенной фотографии или видеозаписи.

Такое решение вполне очевидно: в настоящее время при ретвите оригинальная запись ставится в кавычки, и количество символов на комментарий к ней напрямую зависит от ее длины – все это суммарно также не может превышать стандартные 140 знаков.

Некоторые пользователи также обнаружили, что прикрепленная к посту фотография отображается у них не под записью, как было раньше, а над ней ***(В Twitter тестируют новые варианты комментариев // InternetUA (http://internetua.com/v-Twitter-testiruuat-novie-varianti-kommentariev). – 2014. – 24.06).***

***

Facebook занята разработкой отдельной версии социальной сети для сотрудников компаний. Об этом анонимный источник рассказал блогу TechCrunch. По его словам, «офисный» Facebook будет доступен на всех популярных платформах: iOS, Android, на компьютерах и в браузерах. Проект называется FB@Work – «Facebook на работе», а занятые в нем сотрудники базируются в Лондоне.

Неясно, является ли FB@Work внутренней коммуникационной платформой или открытой, и позволит ли она служащим сосредоточиться на делах, вместо того чтобы растрачивать попусту рабочее время на переписку с друзьями, просмотр видео и обмен смешными картинками. По этой причине, кстати, некоторые работодатели блокируют в офисе доступ к развлекательным ресурсам и соцсетям, включая YouTube, Twitter, «ВКонтакте», «Одноклассники» и тот же Facebook.

Проект FB@Work наверняка курирует Л. Расмуссен (бывший инженер-программист Google), так как именно он возглавляет подразделение Facebook в Лондоне. Л. Расмуссен является техническим директором проекта Graph Search («Социальный поиск»), а до прихода в компанию М. Цукерберга он создал сервис Google Wave для совместной работы.

В то же время, сказали TechCrunch два других источника, в Facebook уже 3–4 года создаются различные версии соцсети, однако их запуск откладывается в последний момент. Помимо версии для предприятий, планировался релиз «детской» версии – для пользователей младше 13 лет. «Их обеих начинали около трех раз, и столько же раз они откладывались», – признался осведомитель ***(Facebook создает «офисную» версию соцсети // InternetUA (http://internetua.com/Facebook-sozdaet--ofisnuua--versiua-socseti). – 2014. – 26.06).***

***

Российская социальная сеть «ВКонтакте» заключила соглашение о партнерстве с американской корпорацией Microsoft, в соответствии с которым приложение «ВКонтакте» будет интегрировано в мобильную операционную систему Windows Phone 8.1., говорится в совместном пресс-релизе компаний.

Интеграция мобильного приложения «ВКонтакте» в платформу Windows Phone подразумевает синхронизацию данных из социальной сети со списком контактов в устройствах на платформе от Microsoft. В частности, пользователи получат возможность следить за социальной активностью друзей напрямую из записной книжки, а также получать интерактивные обновления от избранных контактов, диалогов на стартовый экран.

Первым устройством с синхронизацией «ВКонтакте» и операционной системы от Microsoft станет смартфон Lumia 930, начало продаж которого в России запланировано на июль 2014 г. Обновленное приложение, поддерживающее интеграцию с Windows Phone 8, также будет доступно через магазин Windows Phone Store ***(«ВКонтакте» договорилась с Microsoft об интеграции в ОС Windows Phone // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/06/26/v-kontakte.html). – 2014. – 26.06).***

***

Адміністратор одного з пабліків «ВКонтакте», який ховається за псевдонімом М. Фрай, випустив додаток для Google Chrome, який дає змогу анонімно коментувати записи в соціальній мережі «ВКонтакте».

Як повідомляється в спільноті «Подслушано в Киеве», додаток працює поки лише для їх пабліка і лише з Google Chrome та Opera, але незабаром планується підключити й інші браузери. Після встановлення додатку у користувача зявиться кнопка «Анонимно», за допомогою якої він зможе прокоментувати будь-який запис не від свого імені. Для зручності діалогу, для кожного аноніма буде закріплено власну картинку з тваринкою.

М. Фрай розповів AIN.UA, що ніхто не зможе дізнатися автора оригінального коментаря: інформація на сервер у Німеччині передається за допомогою унікального згенерованого ключа, а сам додаток не порушує правил «ВКонтакте», використовуючи відкрите API.

За словами автора, ідея зробити такий додаток виникла після популярності сервісу Secret.ly, який дозволяє постити анонімні «секрети» ***(Київський розробник створив додаток для анонімного коментування у ВКонтакті // InternetUA (http://internetua.com/ki-vskii-rozrobnik-stvoriv-dodatok-dlya-anon-mnogo-komentuvannya-u-vkontakt). – 2014. – 28.06).***

***

Соцсеть «ВКонтакте» запустит мобильную игровую платформу в приложении для Android на следующей неделе. Об этом «Ленте.ру» сообщил глава пресс-службы «ВКонтакте» Г. Лобушкин.

Подобная платформа для устройств Apple уже готова к запуску и будет добавлена в iOS-приложение соцсети после возвращения в Apple AppStore, откуда оно было удалено весной.

Платформа будет представлять собой отдельную страницу, включенную в мобильное приложение соцсети. Через нее будет осуществляться продвижение игр сторонних разработчиков.

«Мобильная игровая платформа – доступ пользователей “ВКонтакте” к лучшим мобильным играм. В специальном разделе мобильных клиентов будут размещаться ссылки на игры, доступных для установки на устройства с iOS и Android», – пояснил Г. Лобушкин.

В первое время мобильная игровая платформа будет включать в себя четыре игры, затем список будет расширяться на одну-две игры в месяц. Доход от игр будет делиться пополам между соцсетью и разработчиками.

Выплаты разработчикам игр для десктопной версии «ВКонтакте» в 2013 г. составили около 2 млрд р. Весь оборот десктопной игровой платформы превысил 4 млрд р. По информации компании, игроками являются примерно треть из 250 млн пользователей «ВКонтакте» ***(«ВКонтакте» запустит мобильную игровую платформу для Android // InternetUA (http://internetua.com/vkontakte--zapustit-mobilnuua-igrovuua-platformu-dlya-Android). – 2014. – 28.06).***

***

Представители социальной сети Facebook официально объявили об изменении алгоритма ранжирования видеороликов, публикуемых на сайте как частными пользователями, так и с аккаунтов публичных страниц.

Теперь алгоритм новостной ленты будет осуществлять ранжирование публикаций видеоконтента, основываясь не только на количестве его просмотров пользователями, но и на степени длительности просмотра. Кроме того, пользователям, активно просматривающим видео, в лентах новостей будет показываться больше подобных публикаций, чем тем, кто не является любителем данного формата.

«Люди, вовлечённые в просмотр видео, будут видеть в своих лентах больше таких публикаций. И наоборот, пользователи, предпочитающие пролистывать такие сообщения в лентах, не запуская ролики, будут видеть меньше публикаций, содержащих видео», – поясняют разработчики.

Главная цель нововведения – добиться максимальной вовлечённости каждого конкретного пользователя во взаимодействие с контентом новостной ленты Facebook .

«Главная цель новостной ленты предоставлять правильным пользователям правильный контент в правильное время – так, чтобы люди не

пропускали важные и соответствующие их интересам публикации. Видеоконтент всегда являлся важной составляющей новостной ленты Facebook: не случайно, за последние 6 месяцев количество пользователей, просматривающих видео в социальной сети, возросло в 2 раза. …Наша задача сводится к тому, чтобы лучше понимать, какое содержание больше всего интересует пользователей, с тем, чтобы в лентах появлялись самые релевантные ролики», – комментируют представители социальной сети.

На протяжении всего последнего года социальная сеть активно работает над алгоритмом ранжирования публикаций в новостной ленте. Так, результате январского обновления администраторы страниц могли заметить снижение частоты показов апдейтов страниц, однако увеличение показов постов других типов и взаимодействий с ними со стороны аудитории.

Позднее команда Facebook заявила о намерении сократить количество постов, которые автоматически публикуются сторонними приложениями в лентах пользователей. Именно такие публикации чаще всего помечаются как спам ***(Facebook меняет алгоритм ранжирования видео в новостных лентах пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_menyaet_algoritm_ranzhirovaniya_video_v_novostnyh_lentah_polzovateley). – 2014. – 27.06).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Столичный программист Е. Докукин практически в одиночку развернул борьбу с сепаратистами на киберфронте. Он заблокировал электронные счета многих приверженцев ДНР и ЛНР, включая кошельки Webmoney и «Яндекс.Деньги», принадлежащие лидеру луганских сепаратистов В. Болотову. Об этом сам хакер сообщил на своей странице в Facebook. Блокировка кошельков – лишь одно из направлений деятельности «Украинских Кибервойск», созданных Е. Докукиным.

О создании «Украинских Кибервойск» Е. Докукин официально объявил 12 июня. Это батальон для проведения оборонительных и наступательных операций в Интернете, противодействия сепаратистам, террористам, а также информационной войне против Украины. Е. Докукин объявил свободный набор в свой кибербатальон – чтобы вступить в него, нужно написать хакеру на электронную почту или в Facebook.

С батальоном «Кибервойск» Е. Докукин планирует расширить масштаб своих операций. Помимо блокировки электронных кошельков, он проводит операции «Кибершторм» и «Кибераураган», направленные на блокировку мобильных телефонов террористов ДНР и ЛНР.

Также Е. Докукину нужны добровольцы, которые помогут ему в информационной войне в Wikipedia. В популярной онлайн-энциклопедии активист борется с российской пропагандой, распространяющей пропагандистские статьи. Сам Е. Докукин уже неоднократно участвовал в войне правок, а также создавал в украиноязычной версии энциклопедии свои статьи на тему тех же событий.

Взломами и DDoS-атаками на сайты сепаратистов Е. Докукин начал заниматься еще в марте. В частности, ему удалось временно заблокировать официальный сайт ДНР donetsk-gov.su (правда, в настоящее время доступ к сайту временно открыт) ***(Украинский программист заблокировал электронные счета Болотова // InternetUA (http://internetua.com/ukrainskii-programmist-zablokiroval-elektronnie-scseta-bolotova). – 2014. – 17.06).***

***

Губернатор Запорожской области В. Баранов появился в социальной сети Twitter.

Постов у Запорожского губернатора пока немного. Так, он сообщил о количестве беженцев из зон, где проводится АТО:

«На сегодняшнем аппаратном совещании Петр Гончарук сообщил о количестве поселенных в Запорожской области беженцев – уже 1203 человека» ***(Запорожский губернатор теперь "твиттит" // IPnews (http://www.ipnews.in.ua/index.php/2014/06/17/запорожский-губернатор-теперь-пости/). – 2014. – 18.06).***

***

Міністерство оборони України знову звернулося до українців із закликом не поширювати інформацію про пересування військовослужбовців та техніки, не фотографувати і тим паче не викладати фото в соціальні мережі, оскільки це грає на руку ворогам.

«Світлинами в Інтернеті "грішать" і самі військові, але їм слід пам'ятати що вони і так вже герої, краще повернутися додому живими і переглядати альбоми з сім'єю, аніж давати терористам підказки про те, де їх шукати», – ідеться в повідомленні оборонного відомства у Facebook.

«Допоможімо зберегти українських військовослужбовців, які щодня ризикують власним життям за те, аби ми могли спати спокійно», – закликають у Міноборони, наголошуючи, що «будь-яка інформація про їх перебування може стати саме тією кулею, яка забере життя достойного сина України».

«Про це ж вас просять самі військові, які зараз знаходяться безпосередньо у місці проведення АТО», – ідеться в повідомленні міністерства ***(Українців просять не викладати інформацію про пересування військових в мережі // InternetUA (http://internetua.com/ukra-***

nc-v-prosyat-ne-vikladati--nformac-ua-pro-peresuvannya-v-iskovih-v-merej). – 2014. – 18.06).

***

Общественные активисты поставили перед начальником УМВДУ во Львовской области Д. Загарией требование, чтобы все руководители райотделов милиции Львова зарегистрировались в соцсети. Об этом говорилось 19 июня, во время заседания наблюдательного совета в Главном управлении милиции Львовщины, передает ZAXID.NET.

Как отмечают активисты, это нужно для того, чтобы правоохранители могли оперативно получать информацию и реагировать на нее. Кроме того, это позволит каждому гражданину иметь обратную связь с милицией. Таким образом, считают они, милиция станет ближе к народу.

Как выяснилось в ходе заседания, Д. Загария уже имеет аккаунт в Facebook, но не ведет его активно. Он пообещал, что руководители всех райотделов Львова зарегистрируются и будут хотя бы раз в два дня пересматривать сообщения. Общественные активисты лично пообщаются с руководителями шести райотделов милиции Львова и при необходимости помогут им создать страницу Facebook ***(Львовских милиционеров обяжут общаться с народом через Facebook // proIT (http://proit.com.ua/news/gosregulation/2014/06/20/134823.html). – 2014. – 20.06).***

***

Усі начальники райвідділів міліції Львова від сьогодні, 25 червня, зареєстровані в соціальній мережі Facebook. Про це інформує ВЗГ ГУМВС України у Львівській області.

Посилання на сторінки:

https://www.facebook.com/profile.php?id=100004946388848 – полковник міліції Р. Гранківський, в. о. начальника Франківського райвідділу міліції;

https://www.facebook.com/profile.php?id=100007513811079&fref=ts – полковник міліції Є. Березін, начальник Шевченківського райвідділу міліції;

https://www.facebook.com/profile.php?id=100005519836778&fref=ts – полковник міліції І. Іваночко начальник Галицького райвідділу міліції;

https://www.facebook.com/profile.php?id=100005510779541&fref=ts – полковник міліції М. Криштанович, в.о. начальника Сихівського райвідділу міліції;

https://www.facebook.com/profile.php?id=100006444550832&fref=tl_fr_box– підполковник міліції А. Таран, начальник Личаківського райвідділу міліції;

https://www.facebook.com/profile.php?id=100006247875675 – підполковник міліції Я. Грицик, начальник Залізничного райвідділу міліції ***(У Львові начальники райвідділів міліції зареєструвалися у Facebook // Інформаційна агенція «Вголос»***

(http://vgolos.com.ua/news/u_lvovi_nachalnyky_rayviddiliv_militsii_zareiestruvalysya_u_facebook_149381.html). – 2014. – 25.06).

***

В соцсети «ВКонтакте» создана группа «Горловка за независимую Украину» с фотографиями всех, кто воюет за террористическую организацию ДНР и кто за нее агитирует в соцсетях, пишет «Главком» (http://glavcom.ua/news/215394.html

Всего за неделю своего существования группа стала костью в горле тех, кто активно агитирует или принимает участие в боевых действиях на стороне «ДНР».

«Надо ведь людям показывать, что есть те, кто родину не меняют и не продают. Мы ведем мирную работу по возвращению людям здоровых понятий. В других социальных сетях пока не планируем развиваться. Предпочитаем сохранять анонимность своих читателей и подписчиков», – рассказал Gorlovka.ua основатель группы А. Тохтамиш.

При этом подписи к фотографиям, на которых изображены молодые парни и девушки из Горловки, состоящие в Народном ополчении Донбасса, зачастую несут личную информацию. Это свидетельствует о том, что место работы и жительства многих из них известны ***(Горловчане партизанят: в соцсети создана группа с данными тех, кто воюет за террористов // «Главком» (http://glavcom.ua/news/215394.html). – 2014. – 25.06).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Facebook расширяет спектр пользовательских данных, предоставляемых рекламодателям. Теперь компания будет передавать им данные о посещаемых пользователями страницах, сообщает The Wall Street Journal. Данные о посещенных страницах помогут рекламодателям точнее выбирать целевую аудиторию, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-nameren-raskryt-reklamodateljam-dannye-o-poseschaemyh-polzovateljami-stranicah-40028/).

Раньше реклама в Facebook размещалась на основании интересов пользователя, которые определялись через лайки, оставленные пользователем на различных страницах Facebook, и заполненную им анкету о собственных интересах. Кроме того, Facebook разрешала размещение рекламы на основе информации, полученной социальной сетью от сторонних компаний, таких как DataLogix и Acxiom.

Теперь рекламодатели получат куда более точное представление об интересах пользователей, пояснил глава рекламного отдела Facebook Б. Боланд. Следовательно, возрастет и количество специально подобранной рекламы, которую пользователи будут видеть на своей странице. Так,

пользователь, регулярно посещающий сайты о комиксах, но не отметивший комиксы среди своих интересов в анкете Facebook, вскоре может увидеть на своей странице рекламу, так или иначе связанную с комиксами.

Facebook получает данные о веб-истории пользователя и посещаемых им сайтах с помощью специального кода, который сайт размещает на компьютере пользователя. Также Facebook получает информацию о загружаемых пользователем мобильных приложений. Ранее компания заявляла, что собирает эту информацию исключительно в целях безопасности.

Как сообщил официальный представитель Facebook, решение о предоставлении пользовательских данных было согласовано как с Федеральной торговой комиссией США, так и с руководителем ирландского комитета по защите информации (в Ирландии находится европейская штаб-квартира Facebook) ***(Facebook намерен раскрыть рекламодателям данные о посещаемых пользователями страницах // Marketing Media Review (http://mmr.ua/news/id/facebook-nameren-raskryt-reklamodateljam-dannye-o-poseschaemyh-polzovateljami-stranicah-40028/). – 2014. – 16.06).***

***

Вовлеченность поста на Facebook-страницах брендов упала в среднем на 50,4 %. Такие данные обнародованы в отчете аналитической компании Simply Measured, пишет Marketing Media Review (http://mmr.ua/news/id/vovlechennost-posta-na-facebook-stranicah-brendov-upala-na-504-40048/).

Аналитики проанализировали вовлеченность подписчиков 10 крупнейших компаний на Facebook после изменений алгоритмов сортировки в соцсети. Общее число подписчиков страниц брендов, которые попали в отчет, составляет около 358 млн человек.

Невзирая на рост числа публикаций, на страницах на 20,1 %, вовлеченность подписчиков 10 крупнейших компаний в Facebook снизилась на 40 % за последний год.

Для маркетологов постоянное снижение вовлеченности – куда страшнее, чем падение органического охвата само по себе. Число постов на страницах постоянно увеличивается, однако это не приводит к серьезным результатам.

За последний год – с мая 2013 г. по май 2014 г. – лишь две компании (MTV и Harley Davidson) из десяти смогли добиться увеличения показателей вовлеченности (соответственно на 56,31 % и 17,74 %), результаты остальных восьми брендов значительно ухудшились. В частности, если лидер Disney просел на 21,43 %, то Audi USA потеряла 94,77 %.

Учитывая увеличение числа постов, аналитики Simply Measured подсчитали средний показатель вовлеченности публикации брендов. Авторы отчета считают, что падение вовлеченности поста на Facebook-страницах

брендов 50,4 % вынуждают крупные компании уделять больше внимания качеству контента, а также тратить больше денег на рекламу.

Можно предположить, что таким образом соцсеть заставляет компании подходить к стратегии продвижения более серьезно – в том числе и за счет выделения бюджета на рекламу. Пользователи даже подозревают Facebook в намеренном снижении охвата публикаций, чтобы вынудить их покупать рекламу в социальной сети.

Рекламные доходы Facebook за последние три месяца 2013 г. возросли на 76 % в исчислении квартал к кварталу и составили 2,34 млрд дол. С учетом прочих поступлений в октябре – декабре Facebook получил 2,59 млрд дол. против 1,59 млрд дол. в IV квартале 2012 г. Годовая выручка компании достигла в 2013 г. 7,87 млрд дол. против 5,09 млрд дол. в 2012 г.

По прогнозам экспертов, для Facebook этот год ознаменуется развитием рекламных возможностей: компания работает над алгоритмами, которые будут собирать пользовательскую информацию и анализировать ее с тем, чтобы точнее таргетировать рекламу. К тому же, сеть хочет внедрить алгоритм, который позволит определять доход среднего пользователя. Уже в этом году в сети появится блок, которые будет сообщать пользователям о последних новостях и мировых трендах.

Мы сообщали, что с 6 июня социальная сеть Facebook автоматически перевела на новый дизайн все страницы брендов. Facebook откроет доступ к информации о потребпредпочтениях пользователей, а новые объявления Facebook будут больше похожи на рекламу в основной ленте.

В ноябре прошлого года социальная сеть запустила возможность проставлять оценки брендам по пятибалльной системе при помощи «звёздочек» (ранее контент можно было оценивать только при помощи кнопки Like). Так что у интернет-магазинов появилась ещё одна подсказка, товарами каких брендов лучше наполнять свои виртуальные полки ***(Вовлеченность поста на Facebook-страницах брендов упала на 50,4 % // Marketing Media Review (http://mmr.ua/news/id/vovlechennost-posta-na-facebook-stranicah-brendov-upala-na-504-40048/). – 2014. – 17.06).***

***

Получасовой сбой на Facebook, во время которого пользователи по всему миру не могли получить доступ к сервису, стоил компании более 500 тыс. дол. Такую оценку приводит аналитик журнала Forbes.

Если учесть, что за I квартал 2014 г. выручка Facebook составила 2,5 млрд дол., то в среднем в час компания зарабатывала за этот период 1,16 млн дол. Следовательно, получасовой простой обошелся соцсети более чем в полумиллиона долларов. Однако это небольшая сумма с учетом, к примеру, того, что Facebook за прошлый год потратила около 20 млрд дол. только на приобретение других компаний.

Facebook была недоступна в четверг с 11 часов. При попытке зайти на странице соцсети сообщалось, что «что-то пошло не так». Исходя из

сообщений пользователей в Twitter, сбой был глобальным. Ежемесячно активная аудитория Facebook составляет около 1,3 млрд человек, а каждый день в соцсеть заходят около 800 млн пользователей.

«У нас произошел технический сбой, из-за чего люди не могли обновить свои страницы на Facebook в течение непродолжительного времени. Мы быстро исправили этот сбой и полностью восстановили работу. Мы приносим извинения за причиненные неудобства», – сказали «Ленте.ру» в пресс-службе Facebook.

Серьезный сбой в работе соцсети был зафиксирован также в октябре 2013 г. Тогда при попытке зайти в соцсеть отображалось сообщение о закрытии сайта на временные технические работы. Сбой был устранен примерно через три часа. В декабре 2012 г. сайт соцсети не работал около 45 мин. во многих странах мира ***(Получасовой сбой обошелся Facebook в полмиллиона долларов // InternetUA (http://internetua.com/polucsasovoi-sboi-oboshelsya-Facebook-v-polmilliona-dollarov). – 2014. – 20.06).***

***

Twitter приобрел платформу SnappyTV, с помощью которой можно создавать короткие превью-видеоролики, а затем выкладывать их в социальные сети, сообщается в блоге сервиса микроблогов. Об этом пишет sostav.ru

Платформа SnappyTV будет интегрирована с Twitter, однако продолжит существование как отдельный продукт. Команда стартапа станет частью команды сервиса микроблогов.

Компания SnappyTV была запущена в 2010 г., партнерами платформы являются такие телевизионные компании как HBO, NBA, CBS, FOX Sports и т. д.

Приобретение SnappyTV доказывает то, что Twitter прилагает все усилия, чтобы сервис микроблогов стал более удобным для создателей видеоконтента. В мае прошлого года, компания запустила рекламный сервис – Twitter Amplify. Смысл его заключается в том, что телекомпании зарабатывают на видеорекламе, которая запускается перед показом роликов, которые размещены в их Twitter ***(Twitter купил стартап SnappyTV // Media бізнес (http://www.mediabusiness.com.ua/content/view/39764/126/lang,ru/). – 2014. – 20.06).***

***

Запуск кампаний платного продвижения бренда на Facebook усиливает эффект от поисковой рекламы, повышая конверсию почти на 20 %. Такими данными делятся аналитики агентства Kenshoo, сообщает searchengines.ru

В ходе практического эксперимента представители Kenshoo измеряли эффективность продвижения бренда Experian, крупнейшего в мире информационно-аналитического агентства и консалтинговой компании. Годовой оборот компании составляет 4,7 млрд дол. США.

Участников исследования разделили на три группы: первой транслировалась только поисковая реклама бренда Experian; второй – реклама на Facebook; а третьей – реклама на обоих упомянутых каналах.

Как выяснилось, реализация кампаний платного продвижения Experian на Facebook совместно с запуском кампаний поисковой рекламы в ведущих поисковых системах, позволила добиться увеличению конверсии на 19 %. В то время как продвижение бренда с использованием лишь одного канала оказалось менее эффективным.

Данные, полученные по первым двум тестовым группам, позволили судить о том, что коэффициент конверсии в среднем увеличился на 11 %. Статистика по третьей группе показала: если грамотно распланировать бюджеты, то после вычета расходов на рекламу, запускаемую на обоих каналах, можно добиться увеличения конверсии до 20 %.

Также было установлено, что запуск кампаний на Facebook параллельно с поисковой рекламой позволяет снизить затраты на привлечение одного клиента на 10 % и повысить доход от конверсии, в среднем, на 8 %.

«Если каждые 10 тыс. кликов по объявлениям приносят вам 73 дополнительные конверсии и стоимость каждой – не менее 100 дол., то это уже дополнительные 7300 дол. США», – комментируют аналитики Kenshoo.

При этом инициаторы исследования рекомендуют брендам соблюдать оптимальный для их бизнеса баланс при планировании затрат на рекламу ***(Исследование: продвижение бренда на Facebook'е усиливает эффект от поисковой рекламы // Media бізнес (http://www.mediabusiness.com.ua/content/view/39765/126/lang,ru/). – 2014. – 20.06).***

***

То, какие посты показываются каждому конкретному пользователю в Ленте новостей, определяет алгоритм ранжирования Facebook. Он уже подвергался серьёзным изменениям в прошлом, но последние перемены удивили многих маркетологов, пишет Marketing Media Review (http://mmr.ua/news/id/kak-povysit-vidimost-brenda-v-novostnoj-lente-facebooka-40139/).

Ранее Adage сообщал о решении руководства Facebook несколько снизить видимость органических постов, публикуемых администраторами страниц брендов в новостных лентах. Данные основаны на статистике клиентов социальной сети. По словам представителей Facebook, такая ситуация неизбежна: социальная сеть растёт, активно увеличивается количество создаваемого пользователями контента.

В выпуске подкаста «Общественный Медиа-маркетинг» с М. Стелзнером, специалист по маркетингу компании Facebook М. Смит сказала, что число новостей, которые в конкретный момент времени

показываются активному пользователю в ленте новостей, достигло полутора тысяч. И пока это число продолжает расти, разработчикам Facebook приходится много работать, чтобы отобрать для публикации именно то, что хочет увидеть каждый конкретный пользователь. Ранжируя контент, алгоритм должен отдавать предпочтение публикациям, от которых пользователи получат удовольствие, и которые привлекут их внимание. Как результат – люди больше времени проведут на сайте. Как правило, пользователям в большей степени интересен некоммерческий и небрендированный контент.

Это значит, для бизнеса платная реклама становится лучшим способом показать новости бренда в ленте подписчиков. Но существует множество возможностей работать с этими нововведениями и продолжать собирать свою аудиторию без использования платных объявлений. Тем, кто не верит, предлагается опробовать девять перечисленных ниже способов.

1. Покинуть Facebook – не лучшее решение. Наличие публичной страницы в социальной сети предоставляет бренду массу преимуществ, если регулярно и грамотно обновлять её.

М. Смит подчеркнула, что если страницу бренда вовремя не обновлять, то пользователи начнут массово покидать ее, и эта реакция будет цепной. И хотя данное заявление настораживает, у активной страницы бренда есть множество преимуществ. Не имея страницы на Facebook, компания теряет возможность проводить конкурсы, использовать приложения, которые позволяют получить подробные данные о том, как люди взаимодействуют с постами. Есть несколько простых способов, с помощью которых можно проверить, что вы используете все возможности публичной страницы. В посте на Social Media Examiner есть рекомендации на этот счёт. Вот некоторые из них:

• Можно еще полнее использовать возможности изображения обложки, добавив в него, к примеру, целевую кнопку (call-to-action).

• Имеет смысл регулярно обновлять картинку профиля – она должна быть актуальной.

• Лучше следить за актуальностью описания компании, группы или проекта, которое размещается на публичной странице.

• Нужно убедиться, что во вкладке «Информация» разделы «Общая информация» и «Контактная информация» заполнены без ошибок.

2. Важно уделять больше времени выстраиванию своего сообщества.

Ещё один совет от М. Смит – тратить больше времени и денег на построение сообщества. По собственному опыту она знает, что немногие бренды отвечают на вопросы и общаются с пользователями на Facebook. В результате, они теряют возможность построить крепкое сообщество. Не стоит забывать, что поклонники бренда могут распространять информацию о компании и её предложениях не хуже, чем реклама.

Что касается самой М. Смит, то она регулярно отвечает на своей странице на вопросы и комментарии друзей подписчиков, управляя их вовлечённостью в процесс коммуникации.

3. Полезно использовать профили публичных лиц компании для привлечения дополнительных фоловеров.

Представители компаний, желающие набрать как можно больше подписчиков бренда в Facebook, не должны оставлять без внимания и собственные профили. Можно изменить настройки подписки, чтобы позволить пользователям подписываться на публичные посты профиля, и использовать его совместно со страницей бренда в бизнес-целях.

Друзья владельца профиля автоматически подписаны на него и при соответствующих настройках приватности публикаций видят посты в своих новостных лентах.

Чтобы позволить всем подписываться на профиль необходимо:

• Зайти в настройки;

• Кликнуть по кнопке «Подписчики» в меню слева;

• Выбрать «Все» напротив фразы «Кто может подписаться на меня?»

Количество подписчиков будет отображаться в секции «Подробнее» под изображением профиля.

Важное наблюдение: у пользовательских профилей есть преимущество перед публичными страницами при ранжировании публикаций. Вот почему создание персональной страницы и регулярная публикация интересных постов на ней позволит привлечь больше подписчиков. Можно так же воспользоваться группами Facebook чтобы привлечь поклонников за счёт постоянно обновляющегося контента на странице.

4. Допустимо экспериментировать с новыми возможностями Facebook.

Автор ряда статей и консультант по маркетингу Д. Баер также участвовал в выпуске подкаста «Общественный Медиа-маркетинг». По словам Д. Баера, далеко не все маркетологи научились и привыкли использовать в коммерческих целях Instagram, который сегодня находится в тесном родстве с социальной сетью. Instagram стремительно растёт и развивается, к тому же не исключено, что в ближайшем будущем посты из этого социального сервиса будут ранжироваться алгоритмами Facebook выше остального контента.

В Интернете всегда появляется что-нибудь новое, меняющее приоритеты. Эксперименты с этими возможностями в случае удачи помогут компании быть в тренде.

Тем, кто принял решение завести аккаунт бренда в Instagram, стоит прочитать это руководство. Facebook также постоянно вводит много новых инструментов и возможностей, маркетологам следует постоянно быть в курсе этих обновлений.

5. Можно попытаться создать собственную платформу и развивать альтернативные маркетинговые каналы.

И М. Смит, и Д. Баер считают, что любая компания, сосредоточившая маркетинговые усилия только на работе с социальной сетью Facebook, рискует. Особенно такому риску подвержены компании, которые не могут позволить себе выделять серьёзные средства на платное продвижение в Facebook. Один из способов расширить охват – это построить собственную маркетинговую платформу.

Д. Баер считает, что каждый бренд должен использовать три вида маркетинговой стратегии: платные рекламные объявления, собственная платформа, привлечение подписчиков и поклонников бренда в социальных сетях.

В качестве собственной коммуникативной платформы может выступать сайт и/или блог компании, подкаст и т. д. Следует выбирать формат, наиболее соответствующий специфике бизнеса.

6. Страница на Facebook может стать средством привлечения новых подписчиков.

Те, кто не готов строить собственную платформу или просто хочет освоит еще один канал коммуникаций, могут уделить больше внимания e-mail рассылке. Д. Хэлперн советует использовать паблик на Facebook для привлечения подписчиков. Он даже предлагает образец обращения к пользователям, которое можно разместить на своей странице в Facebook. Текст послания может быть примерно таким:

«…Возможно, вскоре вы перестанете получать контент от меня на Facebook, потому что я не вижу смысла платить Facebook за распространение [вставьте, что пожелаете]. Поэтому, чтобы быть уверенными в том, что вы ничего не пропустили, подпишитесь на почтовую рассылку», – говорится в заключительной части обращения.

7. Целевую аудиторию можно отыскать и в других социальных сетях.

По мнению Д. Баера, в 2014 г. вырастет количество компаний, использующих в качестве маркетингового канала социальную сеть Google+. Это произойдёт потому, что маркетологи активно ищут альтернативу Facebook, где они могли бы привлечь больше пользователей.

Не исключено, что в ближайшее время всплеск активности ожидает такие ресурсы, как: Pinterst, LinkedIn, Twitter и даже Snapchat.

8. Имеет смысл поинтересоваться у подписчиков, какие новости они хотели бы видеть у себя в лентах.

Если подписчики не хотят пропускать ваши обновления, можно предложить им настроить параметры Ленты новостей. После установки опции «Последние» вместо «Популярные новости», в Ленте будет отображаться больше постов.

В Facebook также есть инструмент для систематизации друзей, который позволяет перемещать пользователей в разные списки знакомств. При желании пользователю можно предложить рассортировать списки так, чтобы соотношение новостей от брендов к органическим постам было оптимальным.

Кроме того, по итогам одного из последних обновлений в алгоритма, пользователи будут видеть в своих новостных лентах не только публикации с публичных страниц, подписчиками которых являются, но и все «перепосты» этих публикаций другими аккаунтами. В том числе, и теми на которые пользователь не был изначально подписан.

9. Инвестировать в рекламу нужно с умом.

Разработчики Facebook рассчитывают на то, что после изменений в алгоритме новостной ленты бренды будут платить за то, чтобы информация о них отображалась в лентах. Конечно же, довольно неприятно платить за то, что раньше было бесплатным. Однако инвестиции в рекламу на Facebook могут быть успешными, если тратить бюджеты с умом.

Д. Баер не считает удивительным, что руководство социальной сети приняло такое решение – все социальные сети и сервисы активно зарабатывают на рекламе, а Google, к примеру, получает огромные прибыли от поисковой рекламы.

Тем, кто собирается использовать Facebook в качестве канала маркетинговых коммуникаций, полезно усвоить следующие правила:

• Используйте ретаргетинг: показывайте рекламу тем пользователям, которые недавно посещали ваш сайт, но ничего не приобрели. Так вы можете подвести их к конверсии.

• Рекламируйте контент, а не компанию: объявления, предлагающие скачать электронную книгу, поучаствовать в вебинаре или ознакомиться с подкастом, способны заинтересовать пользователей больше, чем обычная реклама бренда или товара.

• Активно используйте таргетинг – анализируйте демографические данные ваших потенциальных клиентов на Facebook»е. Это позволит вам выявить своих потребителей. Не стоит впустую тратить деньги, показывая рекламу пользователям, которым, возможно, даже не интересен ваш товар.

Д. Баер также отмечает: пока далеко не все маркетологи обратили внимание на то, что новости их компаний стали показываться в лентах пользователей реже. Однако никто ещё не заострил внимание на том, почему это произошло. Алгоритм ранжирования постов в новостной ленте призван обеспечивать более высокую видимость публикациям контента, которым пользователи делились между собой органически. В то же время, малозначимый контент от брендов, публикующийся автоматически, практически исчезнет из новостных лент.

Не стоит воспринимать эти изменения в штыки: Facebook изменился, но он не бесполезен с точки зрения продвижения бренда. Нужно приспособиться к этим переменам и понять, как извлечь из ситуации максимальную пользу ***(Купер Б. Как повысить видимость бренда в новостной ленте Facebook'а // Marketing Media Review (http://mmr.ua/news/id/kak-povysit-vidimost-brenda-v-novostnoj-lente-facebooka-40139/). – 2014. – 23.06).***

***

Весной Facebook заявил об изменении формата объявлений в правой колонке. Недавно стало известно, что официальный запуск обновления произойдет в ближайшее время.

Редизайн этих блоков объявлений стал продолжением общей политики социальной сети по работе с рекламой. Кратко ее основную идею можно выразить так: реклама может и должна быть дополнением к основному контенту.

Что значат эти изменения для рекламодателей?

Скорее всего, уменьшение количества объявлений в правой колонке вызовет конкуренцию за рекламное пространство в Facebook, что в свою очередь спровоцирует повышение цен на аукционе. И хотя последнее обстоятельство может быть крайне нежелательным для многих рекламодателей, в Facebook все же надеются, что более интересный и наглядный формат объявлений компенсирует это ***(Новый формат рекламных блоков в Facebook // Marketing Media Review (http://mmr.ua/news/id/novyj-format-reklamnyh-blokov-v-facebook-40151/). – 2014. – 23.06).***

***

Как отмечает The Wall Street Journal, подсчету фанатов и фолловеров нужно положить конец: социальные медиа не обладают такой влиятельной и побудительной маркетинговой силой, как на это надеялись многие компании. Такие выводы сделала Gallup Inc в своем новом отчете, пишет Marketing Media Review (http://mmr.ua/news/id/issledovanija-socialnye-seti-ne-okazyvajut-vlijanija-na-reshenija-o-pokupke-40152/).

Компания отметила, что 62 % из более чем 18 тыс. опрошенных американских потребителей заявили, что социальные медиа не оказывают влияния на их покупательские решения. Другие 30 % отметили некоторое влияние. Американские компании потратили 5,1 млрд дол. на рекламу в социальных сетях в 2013 г., но Gallup отмечает, что «потребители не обращают внимания на контент брендов в Facebook и Twitter».

Как сообщает WSJ, «в исследовании прошлого года, проведенного Nielsen Holdings NV, было обнаружено, что потребители больше доверяют рекламе на ТВ, в прессе, на радио, билбордах и в кинотрейлерах, чем рекламе в социальных сетях. Gallup сообщает, что бренды пришли к неверному предположению, что потребители захотят пригласить их в свою жизнь в соцсетях. Они продвигали навязчивую рекламу и отпугнули от себя многих пользователей.

В последнее время изменения относительно того, как Facebook управляет новостными лентами пользователей, блокировали способность брендов достичь своих фанатов. Теперь Facebook показывает пользователям только те посты, которые, по его мнению, будут им интересны. В результате охват брендами своих фанатов с помощью постов в Facebook в марте

составил 6,5 %, упав на 16 % по сравнению с февралем 2012 г., по результатам аналитической компании EdgeRank Checker».

Большинство потребителей не заходят в социальные сети, чтобы взаимодействовать с брендами – они там для того, чтобы общаться с пользователями, которых они знают. По результатам исследования Gallup, большинство потребителей (94 %), которые находятся в социальных сетях, используют их для общения с друзьями и родными. Их меньше всего интересуют компании или продукты.

Когда Gallup опросила более 18 тыс. потребителей относительно влияния социальных сетей на покупательские решения, 62 % отметили, что они не оказывают такового. Даже среди поколения, родившегося в 1980-х, о которых многие компании думают как о целевой аудитории в социальных сетях, 48 % ответили, что эти сайты не являлись фактором в процессе принятия решения.

В то время как многие компании соотносят количество фанатов и фолловеров с успехом в социальных сетях, Gallup находит такие метрики обманчивыми. Среди потребителей, которые поставили «лайк» или следят за компанией, 34 % заявили, что социальные сети не оказывают влияния на их покупательское поведение, а 53 % указали на небольшое влияние.

Компании часто верят, что социальные медиа могут увеличить осведомленность бренда и предоставить доступ к новой базе потребителей. Но, как считает исследование Gallup, потребители игнорируют контент брендов в Facebook и Twitter ***(Исследование: социальные сети не оказывают влияния на покупательское решение // Marketing Media Review (http://mmr.ua/news/id/issledovanija-socialnye-seti-ne-okazyvajut-vlijanija-na-reshenija-o-pokupke-40152/). – 2014. – 23.06).***

***

В соцсети «ВКонтакте» появятся платные музыкальные сервисы. Об этом «Ленте.ру» рассказал источник, близкий к компании.

Модель монетизации аудиозаписей, по данным источника, будет разработана совместно с Национальным музыкальным издательством (НМИ), с которым заключено соответствующее соглашение.

В каталог издательства входят более 50 тыс. музыкальных произведений российских авторов и около 400 тыс. зарубежных исполнителей. Эти аудиозаписи будут во «ВКонтакте» легализованы. Кроме того, активизируется работа над узаконением аудиоконтента, не входящего в данный список.

Исполнительный директор «ВКонтакте» Д. Сергеев подтвердил «Ленте.ру» заключение соглашения с НМИ.

«Суть договоренностей с НМИ действительно в передаче тех авторских и смежных прав, которые у НМИ есть, и в агрегации других прав с участием НМИ. Также будут совместно разработаны новые сервисы для монетизации

прав. В текущих сервисах музыка останется бесплатной для пользователей», – сказал Д. Сергеев.

Нелицензионные аудиозаписи во «ВКонтакте» регулярно вызывают претензии со стороны правообладателей. В апреле 2014 г. иски в арбитражные суды Санкт-Петербурга и Ленинградской области к ООО «ВКонтакте» подали звукозаписывающие компании Sony Music Russia, Universal Music Russia и Warner Music UK. Они потребовали удалить контрафактную музыку и взыскать в общей сложности 50 млн р. ущерба с ответчика ***(Музыка «ВКонтакте» станет платной // InternetUA (http://internetua.com/muzika--vkontakte--stanet-platnoi). – 2014. – 26.06).***

***

Для обычного пользователя Facebook может быть чем-угодно – возможностью узнать о новых рецептах, сыграть в игры, проверить фото, связаться с родными. Но для тех, кто пытается построить свой бизнес с помощью маркетинга в Facebook, лучше будет выбрать одну-две задачи и сконцентрироваться на них, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-brendam-nuzhno-skoncentrirovatsja-na-neskolkih-zadach-v-seti-40204/).

Выступая на Silicon Beach Fest на прошлой неделе в Санта-Монике, аккаунт-директор М. Воллрапп говорил о том, как много брендов в социальных медиа, включая Facebook, пытаются сделать слишком много или одновременно взяться за слишком много дел, в надежде закинуть более широкую сеть:

«Чтоб создать бизнес или выделиться среди множества информации необходимо взывать к эмоциям или оставаться верным голосу бренда. Я думаю, что более мелкие компании пытаются быть всем для пользователей. Определите, в какой сфере вы лучшие, и затем признайте это и копните глубже. Я думаю, иногда компании пытаются охватить ширину, а так вы никогда не сможете достичь цели».

Другая тема для дискуссии, которую затронул М. Воллрапп, носила название «Крупные бренды, стартапы и социальные сети», и рассматривала инновационные способы, с помощью которых бренды не только охватывали фанатов и потребителей, но и общались с ними.

Taco Bell достиг хороших результатов в Facebook и других социальных каналах. Как отметил Д. Дженкингс, старший бренд-менеджмер Taco Bell «мы изменили модель, как мы продаем и функционируем. Если подумать, кем являются бренды сегодня – они распространители контента. Контент – это прекрасный соединительный элемент. Вот что находит отклик у потребителей. Как вы находите то, что находит отклик? Как вы доносите это с помощью разных каналов? Какова ваша аудитория на разных каналах? Мы всегда слушаем. Вы всегда должны слушать потребителей. Сообщение 24/7».

М. Воллрапп признал, что компании до сих пор пытаются вычислить правильный способ для определения конверсии. Пока эта задача не решена,

Facebook продолжает быть эффективным для построения отношений с фанатами и потребителями.

Среди основных путей достижения охвата участники дискуссии назвали адвокатов бренда. Органический и оплаченный охват может увеличиться при содействии фанатов, которые сами распространяют сообщение (за вознаграждение или потому что им нравится продукт). Многие топ-бренды стараются найти способы вознаградить фанатов за расшаривание сообщения и расширение охвата ***(Facebook : Брендам нужно сконцентрироваться на нескольких задачах в сети // Marketing Media Review (http://mmr.ua/news/id/facebook-brendam-nuzhno-skoncentrirovatsja-na-neskolkih-zadach-v-seti-40204/). – 2014. – 26.06).***

***

Сдвиг социальной парадигмы: зачем пользователям так много сетей?

Согласно данным comScore за март 2014 г., 52 % пользователей Интернет находятся в возрасте от 18 до 49 лет, т. е. – активное большинство на потребительском рынке, пользуются услугами двух или более социальных сетей. При этом многие из них на практике предпочитает не две, а три или даже четыре социальных платформы одновременно – к такому выводу пришли маркетологи из IPG Media Lab и 140 Proof, которые решили копнуть глубже, чем это сделал comScore, и организовали дополнительные изыскания на эту тему несколько недель назад, пишет Marketing Media Review (http://mmr.ua/news/id/sdvig-socialnoj-paradigmy-zachem-polzovateljam-tak-mnogo-setej-40202/).

Все эти данные косвенно подтверждаются цифрами декабрьского исследования Pew Research, в ходе которого 42 % пользователей Интернет заявили о том, что в их социальной обойме постоянно находятся две или более соцсети.

Разницу в 10 % между двумя исследованиями закрывает тот факт, что в последнем случае исследователей интересовало отношение аудитории к строго ограниченной выборке из пяти соцмедиа-ресурсов (Facebook, Twitter, Instagram, Pinterest и LinkedIn), тогда как в первом – ко всем, без исключения, ресурсам такого типа. Кроме того, и это крайне важно, сама логика развития соцмедиа-пространства наталкивает на мысль о том, что «мультиплатформенный подход» – не просто кратковременная дань моде и не только желание попробовать всего по чуть-чуть, но, как минимум – мощный тренд, который быстро развивается и рекрутирует приверженцев.

В самом деле, сколько разноплановых и разноформатных социальных ресурсов необходимо средней компании, чтобы обеспечить адекватное современным вызовам проецирование своих деловых интересов в сети? И почему, в этом смысле, рядовые пользователи должны отличаться от компаний? Ведь, по сути, и те, и другие конкурируют в онлайн-пространстве, как с себе подобными, так и между собой, с одной единственной целью –

отхватить как можно большую часть целевой аудитории на возможно больший срок.

В этом смысле, Российские железные дороги (РЖД) напрямую конкурируют с индивидом по имени Василий за внимание пользователя под ником «Незабудка». Целью первых является заказ клиентом купейного в Сочи, целью второго – примерно то же самое, с той лишь разницей, что он сам готов заплатить за два. Кто из них победит в этой схватке – еще вопрос, но то, что оба конкурирующих субъекта попытаются использовать все доступные им соцмедиа-средства – факт.

И первый шаг к победе – представление своего «товарного предложения» и своих аргументов на всех социальных платформах, которые, по мысли субъектов, являются неотъемлемыми кусочками паззла в картине персональных пристрастий «Незабудки». С другой стороны рыночного уравнения, сама «Незабудка» искренне заинтересована, как в продвижении персонального бренда с помощью всех доступных маркетинговых каналов, так и в диверсификации, а также – классификации своих повседневных интересов и связей на основе комфортной матрицы, которую предоставляют в ее распоряжение социальные медиа.

Так устроен бизнес под названием «реальная жизнь», и это – именно то основание, которое позволяет нам сделать уверенное предположение о том, что мультиплатформенный подход более не является прерогативой юридических лиц и разного рода профессионалов. Теперь это общий подход и для «физиков», у которого есть свои причины, выражение и последствия.

Социальный кошмар или нирвана?

Люди – сложные животные и количество интересов, которые преследует один отдельно взятый индивид, обычно превосходит его способность к отслеживанию этих интересов на порядок, а то и на два. В этом смысле социальные сети предоставляют уникальный шанс попытаться удержать весь этот массив не только в поле зрения, но и в поле воздействия – когда человек получает возможность осознанно управлять колоссальными массивами разнообразных данных, не затрачивая на это всю имеющуюся в его распоряжении жизнь.

На практике это означает распределение своих интересов среди множества социальных платформ, заточенных под разные задачи и разный контент. С одной стороны, такое «расщепление юзера», с точки зрения маркетологов, представляет собой сущий кошмар, предполагающий беготню по всей необъятной сети с целью комплектации обычного потребительского профиля. С другой же, если хорошенько подумать – небывалое облегчение, происходящее из фактического делегирования полномочий по сбору и классификации данных самому предмету исследования – интернет-пользователю.

И если, с точки зрения бизнеса, такая классификация попадает под определение «аналитический труд», то с точки зрения пользователя – это всего лишь «социальная гигиена». 72 % опрошенных IPG Media Lab и 140

Proof согласны с тем, что соцмедиа-платформы представляют собой инструмент, наиболее подходящий для обслуживания определенных интересов, и 60 % утверждают, что контактируют с разными типами индивидуальных пользователей, медиа и брендами на различных, более всего подходящих для этого платформах.

Схожую ситуацию мы наблюдаем и в области пользовательской классификации социальных связей. На разных социальных платформах люди формируют различные контактные круги. Выбор конкретной платформы может зависеть, как от прочности связей с определенными контактами, так и от природы самих связей и той степени, в которой соответствующие отношения включают в себя двустороннюю коммуникацию.

В любом случае, полная картина социальных контактов потребителя, также как и исчерпывающая палитра его подлинных интересов, не могут быть представлены иначе, чем посредством кросс-платформенного анализа всей относящейся к данному субъекту информации. Одна отдельно взятая сеть всегда представляет собой только кусочек паззла, но та же самая сеть, проанализированная в рамках мультиплатформенного подхода, предоставляет бесценный, заботливо выделенный в отдельную строфу и, в этом смысле – совершенно самодостаточный, пакет данных, характеризующих конкретного потребителя с совершенно конкретной стороны.

Мир, основанный на интересах

Развитая система управления собственными интересами и связями в случае, если пользователь намерен поддерживать ее в рабочем состоянии, диктует определенные правила, без которых система превращается в фарс. И первое из таких правил гласит:

«Лайки – это не навсегда».

Данные IPG Media Lab и 140 Proof убедительно свидетельствуют: распространенное предположение о том, что пользователи способны только добавлять друзей, «читать» все новые и новые источники информации и «следовать» все новым и новым брендам, но, при этом не способны сделать шаг назад и отказаться от тех «лайков» и «фоллоу», которые им более не интересны, не более чем маркетинговый миф. Способны, еще как. В особенности те, кому от 18 до 34 лет – среди них количество нонконформистов достигает 69 %.

Приверженцы мультиплатформенного самоменеджмента удаляют свои прошлые, но вышедшие из активного употребления, связи с брендами и людьми с тем же пристрастием, с каким большинство из нас чистит зубы по утрам. Причин тому – миллион: утрата релевантности текущим задачам, которые ставит перед собой пользователь, желание обзавестись новыми связями или, скажем, окончание конкурса, под влиянием которого, в свое время был прожат «лайк».

Важный вывод состоит в том, что огромной части пользователей не жалко своего бесценного времени на управление собственным присутствием

в соцсетях и они искренне заинтересованы в том, чтобы их «социальный портрет» в любой момент времени был актуален. Для брендов такое положение вещей означает возможность полагаться на «заявленные» пользователями характеристики и предпочтения, как на заслуживающие доверия, а значит – обладающие подлинной коммерческой ценностью.

И эту возможность бренды должны использовать в полной мере: по данным IPG Media Lab и 140 Proof, пользователи выражают однозначное предпочтение рекламе, основанной на их текущих интересах (58 %), в отличие от рекламы, которая базируется на истории просмотров и демографических характеристиках.

Социальный ID

В ситуации, когда подлинную ценность обретают текущие интересы пользователей, а сами пользователи приобретают привычку жить на два, три или четыре «социальных дома», подвергая изрядной девальвации метод отслеживания посредством всего лишь одной, пусть даже и крупной, соцсети, на сцену выходит Его Величество Социальный ID.

Предвестником его будущего триумфального шествия может послужить однозначный успех такого близкого по своей сути явления, как социальная аутентификация. 67 % участников исследования IPG Media Lab и 140 Proof применяют его для входа в сторонние сервисы и приложения, а 40 % считают такой инструмент чрезвычайно полезным.

По мнению авторов исследования, кроссплатформенный и универсальный социальный идентификатор, в конце концов, должен не только заменить привычные cookie, в качестве основного средства таргетинга, но и войти в обойму данных Big Data хотя бы затем, чтобы последние сохранили свой маркетинговой потенциал ***(Сдвиг социальной парадигмы: зачем пользователям так много сетей? // Marketing Media Review (http://mmr.ua/news/id/sdvig-socialnoj-paradigmy-zachem-polzovateljam-tak-mnogo-setej-40202/). – 2014. – 26.06).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Эксперты агентства YouGov сообщили, что согласно их исследованию, активность пользователей Интернета в социальных сетях значительно снизилась.

Десять процентов пользователей покинули Twitter, около 9 % оставили Facebook – люди начинают терять интерес к общению в соцсетях.

Опрошенные сотрудниками YouGov – до 55 % – заявили, что потеряли интерес к интернет-общению. Решили, что пора скрыть жизнь от посторонних глаз, и удалили свой аккаунт 26 %. Интернет-реклама достала 21 %.

Каждый шестой – в основном это взрослые люди – не хочет, чтобы посторонний подсматривал и комментировал его жизнь.

Ранее эксперты пришли к выводу, что количество конфликтов в доме и частота общения в сети тесно связаны, напоминает Росбалт. «Конфликты вызваны чаще всего тем, что из-за социальных сетей в отношениях пропадает романтика, люди эмоционально отдаляются друг от друга, а в некоторых случаях социальные сети даже провоцируют супружеские измены», – считают медики ***(Людям надоели соцсети, – исследование // IT Expert (http://itexpert.org.ua/rubrikator/item/36373-lyudyam-nadoeli-sotsseti-issledovanie.html). – 2014. – 16.06).***

***

Крим опинився в числі найбільш нещасних регіонів Росії

Своєрідну карту любові і ненависті Росії склав аналітичний центр Brand Analytics на замовлення «Ленты.ру».

Фахівці проаналізували понад 400 млн російськомовних повідомлень від 35 млн авторів у Facebook, «ВКонтакте», Twitter, LiveJournal та інших соціальних медіа. Крім того, враховувалися коментарі, розміщені на форумах і блогах.

Як розповіла керівник проекту Brand Analytics Н. Соколова, з мільйонів постів і коментарів були відібрані чотири мільйони повідомлень від першої особи про любов і ненависть. Наприклад, «я люблю…», «я обожнюю…», «я ненавиджу…», «мене дратує…».

«Крим у рейтингу зайняв тільки 79-е місце, оскільки майже чверть повідомлень місцевих користувачів (23,83 %) носить негативний відтінок», – ідеться в повідомленні.

Найбільш нещасливими на карті Росії виявилися Дагестан, Чечня і замикає список Інгушетія. Число негативних повідомлень із цих суб'єктів перевищує 30 %.

До п'ятірки «найвелелюбніших» регіонів увійшли Карелія, Забайкальський край, Амурська, Тамбовська і Оренбурзька області.

Примітно, що Москва в рейтингу «любові і ненависті» займає всього лише 68 місце. Санкт-Петербург опустився ще нижче – на 74 місце.

Як пояснюють аналітики, відчуття щастя абсолютно не залежить від комфорту чи фінансового благополуччя користувачів.

«Здебільшого всі вивчені нами повідомлення пов'язані з сьогохвилинними відчуттями. Можна сказати, що в регіонах, які потрапили в першу десятку нашого рейтингу, люди емоційні й не соромляться говорити

про те, що люблять», – пояснила Н. Соколова ***(Крим опинився в числі найбільш нещасних регіонів Росії // FINANCE.UA (http://news.finance.ua/ua/~/1/0/all/2014/06/15/327723). – 2014. – 15.06).***

***

Команда науковців з Університету Корнелла, Університету Каліфорнії, Сан-Франциско, а також із Facebook дослідили, як емоції, виражені в постах та статусах, можуть «поширюватися» на друзів користувача соціальної мережі. Про це пише mashable.com.

Дослідницька група випадково обрала 689003 із 1,3 млрд користувачів Facebook та опрацювала їхню новинною стрічку. У частини людей була відчутна менша кількість позитивних новин, у частини – негативних.

Ті користувачі, які споживали менше позитивних новин, починали використовувати більше негативних слів, а ті, які читали більше позитивних – навпаки, зазначає один з авторів дослідження, професор Університету Корнелла Д. Ганкок.

Окрім ефекту «інфікування», дослідники помітили ефект відступу, коли люди демонстрували менше емоційних постів, намагалися писати менш експресивно.

«Спостереження та той факт, що люди були більш емоційно позитивні у відповідь на позитивні оновлення від своїх друзів, контрастує з теоріями, які кажуть, що споглядання позитивних повідомлень від друзів на Facebook може якось негативно на нас впливати», – розповідає Д. Ганкок.

Попередні дослідження припускають, що «емоційні інфекції» можна застосувати до ситуацій з реального життя: тобто взаємодія з надзвичайно щасливою людиною робить вас щасливим. Однак дослідження Університету Корнелла вважають, що «ефект інфекції» спостерігається не лише у випадку взаємодії, але й через вираження емоцій.

Відповідно до політики використання даних Facebook, дослідники не бачили змісту постів, а лише підраховували кількість позитивних та негативних слів у понад 3 млн дописів загальною кількістю в 122 млн слів. Згідно з даними дослідження, 4 млн слів були позитивними, а 1,8 млн – негативними.

Робота вчених була опублікована на сайті PNAS (Proceedings of the National Academy of Science) ***(Настрій користувача у Facebook може впливати на його друзів – дослідження // InternetUA (http://internetua.com/nastr-i-koristuvacsa-u-Facebook-moje-vplivati-na-iogo-druz-v---dosl-djennya). – 2014. – 23.06).***

Маніпулятивні технології

К информационной войне против Украины РФ подключает и все коммерческие организации – соцсети, мобильную связь и т. д.

Журналисты, активно освещающие АТО и события в Украине, выкладывающие в сеть (в том числе и «ВКонтакте») видео- и фотоматериалы из командировок на Восток и Юго-Восток Украины, обратили внимание, что их «рубит» соцсеть «ВКонтакте», информирует news.eizvestia.com (http://news.eizvestia.com/news_technology/full/314-rf-ispolzuet-socset-vkontakte-v-informacionnoj-vojne-protiv-ukrainy).

Вначале по их словам, стали исчезать ссылки, опубликованные на их страницах и на страничках групп, где они зарегистрированы. А потом, вдруг, «обнулился» доступ к личным страничкам – не удалось зайти в соцсеть с помощью личных логинов и паролей.

Самое интересное начинается, когда люди, попавшие в такую ситуацию, пытаются восстановить доступ, посредством обращения к сервисам службы поддержки «ВКонтакте».

Корреспонденты «Багнета» проверили это на собственном опыте. Вначале «бдительные админы» «ВКонтакте» требуют выслать им номер мобильного телефона. На этот номер приходит смс с кодом, посланным «ВКонтакте». Затем российская соцсеть требует выслать им четкую фотокопию… паспорта (!!!) лица, запрашивающего изменение пароля. Получив такое фото, «ВКонтакте» требует сфотографироваться на фоне монитора компьютера, на котором четко видна страничка сервиса восстановления пароля доступа в соцсеть ***(РФ использует соцсеть «ВКонтакте» в информационной войне против Украины // «Экономические известия» (http://news.eizvestia.com/news_technology/full/314-rf-ispolzuet-socset-vkontakte-v-informacionnoj-vojne-protiv-ukrainy). – 2014. – 19.06).***

***

В России активно набирают «представителей ДНР и ЛНР» для засылки в Украину. Для отправки на Донбасс ищут врачей, летчиков и экипажи боевых машин – особенно танкистов.

Это следует из сканов страниц российских сайтов и сообществ в соцсетях, размещенных киевским юристом К. Братсковским на своей странице в Facebook.

Так, 9 июня в сообществе «Русские добровольцы/Донбасс» во «ВКонтакте» было размещено объявление о приеме для «скорейшей отправки» врачей, офицеров и опытных военных – особенно танкистов.

Также фельдшеров и квалифицированных врачей ищут на сайте «Доброволец.орг». Также требуются добровольцы по следующим специальностям: операторы ПТРК (противотанковый ракетный комплекс),

ПЗРК (переносной зенитно-ракетный комплекс), ЗРК (зенитно-ракетный комплекс), АГС-17 (автоматический гранатомет станковый), огнеметчики, гранатометчики, а также экипажи БМ (боевых машин).

Кроме того, требуются опытные экипажи танков Т-72 с опытом, а также пилоты чехословацких учебно-тренировочных и учебно-боевых самолетов Л-29 и Л-39, вертолетов Ми-2 и Ка-26.

Отметим, что авторы сайта не скрывают, что вербуют добровольцев для оказания «вооруженного милосердия» на территории «бывш. Украины» ***(В России активно набирают «представителей ДНР и ЛНР» для засылки в Украину // «КОММЕНТАРИИ:» (http://comments.ua/life/474100-v-rossii-aktivno-nabirayut.html). – 2014. – 19.06).***

***

Краща зброя терористів – соціальні мережі

Вони знімають відео бойових дій, вчать робити бомби та набирають добровольців для виконання терактів. Для терористів соціальні медіа швидко стали кращим засобом поповнювати свої ряди та інструментом для ведення пропаганди. Адміністрація Twitter та Facebook намагається заблокувати таку діяльність, проте вона поки що програє.

Одним з таких терористичних угруповань, які активно використовують сучасні технології та Інтернет, є радикальне ісламістське угруповання «Ісламська держава Іраку та Сирії» (ISIS). У своїх акаунтах Twitter вони викладають матеріали розстрілів та страт, а керівництву цієї соціальної мережі поки що не вдається їх заблокувати. Сервіс мікроблогінгу вже закрив декілька акаунтів, що належали активістам цієї ісламістської організації, проте вони заводять нові.

Угруповання ISIS не є першим, яке використовує соціальні медіа для поширення своїх пропагандистських матеріалів. Інші також користуються перевагами соцмереж: швидке, легке та масове поширення інформації та думок.

«Twitter нещодавно став улюбленим інтернет-сервісом терористів, – каже Г. Вейнман. Він нещодавно провів дослідження на тему використання злочинцями соціальних медіа. – Він навіть популярніший за зроблені власноруч сайти або Facebook. Через Twitter вони поширюють пропаганду та організують внутрішню комунікацію».

Передають терористи

Світ уже давно стежить за планами терористів через їхні Twitter-акаунти. Наприклад, у вересні минулого року озброєне угруповання Аль-Шабаб запланувало атаку на торговий центр Вестгейт у Найробі (столиця Кенії). Уперше про це світ дізнався з їхнього твіту, де вони зізнавались у заподіяному та брали відповідальність на себе.

Акаунт вів майже прямий ефір нападу, у якому загинула 61 людина. Сама атака на торговий центр в інформаційному просторі виглядала досить

просто: «Святі воїни ввійшли до торгового центру опівдні, і вони ще всередині, воюють з кенійськими невірними на їхній землі».

У своєму звіті Г. Вейнман пояснює, чому терористи стали менше використовувати спеціалізовані веб-сайти та перейшли у соціальні медіа. Спеціаліст каже, що соцмережі дозволяють радикалам буквально «стукати у двері» до людей, на відміну від застарілої моделі спеціальних веб-ресурсів. Останні змушували терористів чекати, поки відвідувачі прийдуть до них.

«Терористи мають гарні причини використовувати соціальні мережі, – пише він. – По-перше, ці канали найпопулярніші у їхньої цільової аудиторії, що дозволяє радикальним угрупованням залишатись в інформаційному мейнстримі. По-друге, канали соціальних медіа мають зручний інтерфейс, надійні в роботі та безплатні. І останнє: соцмережі дозволяють терористам спілкуватися зі своєю аудиторією».

Соціальні мережі як місце навчання радикалів

Г. Вейнман каже, що декілька терористичних організацій створили свої сторінки на Facebook для вербування новобранців та надання їм навчальних матеріалів. Вони, наприклад, пропонують відеоінструкції зі створення бомб, які завантажують на YouTube, та розповсюджують ці ролики через соціальні платформи.

Хоча іноді доступних інструментів радикалам бракує і тоді вони створюють власні. У 2008 р. радикальне угруповання Хамас на Близькому Сході запустило власний аналог YouTube під назвою AqsaTube, на якому вони діляться пропагандистським відео.

Експерти також переконані, що соцмережі активно використовуються зловмисниками для координації та планування терористичних атак. Останньому особливо сприяють дешевизна та доступність мобільного зв’язку, завдяки чому вони можуть точніше відстежувати місцеположення своїх або жертв.

Один з прикладів – терористичні атаки в Мумбаї у 2008 р. Тоді терористи використовували GPS, супутникові знімки Google Earth та мобільні повідомлення командирів, щоб відстежувати чужоземців та нападати на них.

З висновками Г. Вейнмана згодний також консультант Е. Коллман, який працює консультантом в охоронній фірмі Flashpoint Global Partners. Експерт зазначає, що соціальні медіа стали сьогодні дуже важливим інструментом для терористів, які через них поповнюють свої ряди та планують атаки.

«Вони часто шукають порад та підказок в онлайні і знаходять їх, – каже фахівець. – Для них онлайнова мережа сьогодні вже важливіша за національність, плем’я або етнічну групу. Ці онлайнові зв’язки є тим клеєм, який з’єднує докупи угруповання терористів» ***(Краща зброя терористів – соціальні мережі // InternetUA (http://internetua.com/krasxa-zbroya-terorist-v---soc-aln--merej). – 2014. – 19.06).***

***

Администраторы популярной социальной сети «Одноклассники» сообщили о том, что любое сообщение, содержащее критические высказывания в адрес Президента РФ В. Путина, которое будет публично опубликовано на той или иной странице, будет заблокировано, пишет Marketing Media Review (http://mmr.ua/news/id/odnoklassniki-blokirujut-kritiku-na-putina-40133/).

По словам администрации, решение о блокировке подобных текстов было принято самостоятельно, без какого-либо давления сверху.

Стоит заметить, что сам В. Путин неоднократно упоминал в своих выступлениях, что спокойно относится к критике и даже приветствует такого рода высказывания, особенно если они носят конструктивный характер.

Однако от самих участников социальной сети «Одноклассники» начали поступать жалобы на то, что сообщения определенного характера блокируется даже в личной переписке, что является вторжением в личную жизнь ***(«Одноклассники» блокируют критику на Путина // Marketing Media Review (http://mmr.ua/news/id/odnoklassniki-blokirujut-kritiku-na-putina-40133/). – 2014. – 23.06).***

***

Информационная война против Украины: как работают пророссийские интернет-тролли

Недавно впервые были опубликованы документы, подтверждающие, что Россия усиленно работает над формированием «мнения» в западных интернет-СМИ. Одна компания из Санкт-Петербурга привлекла в этих целях несколько сотен так называемых троллей. Следы же этой деятельности ведут в Кремль, пишет немецкое издание Frankfurter Allgemeine Zeitung.

«Открыто девять аккаунтов. Отправлено 305 твитов». Это доклад А. Богачевой о проделанной за неделю работе, который она 22 апреля отправила по электронной почте своему начальнику Д. Осадчему. Уровень цензуры в Twitter минимален, пишет А. Богачева, «и поэтому можно писать более жесткие вещи».

Это ее письмо, как и тысячи других аналогичных писем, были опубликованы в российском блоге Botlai.wordpress.com, который ведет некий участник группировки Anonymous International, которая, судя по названию, является филиалом хакерского движения Anonymous. Кстати, свидетельства с соответствующими ссылками найти больше невозможно. Администрация «облака», на котором они были размещены, пожаловалась на «многочисленные нарушения» правил пользования.

Документы – а это три большие папки, или в цифровом выражении без малого один гигабайт информации – являются первым доказательством того, что Россия посредством некоего Агентства интернет-исследований из Санкт-Петербурга пытается воздействовать на общественное мнение в западных социальных сетях и онлайн-медиа. Согласно опубликованным письмам,

больше всего подобных сообщений появилось на сайтах изданий Huffington Post, Politico и WorldNetDaily.

«Дом троллей»

С начала украинского кризиса пророссийские высказывания в социальных сетях, а также в комментариях на сайтах онлайн-СМИ стали появляться все чаще, в том числе и в Германии. Авторы этих сообщений писали, что за Евромайданом стояли «фашисты», а российский президент В. Путин «защитил» подавляемых жителей Крыма и Восточной Украины, что Европа стала заложником американского империализма и т. п. В комментариях к статьям на тему Украины преобладают пророссийские высказывания, что, однако, противоречит результатам социологических исследований. В России же, в свою очередь, часто указывают на эту «поддержку».

Российская оппозиционная «Новая газета» еще в сентябре 2013 г. писала о «Доме троллей» в Санкт-Петербурге (статья «Где живут тролли. И кто их кормит»). Тогда, правда, речь шла лишь о российском сегменте Интернета. Весной Frankfurter Allgemeine Zeitung (наряду с британской The Guardian) написала о подозрениях, что многие комментарии о России могли быть поддельными, но вызвала в ответ лишь новый шквал пророссийских отзывов.

Однако доказательства российского вмешательства найти не удается. До недавнего времени газета The Moscow Times и некоторые американские сайты, в частности BuzzFeed, писали лишь об обнаруженных электронных письмах российских троллей.

Связь с Кремлем?

Опубликовано было несколько сотен неотсортированных электронных писем, датированных между осенью прошлого года и концом апреля этого года, из которых многие были отправлены на Gmail-адрес руководителя проекта Агентства интернет-исследований по имени Д. Осадчий. Д. Осадчий, однако, утверждает, по данным BuzzFeed, что никогда не работал на это агентство. Документы, в том числе о том, что он получает от агентства вознаграждение в размере 35 тыс. дол, являются, по его словам, подделками и «безуспешной попыткой провокации».

В письмах в его адрес содержатся, однако, доклады об активности в социальных сетях, подсчеты, стратегии и планы, а также сканы паспортов участвующих в этой деятельности сотрудников и бесконечное множество рекламного «спама». Если все это можно подделать, то нужно признать, что этим занимались большие мастера своего дела. Однако, по данным газеты Süddeutsche Zeitung, руководитель Агентства интернет-исследований М. Бурщик признал в телефонном интервью, что эти документы настоящие. Более подробно говорить на эту тему он, впрочем, отказался.

Согласно Süddeutsche Zeitung, в данных документах содержатся указания на связь предприятия с Кремлем. Так, доклады о работе якобы отправлялись некоему человеку по фамилии Володин. Речь идет о

заместители руководителя администрации российского президента В. Володине.

Планомерный саботаж

Согласно документам, оборот данного предприятия в апреле этого года составил 33 млн р. (в пересчете около 700 тыс. евро). На нем работают около 310 сотрудников, в том числе журналисты, блогеры и комментаторы в социальных сетях. Они обязаны четко выполнять все поручения. Из опубликованных писем следует, что некоторым из них положено оставлять порядка 50 сообщений в день на страницах онлайн-медиа, вести по шесть аккаунтов в Facebook и писать там минимум по три сообщения в день. В Twitter сотрудникам положено вести по десять аккаунтов, а на веб-странице Huffington Post и вовсе до ста аккаунтов, которые должны быть связаны друг с другом ссылками, чтобы увеличить цитируемость комментариев.

Согласно другому документу под названием «Аналитический доклад», ведется учет данных американских интернет-пользователей, в частности – предпочтения в социальных сетях разных возрастных категорий, уровень доходов и образования, время суток, когда они проявляют наибольшую активность в Интернете, политические предпочтения и т. д. Далее в документе много внимания уделено теме цензуры в американском сегменте Интернета, а именно формам модерирования в онлайн-СМИ и социальных сетях. Они подразделяются на «цензурируемые» и «нецензурируемые». Соответственно, даются рекомендации, где и что можно писать, не опасаясь, что комментарий позднее будет удален.

Скрытая пропаганда

Приводятся примеры даже на английском языке – правда, в довольно своеобразной его версии: Your nation is a nation of complete idiots. Это, очевидно, был пост на странице, подвергающейся модерации, потому что отмечен как «неопубликованный». Другой пример: Obama did shit his pants while talking about foreign affairs, how you can feel yourself psychologically comfortable with pants full of shit. Этот пост также не был опубликован. Приведены также образцы сообщений на немодерируемых сайтах, где можно писать все, что угодно. Например: Can you live in America without antidepressants? I think nooo.

По поводу Twitter, Facebook, различных форумов и хостинга YouTube даны отдельные указания. Так, было отмечено, что «на форумах уровень культуры и мышления намного ниже», чем на сайтах с политическими новостями, и поэтому там можно опубликовать, к примеру, такое сообщение: I think the whole world is realizing what will be with Ukraine, and only U.S. keep on fuck around because of their great plans and doomed by failure.

Действует ли Россия аналогичным образом в немецкоязычном сегменте Интернета, в документах не указано. Как сказал руководитель организации «Репортеры без границ» К. Мир, до сих пор доказательств этого не было найдено. Сообщения о российских троллях мир считает «правдоподобными и, с учетом нашего опыта, достоверными». По его словам, он переживает по

этому поводу, потому что комментарии нередко принимают форму личных оскорблений и, таким образом, могут привести к самоцензуре. Но еще и потому, что тем самым предпринимается попытка манипуляций общественным мнением. Пиар, в том числе и на государственном уровне, не является чем-то противозаконным, но должен быть узнаваемым именно как пиар, говорит журналист. «А иначе это становится скрытой пропагандой» ***(Информационная война против Украины: как работают пророссийские интернет-тролли // InternetUA (http://internetua.com/informacionnaya-voina-protiv-ukraini--kak-rabotauat-prorossiiskie-internet-trolli). – 2014. – 22.06).***

***

Останні кілька днів черкащани, як і жителі більшості інших областей, змітають з полиць супермаркетів кам'яну сіль. Причина тому – повідомлення в соціальних мережах та ЗМІ про те, що завод «Артемсіль», який розташований у Донецькій області, нібито, підірвали терористи.

У відповідь на ці повідомлення держпідприємство розмістило на своєму сайті офіційну заяву. У ній повідомляється, що чутки, які виникли щодо припинення та зменшення поставок продукції, не мають під собою ніяких підстав.

«Станом на 24 червня підприємство працює в звичайному режимі, постачання продукції в усі області України відбуваються за заздалегідь узгодженими планами, потреби споживачів задовольняються своєчасно і в повному обсязі», – ідеться в заяві.

При цьому повідомляється, що середньодобова навантаження у червні порівняно з попереднім місяцем збільшена майже на половину, а видобуток і реалізація продукції знаходиться на рівні аналогічного періоду минулого року. «Це в повному обсязі дозволяє забезпечити потреби ринку країни», – запевняють на підприємстві.

Так, ні «Артемсіль», ні дилери, ні супермаркети – ніхто не піднімав ціни на продукцію ***(Соляний ажіотаж на Черкащині викликаний фейком у соцмережах // Про Головне (http://progolovne.ck.ua/archives/98239). – 2014. – 26.06).***

***

На сьогодні в соціальних мережах знайдено більш ніж півтори тисячі антиукраїнських співтовариств та груп, що «висвітлюють» діяльність терористів

Зокрема, у соцмережі «ВКонтакте» за запитом «Новороссия» знайдено 965 співтовариств. У найбільшому з них 78 167 учасників; за запитом «ЛНР» – 131, у найбільшому – 27 322 учасників, за запитом «ДНР» – 397, повідомляє Еспресо.TV.

В «Одноклассниках» за тими ж запитами видає 300 груп, у найбільшому з яких 74 840 учасників.

Крім того, у Facebook за запитом «Новороссия» – 28 груп, найбільше – 2303 учасника.

Нагадаємо, російські ЗМІ висвітлюють інформацію про Україну у викривленому світі ***(Терористи створили більш ніж півтори тисячі антиукраїнських співтовариств в соцмережах // Espreso.tv (http://espreso.tv/news/2014/06/25/terorysty_stvoryly_bilsh_nizh_pivtory_tysyachi_antyukrayinskykh_spivtovarystv_v_socmerezhakh). – 2014. – 25.06).***

***

На 90 % поширена останнім часом інформація в соціальних мережах про так званих «невдячних» біженців зі Сходу України є фейковою.

Про такі результати розслідування під час прес-конференції на тему: «Про вимушених переселенців з Донбасу: правда у відповідь на поширювані міфи» повідомив координатор з поселення у Львові О. Коляса, інформує кореспондент «Вголосу».

За його словами, в інтернет-просторі поширюється інформація про невдячних біженців з Донбасу, а також про кричущі випадки їхньої нахабної поведінки. «Ми з деякими журналістами провели невеличке розслідування щодо пошуку джерел цієї інформації, і вияснили, що такі меседжі поширюють люди, які у більшості випадків не мають відношення до поселення біженців зі Сходу України», – додав він.

Коли ж «авторів» просили прокоментувати опубліковану ними інформацію, то вони, як зазначив О. Коляса, не відповідали, посилаючись на конфіденційність та незручність.

Також він додав, що сьогодні саму ідею допомоги біженцям намагаються різними методами дискредитувати та налаштувати Західну Україну проти Східної.

До Львова, як зазначив О. Коляса, приїжджає інтелігенція, і дуже рідко їдуть на Захід люди, які є представниками робочого класу.

«Натомість, завдяки проведеній негативній інформаційній компанії, у нас виникли проблеми у пошуках оренди для біженців. Люди повідомляють, що вони не хочуть селити людей зі Сходу, бо вони такі от невдячні і так далі», – додав він.

О. Коляса також розповів, що нещодавно на рецепції одного із львівських готелів повідомили, що вони не будуть селити чоловіків зі Сходу, мовляв, «нехай ідуть воювати, нехай ідуть стріляти».

«Я говорив із чоловіками, які приїхали. Вони аргументували, що не воювали, не тримали ніколи зброю в руках і якщо їх відправити зараз на фронт, то це буде те саме, що із тими хлопцями під Волновахою. Тобто не всі люди здатні стріляти і часто вони навіть самі говорять, що із того боку барикад стоять їхні колишні друзі, або сусіди. І це є також моральний певний момент», – повідомив координатор з поселення у Львові.

За його словами, наразі поселення біженців у Львові закрили, оскільки місто є уже перезавантажене, люди виснажені. Він додав, що «на квартири львів'яни прийняли 100 сімей із Криму та Сходу України».

Нагадаємо, що раніше Дрогобицька міськрада вирішила не брати і не надавати допомогу здоровим чоловікам зі Східної України з тим, щоб вони не тікали зі сходу, а воювали з терористами ***(Інформація про «невдячних» біженців є фейковою – координатор поселення у Львові // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/informatsiya_pro_nevdyachnyh_bizhentsiv_zi_shodu_ie_feykovoyu__koordynator_poselennya_u_lvovi_149544.html). – 2014. – 26.06).***

***

Twitter повинен стати полем битви для України в інформаційній війні

24 червня провідний американський портал Yahoo розмістив новину:Ukraine helicopter downed by rebel fire, nine killed. Українською це лунає як: «Український гвинтокрил збито повстанцями, дев'ятеро вбито». Я припустив, що такими темпами скоро писатимуть новини як «повстанці» збивають гвинтокрили з… терористами. У Facebook мені зауважили, що слово «rebel» має негативне означення. Не бачу теми для суперечок, бо на Сході України проти громадян країни воюють терористи і жодних «повстанців» там нема за визначенням.

Сила слова величезна. Для людини за кордоном, якій байдуже де Україна, зовсім небайдуже чи лунають в новині слова «повстанець», чи «терорист». Бо «повстанець» – це людина, яка воює з режимом. Це слово, що має конкретний відтінок після rebels (повстанців) Тунісу, Лівії, Єгипту як борців проти автократії. Значення і реакцію на слово «терорист» неважко передбачити.

Слово «повстанець» примушуватиме далекого від українських реалій американця підписувати петицію про припинення вогню «київським режимом». Слово «терорист» викликатиме почуття солідарності американського обивателя з українцями. Які відтінки нестиме світу новина про Україну, так люди за кордоном і сприйматимуть наші події.

Самі медіа, як згаданий вище YahooNews, теж пишуть новини не лише з повідомлень російських інформаційних агентств. Часто вони користуються Twitter та ретельно відстежують трендові повідомлення з яких потім і вибудовують новини. Якщо трендові повідомлення нестимуть слово «повстанці», то це слово, найімовірніше, з'явиться в новині. Такі реалії, бо кожна редакція на Заході має економити, а Twitter є швидким і безплатним способом отримати інформацію.

Варто відкрити сервіси, що дають можливість моніторити повідомлення за хештегами і ввести ключове слово Ukraine. До 90 % повідомлень за цих хештегом спрямовані на підтримку «повстанців». Цікава структура таких твітів. За даними сервісу Tweet Binder лише протягом

півтори години вечора 24 червня оригінальних твітів з хештегом #Ukraine було 153, 536 твітів – були посилання і зображення, 1262 – це були ревіти (аналог репостів у Facebook) ***(Twitter повинен стати полем битви для України в інформаційній війні // UAINFO (http://uainfo.org/yandex/346001-twitter-povinen-stati-polem-bitvi-dlya-ukrayini-v-nformacyny-vyn.html). – 2014. – 25.06).***

Зарубіжні спецслужби і технології «соціального контролю»

1 августа в России начнут действовать нормы, которые обязывают интернет-компании в течение полугода хранить данные о своих пользователях и по первому требованию передавать их уполномоченным органам, которые ведут оперативно-розыскную деятельность, в том числе логины пользователя, все адреса электронной почты (как основной, так и той, что используется для переадресации), список всех его контактов, категории контактов, количество и объем полученных и переданных пользователем сообщений, все изменения в аккаунте и попытки его удаления.

В прошлом месяце наша редакция провела исследование «Какими почтовыми сервисами пользуются украинские госслужащие». Его результаты показали, что многие чиновники используют российские почтовые сервисы в рабочих целях.

Мы решили поинтересоваться, собираются ли российские интернет-компании передавать конфиденциальную информацию о своих пользователях спецслужбам и как будут реагировать на нововведения соседей украинские власти.

Руководитель группы по связям с общественностью Яндекс.Украина Н. Журавлева рассказала нам, что руководство компании пока ожидает обнародования официальных документов.

«Российское ООО “Яндекс” не может прокомментировать планирование своей работы после 1 августа, поскольку основные детали регулирования будут зафиксированы в девяти отдельных подзаконных актах, которые еще пока находятся на этапе обсуждения в рабочих группах при правительстве России. До обнародования официальных документов коллеги затрудняются давать оценку новым правилам.

Вообще же российские СМИ пока пишут о разных вариантах развития событий. Ну а мы, как и сказали, не готовы комментировать планы, слишком рано оценивать новые правила, потому что их еще нет».

Руководитель стратегических PR-проектов Mail.Ru Group Н. Богданович подтвердила намерение компании содействовать работе спецслужб.

«В ответ на ваш запрос можем сказать только то, что мы будем действовать в соответствии с законодательством РФ», – сообщила она нашему изданию.

Представители «Рамблер Интернет Холдинг» на наш запрос не ответили.

Также мы обратились в государственные структуры с вопросом, как они собираются бороться с возможными утечками информации потенциальному противнику.

В СНБО нас уверили в том, что этот вопрос чрезвычайно важен для информационной безопасности государства, однако отвечать не стали, сославшись на более компетентных в этом вопросе Госспецсвязи.

Глава Государственной службы специальной связи и защиты информации В. Зверев уверил нас, что работники госслужб, которые работают с секретной информацией, никогда не станут использовать для ее передачи Интернет. Остальным госслужащим достаточно соблюдать разработанные ведомством рекомендации по информационной безопасности.

«Если сотрудники госслужбы работают с секретной информацией, у них вообще нет доступа в Интернет, они пользуются выделенной сетью. Также разработаны рекомендации Госспецсвязи по информационной безопасности государственных учреждений, которые, к сожалению, не все читают. В целом существует около 140 нормативных документов в области связи, которые мы регулярно дополняем. Если их придерживаться, никакой утечки информации не будет. Но самое главное – человеческий фактор. Если госслужащий понимает, что информация несет конфиденциальный характер, но разглашает ее, к примеру, по телефону, ответственность только на нем. Защитить его от всех возможных угроз служба не в состоянии, и у нас нет такой задачи. Чтобы минимизировать риск утечки, на любом предприятии, даже коммерческом, работает офицер по безопасности, который отвечает не только за доступ в помещение, а и за сохранение информации, которая циркулирует у него на предприятии. И он несет персональную ответственность за это перед руководителем. А по поводу почтовых ящиков – нужна определенная дисциплина. Для государственных структур необходимы рекомендации об использовании украинских почтовых ресурсов. Но это не наша функция, а Госинформнауки, которым уже давно стоило подталкивать к этому общество. К тому же никто не думал, что у нас будет такая ситуация с Россией. Так было удобнее, российские почтовые сервера лучше работали и т. д. Поэтому этот вопрос был упущен, ведь у нас свободное интернет-сообщество».

Также мы получили ответ от СБУ, в котором нам сообщили, что согласно требованиям ст. 8 Закона Украины «О защите информации в информационно-телекоммуникационных системах» информация, которая является собственностью государства или информация с ограниченным доступом, требование относительно защиты которой установлено законом, должна обрабатываться в системе с применением комплексной защиты информации с подтвержденным соответствием.

Руководитель пресс-центра М. Остапенко уверила нас, что органы Службы безопасности Украины работают над усовершенствованием законодательной базы в сфере информационной безопасности страны, а

также, в рамках закона, занимаются предупреждением нарушений конфиденциальности информации, которая обрабатывается в госорганах.

Нам сразу стало спокойней на душе. Неважно, что добрая половина украинских чиновников переписывается с ящиков расположенных на заграничных серверах, которые доступны иностранным спецслужбам – главное СБУ бдит.

Кстати, почему-то ящики директора дочернего предприятия минобороны «Укрспецчастоты» расположены один на Gmail, а основной на yandex.ru – это так, для примера ***(ФСБ сможет читать переписку украинских чиновников // InternetUA (http://internetua.com/fsb-smojet-csitat-perepisku-ukrainskih-csinovnikov). – 2014. – 17.06).***

***

Прокуратура Львовской области начала расследование деятельности интернет-сообщества «Львовская народная республика», которая направлена на нарушение территориальной целостности Украины, сообщает корреспондент proIT со ссылкой на пресс-службу ведомства.

Так, 14 июня в Единый реестр досудебных расследований внесены ведомости о совершении уголовного правонарушения предусмотренного ч. 1 ст. 110 Уголовного кодекса (посягательство на территориальную целостность и неприкосновенность Украины).

Поводом для регистрации указанного уголовного производства стало обнаружение в Интернете информации о противоправной деятельности агитационного интернет-сообщества «ЛНР – Львовская народная республика», которая функционирует в социальной сети «ВКонтакте». «В группе формируются деструктивные взгляды и мысли отдельных граждан, связанные с посягательством на территориальную целостность и неприкосновенность Украины», – сообщает ведомство.

Производство для проведения дальнейшего досудебного расследования направлено в следственный отдел управления Службы безопасности Украины в Львовской области.

По состоянию на 14:30 вторника сообщество насчитывает 6221 аккаунтов, 3245 из которых зарегистрированы в Украине, а 2439 – в России ***(Прокуратура завела дело на группу ЛНР во «ВКонтакте» // proIT (http://proit.com.ua/news/telecom/2014/06/17/153605.html). – 2014. – 17.06).***

***

Представители Британской разведывательной службы заявили о праве перехвата коммуникаций, которые проходят через такие популярные сервисы как Facebook, Google и Twitter, серверы которых расположенные в США или других странах, даже если информационных обмен происходит между британскими гражданами. Об этом сообщает New York Times со ссылкой на отчет Privacy International.

В отчете сообщается, что вышеупомянутая информация получена в результате данных правительственного документа, предоставленного адвокатам во время судебного процесса.

В кратком изложении документа сказано, что все коммуникации между британцами, которые осуществляются при помощи социальных сетей, независимо от местонахождения их серверов, и случаи использования поисковых систем, которые не являются британскими, являются «внешними контактами» и подлежат перехвату.

Адвокатская организация Privacy International отказалась комментировать правительственное решение до тех пор, пока информация официально не подтверждена.

Представители компании Google заявили: «Мы предоставляем данные пользователей правительству только в соответствии с законом. Команда наших юристов рассматривает каждую заявку. Если причины запроса данных пользователей не соответствуют законодательству – мы отказываем в предоставлении информации».

В прошлом году организации Privacy International Amnesty International подали иск против британских властей в связи с информацией, предоставленной Э. Сноуденом. Активисты различных групп добиваются остановки британской программы разведки Tempora, которая позволяет спецслужбам перехватывать интернет-трафик ***(Британские разведывательные службы обвиняются в перехвате web-трафика // InternetUA (http://internetua.com/britanskie-razvedivatelnie-slujbi-obvinyauatsya-v-perehvate-web-trafika). – 2014. – 18.06).***

***

Служба безопасности Украины возбудила дело против пользователя Facebook за призывы к свержению государственной власти. Об этом сообщает пресс-служба прокуратуры Закарпатской области.

«В ходе мониторинга социальных сетей установлено, что на публичной странице социальной сети Facebook одним из пользователей были распространены открытые обращения, содержащие публичные призывы к насильственному изменению или свержению конституционного строя и захват государственной власти, то есть признаки уголовного правонарушения, предусмотренного ч. 2 ст. 109 УК (публичные призывы к насильственному изменению или свержению конституционного строя или к захвату государственной власти, а также распространение материалов с призывами к совершению таких действий)», – рассказал начальник отдела прокуратуры Закарпатской области А. Василенко.

По указанному факту следственным отделом Управления СБУ в Закарпатской области начато досудебное расследование уголовного правонарушения, предусмотренного ч. 2 ст. 109 УК Украины.

Отраслевым отделом прокуратуры области, в свою очередь, обеспечивается прокурорский надзор за соблюдением законов при

осуществлении досудебного расследования указанных уголовных производств. С целью быстрого и полного проведения досудебного расследования и принятия окончательного процессуального решения, даны соответствующие указания и определены сроки их выполнения ***(СБУ возбудила дело против пользователя Facebook за призывы к свержению госвласти // Весь Харьков (http://all.kharkov.ua/news/crime/sby-vozbydila-delo-protiv-polzovatelia-facebook-za-prizyvy-k-sverjeniu-gosvlasti.html). – 2014. – 20.06).***

***

Кибервойна в Украине идет уже не первый год

Несколько дней назад издание The Financial Times фактически шокировало украинскую публику сообщением о том, что Россия проводит против Украины высокотехнологичную кибероперацию, о которой власти в Киеве едва догадываются.

По данным источников FT, Россия еще за несколько лет до крымского кризиса начала проникать в компьютерные системы Украины. В настоящее время речь идет как об «актах цифрового вандализма» («порча сайтов и атаки, затрудняющих доступ к сервисам»), так и о более серьезных вещах. С точки зрения опрошенных FT экспертов, эта операция станет «ключевым моментом» в истории кибервойн.

О том, насколько изложенная в газете информация, отвечает действительности, и почему украинская ИТ-инфраструктура оказалась настолько уязвимой для кибератак, рассказывает О. Сыч, технический директор антивирусного проекта Zillya!

По его словам, ситуация в киберпространстве Украины в настоящее время действительно тревожная, однако таковой она стала ещё до украино-российского конфликта. Дело в том, что наша страна всегда была в списке лидеров по распространённости киберугроз. Кроме того, Украина периодически появляется в топах различных рейтингов по ряду критериев: происхождение вредоносных программ, размещение серверов управления ботнетами, родина крупнейших хакерских группировок. В этом плане украинское государство напоминает «дикий» запад: можно много чего себе позволить, и за это, с высокой долей вероятности, ничего не будет. Причин тому много: несовершенное законодательство, отсутствие профессиональных, мотивированных и поддерживаемых государством киберподразделений, практически отсутствие собственных разработчиков решений в области информационной безопасности (ИБ).

Сегодня ситуация обострилась ещё больше: ранее хакерские атаки, взломы серверов и заражение ПК были только «черным» бизнесом, применяемым в качестве инструментов в конкурентных войнах, вымогательстве и краже финансовой информации с целью наживы. С обострением политической обстановки многие группировки киберпреступников сменили вектор борьбы, применяя те самые методики

уже в других целях – для хищения государственных секретов, блокировки информационных ресурсов, дискредитации официальных сайтов. Известная история со взломом сети ЦИК, произошедшая накануне выборов, шокировала многих экспертов. Ведь сеть ЦИК находилась под контролем более двух месяцев, и этот факт не был замечен специалистами до того момента, пока хакеры не начали активные действия.

Кибервойна идёт уже не первый год – для специалистов это очевидно. А вот рядовые граждане узнают об этом по таким громким событиям, как взлом сети ЦИК. Но в тот момент, когда мы получаем информацию о взломе, операция атакующей стороны, по сути, завершается; их задача к тому времени или выполнена, или же ее выполнение сорвано. Кстати, в большинстве же случаев мы даже ничего не узнаем об успешных атаках, пока нападающая сторона не захочет воспользоваться её плодами, либо государство не займётся всерьёз вопросом защиты IT-инфраструктуры в целом и каждой отдельной информационной единицы в частности.

К сожалению, вышеописанная атака ЦИК может быть лишь вершиной айсберга, убежден О. Сыч. Нашей стране нужно больше внимания уделять «выращиванию» собственных специалистов по информационной безопасности, в то время как государство закупает импортные средства защиты, лишая тем самым возможности развития собственную отрасль. Специалисты по ИБ, в основном, стремятся получить максимум сертификатов по использованию и конфигурированию различных решений в области информационной безопасности, превращаясь, таким образом, в обслуживающий персонал по установке и настройке программ и оборудования. На фоне этого ИТ-специалисты и администраторы занимаются безопасностью систем по остаточному принципу (причем нередко времени на это совсем не остаётся). Для государственных систем разработано большое количество нормативных документов, решений для организации комплексной защиты информации и т. п. Но многие из них сложны в реализации, не продуманы в части практического применения и, порой, просто игнорируются на местах. В результате, формально мы имеем разработанные и внедрённые методики защиты, а фактически они есть далеко не везде.

Таким образом, шокирующая своей прямотой информация, изложенная на страницах The Financial Times, во многом может оказаться горькой правдой ***(Кибервойна в Украине идет уже не первый год // InternetUA (http://internetua.com/kibervoina-v-ukraine-idet-uje-ne-pervii-god). – 2014. – 20.06).***

***

Роскомнадзор договорился с Twitter об удалении в ближайшие несколько дней новых аккаунтов «Правого сектора». Об этом сообщил журналистам глава ведомства А. Жаров.

По его словам, на переговорах с вице-президентом Twitter К. Кроуэллом стороны обсудили незаконность с точки зрения российского законодательства десятка аккаунтов, зарегистрированных в соцсети.

«Это касается новых аккаунтов “Правого сектора”, которые появились в Twitter, и в отношении которых к нам пришли соответствующие требования со стороны Генпрокуратуры. Мы договорились с Twitter, что эти аккаунты, а их около десятка, будут в ближайшие несколько дней удалены», – сказал А. Жаров.

Он отметил, что на решение об удалении аккаунтов не влияет тот факт, что они зарегистрированы не на территории России.

«Для нас важно, что они распространяют информацию на понятном гражданам России языке и что она является незаконной. Поэтому мы надеемся, что в ближайшие дни этот вопрос будет урегулирован», – сказал А. Жаров ***(Twitter удалит аккаунты «Правого сектора» по просьбе Роскомнадзора // InternetUA (http://internetua.com/Twitter-udalit-akkaunti--pravogo-sektora--po-prosbe-roskomnadzora). – 2014. – 23.06).***

***

Представник сервісу мікроблогів Twitter спростував заяву глави Роскомнадзора О. Жарова про блокування акаунтів, які російська влада вважає екстремістськими. Про це в понеділок, 23 червня, повідомили на телеканалі «Дождь» із посиланням на інтернет-видання BuzzFeed, пише Zaxid.net (http://zaxid.net/news/showNews.do?twitter_sprostuvav_zayavu_roskomnadzora_pro_mozhlive_blokuvannya_akkauntiv_pravogo_sektoru&objectId=1312498)

«Заява не зовсім вірна, ми не домовлялися видаляти акаунти», – заявив співрозмовник видання.

Крім того, BuzzFeed повідомило, що компанія не буде наймати спеціального представника для зв’язків з російською владою ***(Ганкевич Р. Twitter спростував заяву Роскомнадзора про можливе блокування аккаунтів «Правого сектору» // Zaxid.net (http://zaxid.net/news/showNews.do?twitter_sprostuvav_zayavu_roskomnadzora_pro_mozhlive_blokuvannya_akkauntiv_pravogo_sektoru&objectId=1312498). – 2014. – 23.06).***

***

Американская секретная служба США – Агентство по национальной безопасности – собирается приобрести программу, которая будет считывать сарказм в определенных социальных сетях. Целью этой покупки является обеспечение безопасности главе Соединенных Штатов Америки. Данная программа должна будет отслеживать необходимые сообщения и уметь работать с большими объемами информации. Только это, по мнению сотрудников секретной службы, обеспечит поиск нужной информации и позволит получить оптимальные результаты.

Агентство планирует заключить контракт с производителем данной программы, а его срок составит пять лет..

Помимо этого заказчик заинтересован в следующих полезных функциях программы: умение распознавать лидера какого-либо мнения общественности, делать подробный анализ информации на сегодняшний момент, подключаться к архивам социальной сети Twitter. Важным условием в работе программы является ее совместимость с Internet Explorer 8.

Э. Донован утверждает, что данная программа сделает анализ социальных сетей более простым занятием, что позволит быстрее решать проблемы, которые интересуют пользователей мировой сети. Пресс-секретарь агентства говорит о том, что основной целью является мониторинг средств массовой информации в соцсетях. А это, в свою очередь, является одной из 16–18 целей агентства ***(Секретная служба США планирует приобрести программу по контролю соцсетей // IT Expert (http://itexpert.org.ua/rubrikator/item/36519-sekretnaya-sluzhba-ssha-planiruet-priobresti-programmu-po-kontrolyu-sotssetej.html). – 2014. – 24.06).***

***

Главный юрист компании Microsoft Б. Смит в своем выступлении в рамках конференции GigaOm Structure в Сан-Франциско утверждает, что шпионский скандал, связанный с Агентством национальной безопасности США, будет иметь негативные последствия для американских технических компаний. Об этом сообщает The Register.

Он также добавил, что ситуация, которая наблюдается с июля, снижает уровень доверия населения к американским техническим компаниям в таких значимых городах как Брюссель и Берлин.

Китай уже отказался от использования операционной системы Windows 8 согласно договору о закупках в государственном секторе. Китайские власти объяснили это тем, что операционная система Windows 8 несет угрозу кибербезопасности страны.

В случае, если власти США не объяснят правила, согласно которым ведется перехват информации в стране и за рубежом, а также в какой мере спецслужбы используют свои методы против технических компаний, то есть реальная вероятность того, что это нанесет серьезный удар по американским техническим компаниям.

Б. Смит также добавил, что основополагающей успешного бизнеса является предоставление услуг, которым люди доверяют. Представители Microsoft придерживаются мнения о том, что даже если компания оснащена наилучшим оборудованием, обеспечивающую ее информационную безопасность, это не может уберечь от хищения данных спецслужбами ***(Microsoft: Шпионский скандал АНБ снижает уровень доверия к американским техническим компаниям // InternetUA (http://internetua.com/Microsoft-shpionskii-skandal-anb-snijaet-uroven-doveriya-k-amerikanskim-tehnicseskim-kompaniyam). – 2014. – 22.06).***

***

В МТС розповіли, як спецслужби можуть прослуховувати абонентів

Розробники телекомунікаційного обладнання залишили «дірки», які можуть використовувати спецслужби для прослуховування абонентів. Про це заявив директор з корпоративного управління і контролю «МТС Україна» О. Проживальський в інтерв'ю AIN.

За його словами, звинувачення операторів мобільного зв'язку в тому, що вони «оповіщали» людей на Майдані відомими СМС про заборону участі у заворушень безпідставні, пише «Українська правда».

«Ці повідомлення розсилали піратські базові станції, які підключились до наших мереж», – розповів О. Проживальський.

Він пояснив, що телефони абонентів «запрограмовані таким чином, щоб підкючатись до найсильнішого сигналу, який вдається зловити».

«Спецслужби встановлювали поблизу Майдану такі базові станції, телефонии протестувальників прив'язували до цих станцій, і на ці телефонии надсилали СМС», – розповів представник МТС.

«Буду говорити як є, не приховуючи – з цими станціями працювали українські спецслужби за завданням колишньої влади», – додав він.

О. Проживальський пояснив, що в Криму, коли операторів, зокрема МТС звинуватили у співпраці з окупантом, такими ж станціями просто користувались уже російські спецслужби.

За його словами, це можливо тому, що «очевидно, розробники телекомунікаційного обладнання спеціально залишили таку "дірку" для своїх спецслужб – щоб у випадку чого нею можна було скористатись» ***(В МТС розповіли, як спецслужби можуть прослуховувати абонентів // InternetUA (http://internetua.com/v-mts-rozpov-li--yak-specslujbi-mojut-prosluhovuvati-abonent-v). – 2014. – 21.06).***

***

Китайские власти запустили кампанию против «интернет-контента, провоцирующего терроризм и насилие».

Как передает государственное информагентство Синьхуа, по данным экспертов, видео- и аудиозаписи, опубликованные в Интернете, стали одной главных причин высокого уровня «террористических атак».

Предполагается, что с помощью всемирной сети людей провоцировали на нападения и обучали делать бомбы.

В Китае регулярно происходят нападения на мирное население, в которых власти обвиняют этнических уйгуров из Синьцзяна, борющихся за независимость. Однако корреспонденты Би-би-си отмечают, что кампания в Интернете может быть направлена не только против уйгуров.

Пекин уже осуществляет жесткий контроль за Интернетом. Сайты, которые признаны подрывными, немедленно блокируются, а политически двусмысленные комментарии удаляют ***(Китай решил бороться с***

«терроризмом в интернете» // InternetUA (http://internetua.com/kitai-reshil-borotsya-s--terrorizmom-v-internete). – 2014. – 21.06).

***

Блог WhoIsHostingThis підготував інфографіку «Інтернет цензура: Карта світу». На ній позначена інформація про свободу мережі на всіх континентах.

Як зазначають в описі інфографіки її автори, вільний доступ до інформації та розваг через Інтернет для багатьох є швидше правом, ніж привілеєм. Натомість є суспільства, які потерпають від цензури.

«Переважно інтернет-цензура здійснюється під виглядом боротьби із піратством комп'ютерних програм та іншими типами нелегального обміну контентом», – ідеться в повідомленні.

Іншими правовими підставами цензури та моніторингу контенту є державний захист моралі. Однак часто ті ж самі країни, що нібито діють на благо своїх громадян, агресивно придушують громадські протести, зазначають автори.

Інфографіка складається з карт кожного континенту, на яких кольором позначений ступінь цензурованості Інтернету в певній країні. До кожної мапи додається більш детальне пояснення, щодо характеру онлайн-заборон. Інфографіка доступна на сайті за посиланням: http://osvita.mediasapiens.ua/material/31926.

Найбільш негативна ситуація спостерігається в Сомалі, Північній Кореї, Китаї, Сирії, В'єтнамі.

Україну віднесли до категорії країн із низьким рівнем заборон в Інтернеті ***(Сервіс WhoIsHostingThis опублікував світову карту інтернет-цензури // Громадська організація «Телекритика» (http://osvita.mediasapiens.ua/material/31926). – 2014. – 23.06).***

***

Нижняя палата конгресса США поддержала законопроект, который будет ограничивать действия Агентства по национальной безопасности США. Теперь АНБ не сможет прослушивать и перехватывать информацию без соответствующего ордера.

Напомним, что согласно информации, предоставленной Э. Сноуденом в 2013 г., АНБ обвинялось в отслеживании коммуникаций американских граждан без необходимых для этого ордеров.

Член конгресса З. Лофгрен подала законопроект «Запрет на использование средств для проведения несанкционированного перехвата информации американских граждан». 293 участника заседания нижней палаты конгресса США поддержали законопроект, 123 проголосовали против. Постановление касается только США, и все же было принято из-за того, что АНБ использует свои полномочия зачастую нелегитимно.

М. Румольд, юрист по гражданским свободам в Electronic Frontier Foundation, заявил, что он доволен результатами голосования.

В конгрессе приняли решение об ограничении полномочий Агентства национальной безопасности. Теперь АНБ не сможет вторгаться в международные коммуникации американских граждан, а также устанавливать вредоносное ПО на устройства. Для того чтобы законопроект стал законом необходима подпись главы США Б. Обамы ***(Американские власти одобрили законопроект, ограничивающий нелегитимные действия АНБ США // InternetUA (http://internetua.com/amerikanskie-vlasti-odobrili-zakonoproekt--ogranicsivauasxii-nelegitimnie-deistviya-anb-ssha). – 2014. – 23.06).***

***

ДАІ знаходить порушників через коментарі у Facebook

У Державтоінспекції стверджують, що враховують відео та публікації в Інтернеті про скоєні правопорушення і навіть стежать за коментарями під новинами.

У ДАІ розповідають нещодавній випадок, який стався з дівчиною і водієм на Toyota Land Cruiser Prado. Дізнавшись із коментарів у соцмережі Facebook, що державний номер на автомобілі нібито належить зовсім іншому авто, ДАІ перевірила дану інформацію і склала на водія позашляховика адміністративний протокол за керування ТЗ із номером, який йому не належить.

«Ми вдячні громадянам, які повідомляють про факти порушення законодавства. Небайдужість учасників дорожнього руху, помножене на співпрацю з правоохоронними органами, дозволяє швидко виявляти порушників і приймати відповідні заходи», – заявляє начальник Департаменту ДАІ МВС України А. Сіренко ***(ДАІ знаходить порушників через коментарі у Facebook // Інформаційний портал «Стик» (http://styknews.info/novyny/sotsium/2014/06/26/dai-znakhodyt-porushnykiv-cherez-komentari-u-facebook). – 2014. – 26.06).***

***

В России будут судить за ретвиты и репосты

Российские Минкомсвязи и Минкультуры отказались поддерживать инициативу Минэкономразвития, предлагавшего распространить действие антипиратского закона только на полные тексты литературных произведений. В итоге даже за небольшую цитату из чужого текста можно оказаться в суде, пишут «Известия».

Согласно местному законодательству, без согласия правообладателя и без выплаты вознаграждения, но с обязательным указанием имени автора произведения, разрешается «цитирование... произведений в объеме, оправданном целью цитирования». Однако законом не определено, какой

именно объем цитирования является оправданным, поэтому суд будет решать, принимать ли меры в каждом конкретном случае.

В Минэкономразвития уверены, что переносить эти вопросы на уровень суда неправильно: конкретики нет, и любая цитата или репост могут быть признаны нарушением закона, считает представитель Минэкономразвития.

«Принятие законопроекта в нынешнем виде – мощная диверсия против российской экономики. В сети может появиться новый вид мошенничества – наподобие патентного троллинга», – считает президент Ассоциации интернет-издателей И. Засурский.

В Минкомсвязи никаких угроз не видят. «Мы не думаем, что серьезные правообладатели будут гоняться за репостами. Их бизнесу сие не грозит», – заявил замглавы Минкомсвязи А. Волин.

С августа 2013 г. в России действует антипиратский закон в отношении видео, напоминает «Лента.ру». Администрации сайтов, на которых правообладатель обнаружил нарушение своих прав на фильм, направляется требование закрыть доступ к соответствующим страницам. Если это не сделано в положенные сроки, пиратский контент блокирует Роскомнадзор ***(В России будут судить за ретвиты и репосты // InternetUA (http://internetua.com/v-rossii-budut-sudit-za-retviti-i-reposti). – 2014. – 24.06).***

***

Исследователи, разработавшие концепцию вики-сайтов, создадут базу данных террористов в виде социальной сети.

Компания Modus Operandi из Флориды, разработавшая концепцию вики-сайтов, решила создать базу данных, которая позволит пользователям отслеживать террористов. Ее особенностью станет интерфейс, созданный в виде социальной сети. Кроме того, функционал сайта будет схожим с Facebook. Об этом сообщило издание VentureBeat со ссылкой на главного ученого Modus Operandi Э. Литтла.

Естественно, публиковать информацию о террористах и обновлять статусы будут не сами преступники. Этим займутся аналитики спецслужб США. Примечательно, что Modus Operandi, клиентами которой являются Сухопутные войска, Корпус морской пехоты и Военно-морской флот США, уже разработала вики-программу, сфокусированную на террористах и используемую Министерством обороны США.

Э. Литтл объяснил, что Modus Operandi решила создать новую базу данных, напоминающую Facebook, в связи с тем, что многие солдаты поступают на службу прямиком из учебного лагеря в возрасте 18–19 лет. Являясь практически подростками, они выросли на социальных сетях.

«Она (база данных. – Ред.) предназначена для отслеживания плохих парней. Если вы находитесь в Кабуле, а я в Лахоре, и у вас есть информация о парне, который был в городе на прошлой неделе и сидел в этом кафе, она автоматически попадает в графу данных», – описал Э. Литтл действующую

вики-программу, использующую тот же интерфейс, что и «Википедия» ***(Эксперты создадут Facebook для террористов // InternetUA (http://internetua.com/eksperti-sozdadut-Facebook-dlya-terroristov). – 2014. – 30.06).***

***

ЦРУ укрепляет сотрудничество с Amazon в сфере облачных технологий, все чаще используя облачную инфраструктуру компании для своей аналитической работы, пишет Financial Times.

В одном из немногих своих публичных выступлений директор по информационным технологиям ЦРУ Д. Вульф рассказал, что сценарий, который развивался в Ираке и Украине, – пример того, насколько агентству необходим доступ к лучшим технологиям для качественного выполнения своей миссии.

Работа ЦРУ с компанией Amazon стала подтверждением безопасности и надежности облачных разработок Amazon Web Services (AWS) – в числе их клиентов есть различные государственные учреждения и частные компании.

О том, что Amazon создаст облачный сервис для ЦРУ за 600 млн дол., стало известно в марте 2013 г. Тогда же руководитель информационной службы ЦРУ Д. Тисингер, выступая перед членами ассоциации технологических компаний Northern Virginia Technology Council, заявила, что ведомство рассматривает возможность сотрудничества с известными производителями программного обеспечения. СМИ тогда сообщали, что разведывательное управление заключило с Amazon контракт на 10 лет на создание облачного сервисД. Вульфа, ЦРУ не хочет ограничиваться только серверами Amazon – ведомство намеревается также воспользоваться программными приложениями, которые предоставляет компания.

Выступая на конференции Amazon в Вашингтоне, Д. Вульф привел в пример приложения Amazon Kinesis и Redshift – которые позволяют обрабатывать и анализировать массовые потоки данных, – как вид программного обеспечения, которое ЦРУ хочет использовать.

Также он отметил, что ЦРУ уже перенесло часть своей работы в облачные технологии Amazon. С. Шмидт, директор по информационным технологиям безопасности AWS, не рассказал о мерах безопасности, которые были разработаны для ЦРУ, но описал общий подход Amazon как «безопасность через сокрытие» ***(ЦРУ укрепляет сотрудничество с Amazon в сфере облачных технологий // ООО «Центр інформаційної безпеки» (http://www.bezpeka.com/ru/news/2014/06/27/Amazon-cia.html). – 2014. – 27.06).***

***

История слежки: Как Facebook отрицал трекинг для кнопки Like

В середине июня текущего года в Facebook объявили о том, что кнопка Like и аналогичные ей инструменты соцсети будут использоваться для

рекламного таргетинга. Издание ProPublica опубликовало хронологию изменений в политике социальной сети по поводу слежки за действиями пользователей.

Отслеживание действий пользователей в социальной сети Facebook напрямую привязано к всем знакомой кнопке Like. Именно она служит основным инструментом для отправки данных о действиях пользователей на сторонних сайтах. Как отмечает ProPublica, всякий раз, когда механизм работы «лайков» переживал новый виток изменений, компании приходилось уверять СМИ и пользователей, что их личные данные не передаются в коммерческих целях третьим лицам и не используются без их ведома на усмотрение Facebook. За четыре года М. Цукерберг и его команда неоднократно меняли точку зрения относительно конфиденциальности действий в социальной сети, и этот процесс до сих пор не завершился.

Вот как появился этот инструмент, и как менялась политика Facebook касательно личных данных в течение последних нескольких лет.

21 апреля 2010 г. – в ходе своей конференции для разработчиков соцсеть Facebook представила кнопку Like. М. Цукерберг со сцены заявил, что этот инструмент станет ключевым для трансформации привычного веб-пространства.

По его словам, цель «лайк-кнопки» – присвоение идентификации ко всем товарам, услугам и предпочтениям, персонализация жизни пользователя в соцсети в тесной связке с реальной жизнью.

30 ноября 2010 г. – голландский аналитик А. Роозендааль опубликовал исследование, согласно которому кнопка Like передает данные от пользователей даже тогда, когда человек не кликает по этой кнопке. В Facebook позже заявили, что А. Роозендааль просто обнаружил баг в системе.

18 мая 2011 г. – издание The Wall Street Journal сообщило, что кнопки и виджеты Facebook собирают данные о пользователях без их ведома. СТО Facebook отвечает, что виджеты и кнопка Like не использовались для отслеживания действий пользователей в Интернете.

24 сентября 2011 г. – блогер с многолетним опытом Д. Вайнер написал, что Facebook «пугает» своим количеством информации, которая автоматически отправляется в соцсеть о прочитанном, увиденном и посещенном в Интернете. По мнению Д. Вайнера, такая ситуация делает соцсеть М. Цукерберга похожей на фишинг, спам и другие виды незаконных действий в Интернете. Блогер рекомендовал пользователям отказаться от использования Facebook и отозвать авторизацию в нем, чтобы избежать несанкционированной слежки. Соцсеть никак не стала комментировать эти заявления.

25 сентября 2011 г. – австралийский блогер Н. Кубрилович заявил, что просто выйти из Facebook недостаточно. По его словам, контроль за пользователями остается даже после выхода из соцсети. В Facebook признали наличие подобной проблемы и заявили, что начали работать над устранением

уязвимости, которая позволяла следить за человеком даже после выхода из соцсети.

27 сентября 2011 г. – в комментарии для издания New York Times представители социальной сети настаивали, что не используют данные, полученные при помощи кнопки Like, для таргетирования рекламы. Также спикер компании заявил, что данные, собранные при помощи кнопок и виджетов Facebook, удаляются либо анонимизируются спустя 90 дней после получения.

1 октября 2011 г. – блогер М. Аррингтон обнародовал патент на приложение Facebook, в основу которого положено отслеживание пользовательской информации авторизированного участника соцсети в тот момент, когда он находится на сторонних сайтах. Публикация об этом была озаглавлена Brutal Dishonesty («Вопиющая нечестность»).

7 декабря 2012 г. – издание Wall Street Journal пишет о том, что данные виджетов и кнопок Like используются для трекинга на 2/3 из 900 изученных сайтов, компания снова опровергает все подозрения. По словам представителей Facebook, данные нужны им исключительно в целях пользовательской безопасности и для контроля возможных ошибок в работе собственного программного обеспечения.

12 июня 2014 г. – спустя почти два года после последних обсуждений и скандалов с возможным несанкционированным использованием личных данных, в Facebook подтверждают, что соцсеть начнет отслеживать действия и предпочтение пользователей в Интернете при помощи кнопок и виджетов Like.

Как отмечает ProPublica, приход к отслеживанию и рекламной конверсии по кнопке Like напрашивался уже давно, и не совсем понятно, почему коллеги М. Цукерберга столько лет упорно отрицали саму возможность подобного. Такие социальные сервисы, как Twitter и Pinterest, давно используют данные о кликах и лайках внутри собственных площадок для таргетирования рекламы. А Google уточнил, что данные, полученные при работе с рекламной сетью DoubleClick, не будут привязаны к личным аккаунтам без явного согласия конкретного пользователя. У Facebook, похоже, будет использоваться аналогичный механизм монетизации лайков, только без возможности его отключения, делает вывод редакция ProPublica. Правда, в соцсети заявляют, что дадут возможность настроить, какие типы рекламных объявлений и продвигаемого контента хотел бы видеть пользователь в своей ленте.

19 июня пресс-служба Facebook прокомментировала свои планы обозревателю ProPublica. По ее словам, трекинг сначала включат только для мобильных устройств, а позже он заработает и в основной версии социальной сети. При этом данные о привычках и вкусах пользователей не станут передавать напрямую рекламодателям, а будут накапливать для настройки таргетирования в интерфейсе рекламодателя, создающего объявление на Facebook ***(История слежки: Как Facebook отрицал трекинг для кнопки***

Like // InternetUA (http://internetua.com/istoriya-slejki--kak-Facebook-otrical-treking-dlya-knopki-Like). – 2014. – 30.06).

***

На прошлой неделе Агентство национальной безопасности США впервые опубликовало отчет о количестве запрошенных для раскрытия данных о телефонных звонках пользователей. Согласно документу, в 2013 г. АНБ интересовала информация только 248 граждан США. Напомним, что согласно документам, рассекреченным бывшим сотрудником спецслужбы Э. Сноуденом, агентство осуществляло массовый сбор данных о коммуникациях американцев.

Согласно отчету, в прошлом году АНБ получило около 2 тыс. ордеров от Суда по делам внешней разведки США (Foreign Intelligence Surveillance Court). 1767 из них касались проводимых расследований, еще 131 ордер разрешал агентству получать телефонные номера с использованием устройств pen register и trap and trace. Раздел 702 Закона о внешней разведке, разрешающий получать данные о пользователях, не являющихся гражданами США, использовался только один раз.

Тем не менее, потенциальных «целей» АНБ (отдельных лиц и целых организаций) в прошлом году было 89 138. В документе сообщается, что в общей сложности за указанный период власти направили 19 212 так называемых «писем национальной безопасности» (административных повесток в суд, которые позволяют ФБР собирать информацию без ордера), содержащих 38 832 запросов на предоставление пользовательской информации ***(АНБ опубликовало первый в своей истории отчет о количестве правительственных запросов // InternetUA (http://internetua.com/anb-opublikovalo-pervii-v-svoei-istorii-otcset-o-kolicsestve-pravitelstvennih-zaprosov). – 2014. – 30.06).***

Проблема захисту даних. DDOS та вірусні атаки

Microsoft и ряд других технологических компаний, в том числе Apple и Cisco, выступают против того, чтобы американское правительство имело право на выдачу ордеров на раскрытие электронной корреспонденции, хранящейся за границей. Соответствующее заявление союзники подали в конце прошлой недели. Ранее подобные документы были поданы Verizon и AT&T.

Фонд Электронных Рубежей (Electronic Frontier Foundation, EFF) также оформил записку по делу советнику в судебном процессе. В документе организация отметила, что ордеры не могут выдаваться для получения доступа к электронным письмам, которые хранятся на сервере в другом государстве.

«Четвертая поправка защищает [пользователей] от необоснованного обыска и изъятия [данных]. Нельзя игнорировать часть “изъятие” только из-за того, что собственность цифровая, а не физическая, – отметил в официальном заявлении юрист EFF Х. Фэкури. – Игнорирование этого основного пункта может иметь опасные последствия».

По его мнению, подобная практика способна привести к необоснованному получению правоохранительными органами доступа и сбору данных, хранящихся по всему миру ***(Техногиганты выступают против выдачи электронных писем, хранящихся за границей // InternetUA (http://internetua.com/tehnogiganti-vistupauat-protiv-vidacsi-elektronnih-pisem--hranyasxihsya-za-granicei). – 2014. – 16.06).***

***

Общее количество регистраций, объем трафика и даже определенные виды активности пользователей в социальных сетях перестают быть столь важным критерием развития, как это было еще несколько лет назад. Крупнейшие ресурсы, к которым относится российская сеть «ВКонтакте», начинают масштабную чистку своих рядов – боты, фейки, дубли и украденные у честных пользователей аккаунты не просто перестали приносить прибыль, но и наносят убытки администрации сервиса.

16 июня в социальной сети «ВКонтакте» было опубликовано сообщение, в котором описывается новая система защиты пользовательских аккаунтов от взлома. Каждый активный пользователь ресурса может лично убедиться в том, насколько часто взламываются аккаунты – для этого достаточно заглянуть в раздел «Спам» в левой нижней части окна диалогов (в браузерной версии). Конечно же, после введения системы восстановления пароля посредством номера мобильного телефона ситуация несколько улучшилась, но говорить о приемлемом уровне безопасности пока рано.

Итак, вот что нам предложил разработчик команды «ВКонтакте» по имени А. Набиуллин – теперь в разделе «Мои настройки», вкладка «Основные», появился пункт «Подтверждение входа», активировав который вы значительно повысите безопасность страницы. Единственное обязательное условие – наличие привязанного номера мобильного телефона, на который будет приходить проверочный код.

Отмечается, что подтверждать вход в аккаунт нужно не каждый раз – можно «запоминать» браузеры устройств, с которыми не работают посторонние. С помощью специального меню можно также «забыть» эти браузеры и тогда процедуру подтверждения входа необходимо будет повторить ***(Как защитить свою страницу Вконтакте от взлома // InternetUA (http://internetua.com/kak-zasxitit-svoua-stranicu-vkontakte-ot-vzloma). – 2014. – 17.06).***

***

За полгода киевлян обворовали через сеть на 9 млн грн. По сравнению с предыдущими годами, говорят в столичной милиции, сумма убытков от так называемых электронных преступлений существенно возросла.

Для примера: за последние четыре года общая сумма убытков составила 30 млн грн.

Чаще всего компьютерные мошенники воруют деньги с банковских карт при помощи скиммеров, а также обманывают доверчивых покупателей, требуя предоплату за товар.

«Столицей» хакеров в нашей стране считается Одесса. Недавно правоохранительным органам удалось раскрыть преступную группу, которая нанесла ущерб примерно на 75 млн евро ***(За полгода киевлян обворовали через сеть на 9 млн грн // InternetUA (http://internetua.com/za-polgoda-kievlyan-obvorovali-cserez-set-na-9-mln-grn). – 2014. – 17.06).***

***

Одна из многочисленных дешёвых копий Samsung Galaxy S4, смартфон Star N9500, продающийся в интернет-магазинах по всему миру по цене 130–165 евро, поставляется с предустановленным трояном Uupay.D. Он позволяет следить за владельцем смартфона, копируя без его ведома личные данные и прослушивая разговоры. Приложение выдаёт себя за Google Play. Удаление трояна весьма проблематично, так как он является частью прошивки смартфона.

Есть подозрения, что не только Star использует продажу персональных данных, полученных через Uupay.D, в качестве средства для снижения цены девайса. Ранее «Лаборатория Касперского» сообщала, что троян замечен на некоторых девайсах Goohi ***(Китайский смартфон Star N9500 имеет предустановленный троян // // InternetUA (http://internetua.com/kitaiskii-smartfon-Star-N9500-imeet-predustanovlennii-troyan). – 2014. – 17.06).***

***

Недавно известный репортёр и специалист по кибербезопасности Б. Кребс сообщил о масштабной утечке из национальной сети китайских забегаловок P. F. Chang’s в США: по его оценке, тысячи кредитных карт были выставлены на продажу на чёрном рынке.

TJournal разобрался, откуда берутся краденые карточки в Интернете, как злоумышленники получают к ним доступ и что нужно сделать, чтобы максимально обезопасить себя от потери денег.

Минутка истории: как хакеры заставили P. F. Chang’s перейти на дореволюционные технологии

9 июня на сайте подпольного магазина rescator[dot]so появилась свежая партия краденых карт, рассказал в своём блоге Б. Кребс. Связавшись с несколькими банками, начавшими реагировать на утечку данных, он выяснил, что все карты, которые удалось проверить, использовались в сети

китайских бистро P. F. Chang’s в промежуток между началом марта 2014 г. и 19 мая.

Спустя двое суток представители P. F. Chang’s подтвердили кражу карт, вызванную кибератакой на рестораны сети. Компания начала расследование произошедшего, а пока что вместо привычных электронных терминалов P. F. Chang’s будет использовать старые считыватели кредитных карт, работающих на дайлап-интернете, а также сохранять бумажные чеки от платежей по картам.

Как именно это повысит безопасность, компания не сообщила, однако ясно, что удалённо украсть (а затем перепродать) большой объём бумажных чеков гораздо сложнее, чем взломать тысячи карт через одно современное устройство.

В начале марта стало известно о краже данных 282 тыс. банковских карт, которыми расплачивались в сети салонов красоты Sally Beauty. Когда компанию спросили о произошедшем, её представители сообщили, что хотя проникновение в сеть компании было зафиксировано, ни сотрудники безопасности Sally Beauty, ни сторонние эксперты не смогли найти следов кражи данных.

Чтобы опредилить точку, в которой и было проведено преступление, банки производят «контрольную закупку» карт – обычно несколько десятков штук. Проверяя их по своей базе, они вычисляют так называемый CPP, common point of purchase – магазин, в котором расплачивались всеми картами из партии.

Однако мастшаб этой операции не идёт ни в какое сравнение со взломом сети супермаркетов Target, произошедшей в ноябре 2013 г. Тогда были украдены данные 110 млн покупателей, которые позднее появились на сайте уже упомянутого магазина, rescator[dot]so. По некоторым данным, 70 млн из карт были взломаны при помощи вируса Kaptoxa, созданного российским подростком, однако в разговоре с TJournal он опровергал своё участие.

Несмотря на существующую угрозу безопасности остальных своих клиентов, Target не отказался от использования электронных систем обработки платежей с кредиток: в масштабе гигантской сети супермаркетов это было бы равносильно переводу всех грузовиков с товарами на лошадиные повозки.

Кратко об устройстве бизнеса кражи данных карт

Мошенничество с угоном данных карт называется кардингом. Иногда злоумышленники ограничиваются несколькими частными кражами, но серьёзную угрозу представляют масштабные спланированные операции, в результате которых оказываются скомпрометированными не десятки и сотни, а тысячи и миллионы пластиковых карт. Такие партии пластика тяжело воспроизвести в виде копий и опасно обналичивать, поэтому добывшие их взломщики сбывают их другим преступникам, по пути выручая крупную сумму денег.

Существуют сотни подпольных интернет-магазинов, продающих карты. Один из самых известных – McDumpals (да, магазин косит под сеть фастфудов, играя на ассоциации со скоростью обслуживания), о котором недавно рассказывал Б. Кребс. Стремясь обеспечить собственную безопасность, магазин пускает не всех, а только по вступительному взносу в 100 дол. Как и остальные платежи, вступительный взнос можно заплатить только в биткоинах.

Например, магазин McDumpals продаёт 1245 карт за 10,5 тыс. дол.

Несмотря на то что большинство дамп-шопов используют множественных поставщиков краденых карт, они не занимаются повторной перепродажей данных. После того как карту продают покупателю, она исчезает из магазина, и если кто-то попробует перепродать её повторно, он будет удалён из цепочки и внесён в чёрный список.

Иногда магазины продают карты пачками свыше тысячи штук. Всё, что покупатель знает об этих картах – место, откуда они происходят, и их «свежесть»: чем свежее, тем больше вероятность, что карты окажутся рабочими (а не будут сломаны, потеряны или перевыпущены).

Главная характеристика продаваемых партий – процент валидности. Например, если продавец заявляет, что этот показатель поставляет 50 %, это означает, что каждая вторая карта из партии не сработает в банкомате и полностью бесполезна. Чем свежее карта, тем меньше шанс, что банки уже успели отреагировать на кражу партии их карт и заблокировать их.

Карты, украденные в ходе атаки на Target, продавались несколькими последовательными партиями, каждая из которых постепенно дешевела из-за падающего процента валидности.

Сохранившийся высокий процент валидных карт – вина и самих банков, не пожелавших перевыпускать карты: по словам Б. Кребса, выпуск одной карты стоит от 3 до 5 дол., а взлом ещё и неудачно выпал на время рожденственских праздников, когда все клиенты активно пользуются кредитками и не готовы ждать, пока их перевыпустят.

Первые партии, имевшие максимальный рейтинг, продавались частями по миллиону штук от 20 до 100 дол. за карту, рассказывал Б. Кребс, однако впоследствии цена упала вплоть до 8 дол. Высокие цены на краденые карты были связаны также и с тем, что rescator[dot]so продавал так называемые дампы – данные с магнитных полос, позволяющие воспроизводить копии кредиток.

Как используют украденные карты

Дампы – это данные, которые при помощи вредоносного кода, встроенного в скиммеры в банкоматах и мобильных терминалах оплаты, извлекаются из непосредственно магнитной полосы. Получив эти данные, кардеры могут создать реплику оригинальной карты, чтобы использовать её для покупок в больших супермаркетах.

В обычном же случае покупатель имеет только данные, годящиеся для покупок в Интернете. Хотя сегодня в сети можно купить всё что угодно, от

пиццы до оружия и наркотиков, использовать краденые кредитки для крупных покупок в Интернете не так удобно, как превратить всю сумму в наличные в удобном тебе банкомате. По крайней мере, бумажные деньги отследить гораздо сложнее.

Кардеры предпочитают покупать карточки, прежние владельцы которых жили неподалёку или в том же городе. Это связано с системой безопасности: если банк видит, что при помощи карты некто пытается совершить платёж из места, откуда владелец ранее не производил покупок, он помечает операцию как подозрительную. Тогда в дело вмешивается служба безопасности: обычно транзакция блокируется до тех пор, пока владелец лично её не подтвердит.

Как крадут карты и как защитить себя

Поскольку от одного номера карты и кода подтвержения (CVV или CVC2) толку мало, кардеры стараются получить дампы, для чего нужен физический доступ к карте. Получить его они могут двумя путями: установив скиммер в банкомат или взломав мобильный терминал, при помощи которого карты принимают к оплате, например, в ресторанах и барах. Если в последнем случае хакерам потребуется сотрудничество сообщника в лице официанта или кассира, то в случае скиммера всё проще и распространённее.

Скиммер (от «skim» – снимать сливки) – специальное считывающее устройство, работающее прослойкой между картой и банкоматом. Оно присоединяется к лотку приёма карт в банкомате и пропускает карты сквозь себя, считывая с них информацию специальной головкой. Иногда считыватель дополняет мобильная камера, записывающая PIN, вводимый пользователем на клавиатуре, или специальная накладная клавиатура, запоминающая введённую последовательность.

Один из примеров внешнего вида скиммеров

Скиммер и камеру обычно маскируют под цвета банкомата, на который их устанавливают, или даже под рекламные материалы, чтобы возникало ещё меньше подозрений. Они работают от батареек, но чаще всего не передают информацию по сети: злоумышленнику предстоит снять их с банкомата и подключить к компьютеру, чтобы заполучить собранные данные.

Обычно скиммеры выглядят чужеродно и слегка выпирают над поверхностью корпуса банкомата, однако их можно спутать с антискимминговыми устройствами. Есть и более незаметные варианты – шиммеры – которые представляют собой считывающую полоску толщиной 0,1-0,2 миллиметра, устанавливаемой внутрь отверстия для приёма карты.

Инкассаторы каждый раз проверяют банкоматы на наличие скимминговых устройств, поэтому обычно их стараются помещать на устройства в людных местах – там, где за короткое время между двумя инкассациями удастся считать наибольшее количество карт: например, на вокзалах и в торговых центрах. Банки тоже не сидят на месте: устанавливают специальные антискиммеры, усложняющие насадку и использование считывателей.

Антискиммер

Приведём несколько советов по тому, как снизить риск угона пластиковой карты.

1. Пользоваться проверенными банкоматами вашего банка в офисе банка – там, где он охраняется и за его безопасностью следит несколько камер.

2. Внимательно осматривать банкомат перед тем, как воспользоваться им. Если внешний вид устройства для приёма карт вызывает подозрения (например, он выпирает, не зафиксирован, другого цвета или материала), клавиатура выглядит непривычно, а рядом находится лоток с рекламными материалами, куда может быть встроена камера, лучше не пользоваться банкоматом.

3. При наборе PIN лучше прикрывать клавиатуру рукой сверху, страхуясь от возможных камер или подсматривающего злоумышленника. Некоторые банкоматы оснащены специальными шторками.

4. По возможности выпускать не обычную карту, а смарт-карту с электронным чипом. Её обслуживание обходится дороже, но безопасность выше: её сложнее подделать, а для всех операций необходимо введение PIN-кода (в отличие от обычных карт, где может хватить росписи владельца). Однако не все банкоматы поддерживают использование чипов: в этом случае они проходят через магнитную полосу.

5. Банальный, но действенно: не показывайте свою карту посторонним. Подсмотреть вводимый PIN может улыбающийся официант.

В случае, если вы всё-таки воспользовались подозрительным банкоматом, и теперь вас мучают сомнения, не нарвались ли вы на скиммер, позвоните в банк и заблокируйте карту, а затем перевыпустите с новыми данными. Несмотря на то что некоторые мошенники могут мгновенно получить данные вашей карты в случае беспроводного подключения к скиммеру (один из читателей «Хабрахабра» описывал такой случай), массовые взломы обычно осуществляются много позже. Оперативным перевыпуском карты можно избежать потери денег ***(Разбор полётов: Как крадут наши карты // InternetUA (http://internetua.com/razbor-pol-tov--kak-kradut-nashi-karti). – 2014. – 17.06).***

***

Технологии DRM – угроза для компьютерной безопасности

«Цифровое управление авторскими правами» (или попросту системы защиты от копирования) формально призвано защищать интеллектуальную собственность. Однако на деле оно не только не выполняет своей непосредственной функции, но и делает наши компьютеры уязвимыми для злоумышленников. Как и почему это происходит?

Прежде всего системы DRM сами по себе могут быть небезопасными: некорректные варианты реализации защиты от копирования могут открывать дыры в системе безопасности компьютераы, которые в случае отсутствия DRM были бы закрыты. Дело в том, что для блокирования обычных функций

копирования в операционных системах программные пакеты управления правами требуют самых широких прав доступа к системным файлам и фактически перехватывают управление такими функциями.

Типичный пример опасной реализации DRM – появившаяся в 2005 г. система защиты от копирования CD-аудио компании Sony BMG. Этот руткит в своё время был размещён на огромном числе компакт-дисков одного из ведущих музыкальных лейблов мира. При загрузке такого диска в компьютерный дисковод автоматически запускалась установка специальной программы XCP для Windows, которая была призвана воспрепятствовать копированию всего альбома или «граблению» отдельных треков с этого диска.

Руткит XCP проникал глубоко внутрь операционной системы, причём он устанавливался без какого-либо участия пользователя, а деинсталлировать обычными способами его было невозможно. Более того, в процессе работы он отнимал заметную часть вычислительных ресурсов и мог служить причиной сбоев. И, наконец, об этом рутките и о том, как он работает, ни слова не говорилось в пользовательском соглашении (EULA); не будем здесь о том, что их всё равно никто не читает.

Но самое главное – руткит XCP создавал явную угрозу для безопасности всей системы. В частности, после его установки все файлы, начинающиеся с sys, становились скрытыми, чем не преминули воспользоваться вирусописатели. К примеру, «троянский конь» Breplibot, рассылавшийся во вложениях к электронным письмам, можно было обнаружить только с помощью антивирусных программ и сканеров, а для пользователя потенциально опасные файлы были просто не видны.

К сожалению, этот пример не единственный. Совсем недавно, в 2012 г., разразился громкий скандал вокруг игрового программного обеспечения Ubisoft uPlay: для доступа к сетевым сервисам нужно было установить специальный плагин для браузера, который мог открыть злоумышленникам полный удалённый доступ к системе.

Определённым образом составленный Java-скрипт, размещённый на веб-странице, мог автоматически запустить uPlay, что, в свою очередь, позволяло беспрепятственно загрузить на компьютер жертвы практически любую программу. Ссылки на такие страницы могли рассылаться в том числе и в виде спама по электронной почте. К чести Ubisoft, она быстро выпустила патч и исправленную версию uPlay, однако осадок от того, что даже такие крупные компании позволяют себе распространять столь неряшливо написанный код, всё-таки остался.

Между тем далеко не всегда удаётся установить опасные недостатки систем DRM. Более того, такая работа с лёгкостью может быть признана незаконной! Например, действующий в США «Закон об авторском праве в цифровое тысячелетие» (DMCA) напрямую запрещает обход систем ограничения доступа. Существует несколько исключений из этого правила, в том числе касающихся случаев изучения проблем безопасности, но в

широком смысле все попытки обхода систем защиты могут быть признаны незаконными.

Подобные законы и подход к проблеме сам по себе провоцирует многочисленные угрозы безопасности, ведь чтобы не подпасть под действие санкций, специалисты вынуждены не афишировать работы по изучению присутствующих на рынке систем DRM и сохранять в тайне от общества выявленные ими уязвимости.

Именно это в своё время произошло при обнаружении опасных свойств руткита Sony BMG: после того как сведения о них просочились в прессу, многие исследователи систем безопасности заявили, что им уже давно было известно об уязвимости в XCP, но они просто боялись обнародовать эти сведения, опасаясь преследований со стороны государства.

По результатам опроса Sophos, 98 % бизнес-пользователей считают систему DRM Sony BMD угрозой, и лишь 2 % – допустимым средством борьбы с пиратством. Между тем, согласно букве DMCA, даже деинсталляция руткита XCP может быть признана незаконной – ведь это в прямом смысле способ обхода системы DRM.

Любые системы DRM применительно к персональным компьютерам ограничивают ваши возможности управления собственным ПК. Если перед вами обычная машина на Windows или OS X, то вы можете делать на ней всё что угодно – при наличии соответствующих навыков и программного обеспечения. А это значит, что вы имеете возможность нарушать авторские права самыми разными способами – от записи потокового видео и копирования CD до скачивания и распространения торрент-файлов с новинками киноиндустрии.

Соглашаясь на ограничения, мы настолько доверяем разработчикам софта или владельцам авторских прав, что передаём им часть возможностей по управлению нашими собственными компьютерами. Именно поэтому, например, для установки многих брандмауэров, диспетчеров аккаунтов или трекинговых приложений на Android требуется получить права «рута», поскольку такие программы не могут работать в условиях установленных производителем ограничений для пользователя.

Современные компьютеры, смартфоны и планшеты становятся всё более закрытыми для пользователя: сегодня, не прибегая к различным ухищрениям, мы не можем устанавливать программы, полученные не из официального магазина производителя, не можем смотреть видеоконтент, предназначенный не для нашей страны, не можем обмениваться файлами между нашими же собственными устройствами.

Что же напоминает такая ситуация? Совершенно верно: машину, заражённую вирусом, шпионской программой, которая, не спрашивая нашего разрешения, меняет настройки, мешает выполнять привычные и естественные операции и в конце концов полностью выводит компьютер из подчинения владельца. То есть DRM – это тот же самый вирус, только

распространяемый на совершенно законных основаниях и защищаемый тем же самым законом.

Давно пора признать, что технологии DRM не только не препятствуют незаконному копированию и распространению интеллектуальной собственности, но и создают серьёзные проблемы с безопасностью компьютерных систем. Ситуацию усугубляет законодательство, препятствующее поиску уязвимостей в таких технологиях и вынуждающее скрывать результаты таких исследований. Может быть, хотя бы наши законодатели, обожающие запрещать всё, что попадает в их поле зрения, подадут наконец пример всему миру и запретят что-то действительно вредное и опасное? ***(Технологии DRM – угроза для компьютерной безопасности // InternetUA (http://internetua.com/tehnologii-DRM---ugroza-dlya-kompuaternoi-bezopasnosti). – 2014. – 18.06).***

***

Национальное агентство по борьбе с преступностью Великобритании (National Crime Agency, NCA) сообщило, что тысячи компьютеров все еще заражены вариантами Gameover Zeus (Gozeus) и Cryptolocker, несмотря на то, что пользователи, чьи системы были частью ботнета, должны были удалить вредоносное ПО.

Отметим, что 2 июня нынешнего года NCA сообщило о том, что ему удалось ослабить глобальную ботсеть, и предоставило общественности возможность в течение двух недель очистить свои системы от вредоносов. С тех пор агентство напоминает британским пользователям о том, что их компьютеры все еще уязвимы к Gozeus и Cryptolocker, и необходимо избавляться от вредоносного ПО.

«Существуют факты, доказывающие, что с 2 июня нынешнего года количество компьютеров, зараженных Gozeus и Cryptolocker, сократилось, однако тысячи систем все еще остаются инфицированными или подвергаются риску заражения», – сообщает NCA ***(Тысячи компьютеров все еще подвержены риску заражения Gozeus и Cryptolocker // InternetUA (http://internetua.com/tisyacsi-kompuaterov-vse-esxe-podverjeni-risku-zarajeniya-Gozeus-i-Cryptolocker). – 2014. – 18.06).***

***

Национальная комиссия, осуществляющая государственное регулирование в сфере связи и информатизации, заявляет о зафиксированных Министерством обороны нарушениях в части безопасности данных в сетях у входящих в тройку крупнейших мобильных операторов компаний «Киевстар», «МТС-Украина» и «Астелит». Об этом на заседании комиссии во вторник, 17 июня, сообщил журналистам председатель НКРСИ А. Семенченко, передают «Українські новини».

«Угрозы безопасности сети были зафиксированы не только у компании МТС, но также у компаний «Астелит» и «Киевстар». Об этом идет речь в

письме Министерства обороны, текстом которого располагает комиссия», – заявил А. Семенченко.

Он также уточнил, что на сегодняшний день отсутствует регламентированная на международном уровне система защиты от вмешательства извне в сети операторов, а также отметил отсутствие регламентированных систем защиты от подобного вмешательства.

А. Семенченко также уточнил, что комплекс защиты от вмешательства извне должен вмещать четкий план организационно-технических мероприятий, что на сегодняшний день также не реализовано ***(Представители Минобороны зафиксировали нарушения безопасности данных в сетях «Киевстара», МТС и life:) // InternetUA (http://internetua.com/predstaviteli-minoboroni-zafiksirovali-narusheniya-bezopasnosti-dannih-v-setyah--kievstara---mts-i-life). – 2014. – 18.06).***

***

Турецкая хакерская группа «Акынджылар» (налетчики, Cyber-Warrior Akincilar) взломала сайт министра европейских и международных дел Австрии С. Курца в знак протеста против высказанной им критики в адрес главы турецкого правительства Т. Эрдогана.

Хакеры разместили на первой странице сайта изображения османского герба и портретов султана Сулеймана Великолепного и Т. Эрдогана, оставив под изображениями подпись на турецком, английском и немецком языках. «Малыш, ты кто такой? Не тебе решать, что будет говорить наш премьер-министр. Эрдоган – внук тех предков, которые дошли до Вены, до земель, на которых вы сейчас живете. Мы Налетчики, мы Османы, мы Турция», – заявили представители «Акынджылар».

Причиной атаки стало предупреждение от С. Курца Т. Эрдогану, планирующему в июне визит в Австрию. В соответствии с публикациями в австрийской прессе, министра обеспокоило выступление главы турецкого правительства в Германии, в котором Т. Эрдоган призвал турецкую диаспору интегрироваться, но не ассимилироваться. «Я прямо предупредил Эрдогана о том, что он не может провоцировать раскол в австрийском обществе. Интеграция – это сложный процесс. Некорректная речь премьера может отбросить нас назад и повредить общественному климату», – заявил С. Курц в интервью одному из австрийских таблоидов. Эти слова и стали причиной недовольства хакеров, заявивших, что «ни одна страна не вправе диктовать или учить турецких руководителей, что и как говорить». «Они в Европе с ее растущим расизмом и ущемлением прав турецких граждан не хотят, чтобы мы высказывались», – утверждают хакеры из «Акынджылар».

В Европе, особенно в Германии, Австрии и некоторых странах северной Европы проживает несколько миллионов турок, составляющих уже существенную часть электората. Одновременно турки не стремятся полностью ассимилироваться в странах проживания, поддерживая крепкие

контакты с родиной – что также влияет на денежные потоки, значительная часть которых уходит в Турцию.

«Акынджылар» с 2001 г. пропагандирует и защищает исламские ценности и нормы морали. «Кибер-воины» взломали большое количество сайтов антитурецкой и антиисламской направленности, причем значительная часть атак направлена на зарубежные ресурсы. При этом «Акынджылар» не устраивают взломы государственных и официальных интернет-страниц Турции, считая их суверенной территорией республики, которую необходимо защищать. Этот принцип привел ранее к серьезным разногласиям между «Акынджылар» и другой крупной турецкой хакерской группой «РедХак» – данная левацкая марксистская группа настроена против нынешнего руководства Турции, в особенности Т. Эрдогана и его партии. «Красные хакеры» взламывают правительственные ресурсы, устраивая DDoS-атаки, заменяя содержимое главных страниц сайтов, либо крадут с официальных серверов закрытую информацию, которую впоследствии частично обнародуют ***(Турецкие хакеры атаковали сайт австрийского министра // InternetUA (http://internetua.com/tureckie-hakeri-atakovali-sait-avstriiskogo-ministra). – 2014. – 17.06).***

***

Часть наиболее посещаемых интернет-ресурсов, которые шифруют данные при помощи SSL-протоколов, все еще уязвимы к атакам с эксплуатацией бреши в OpenSSL 16-летней давности. Согласно данным И. Ристика из Qualys, количество таких сайтов составляет порядка 49 % всех веб-страниц. Кроме того, он утверждает, что на 14 % ресурсов уязвимость можно успешно проэксплуатировать.

Напомним, что впервые о бреши стало известно в начале июня текущего года. Тогда сообщалось, что брешь позволяет настроить параметры рукопожатия таким образом, чтобы для связи между клиентом и сервером OpenSSL SSL/TLS использовались слабые ключи шифрования. Благодаря этому злоумышленник мог осуществить атаку «человек посередине».

Несмотря на то что практически все версии OpenSSL уязвимы, эксплуатация бреши возможна исключительно в двух случаях, пишет Ристик. Так, для проведения атаки нужно, чтобы обе стороны использовали OpenSSL, или чтобы сервер поддерживал работу уязвимой версии OpenSSL ветки 1.0.1.

«Хорошая новость заключается в том, что большинство браузеров не задействуют OpenSSL, а это означает, что большая часть пользователей затронута не будет. Однако Android-обозреватели используют OpenSSL и являются уязвимыми к таким атакам», – пишет в блоге эксперт ***(49 % всех web-ресурсов все еще уязвимы к атакам с эксплуатацией бреши в OpenSSL 16-летней давности // InternetUA (http://internetua.com/49--vseh-web-resursov-vse-esxe-uyazvimi-k-atakam-s-ekspluataciei-breshi-v-OpenSSL-16-letnei-davnosti). – 2014. – 17.06).***

***

Как сообщили порталу SecurityLab представители компании Zecurion, в понедельник, 16 июня, пользователи популярного сервиса Evernote стали жертвами хакерской атаки. Злоумышленникам удалось получить доступ к таким персональным данным, как хэши паролей (это касается только пользователей, создавших пароли до 2011 г.), имена, даты рождения и адреса электронной почты.

В Evernote утверждают, что пароли пользователей не хранятся на серверах форума, поэтому их можно не менять. Однако если они также используются для входа в учетные записи на других сайтах, пароли рекомендуется сменить. Кроме того, сеть, в которой размещен сервис, не была затронута, и заметки пользователей, а также их переписка находятся в безопасности.

Отметим, что в этом месяце Evernote подверглась кибератаке уже во второй раз. Так, 11 июня компания сообщала, что стала жертвой DDoS-атаки. Кроме того, в начале нынешнего года сервис был взломан группой хакеров, которым удалось заполучить данные его пользователей. Тогда Evernote в принудительном порядке сменила пароли.

Количество пользователей, ставших жертвами атаки, пока не раскрывается. Также неизвестны причины взлома ***(Пользователи сервиса Evernote стали жертвами хакерской атаки // InternetUA (http://internetua.com/polzovateli-servisa-Evernote-stali-jertvami-hakerskoi-ataki). – 2014. – 17.06).***

***

Несмотря на то что деятельность ботнета GameOver Zeus и программы-вымогателя CryptoLocker фактически прекращена, 8 июня «Лаборатория Касперского» обнаружила троян Svpeng, атакующий мобильные устройства. В настоящее время он наиболее распространен в США и Великобритании. Svpeng функционирует в качестве финансового вредоносного ПО со функциональными способностями программы-вымогателя. Вредоносное ПО Svpeng, которое является известным в России трояном и похищает деньги с мобильных устройств, впервые обратило на себя внимание других площадок.

Trojan проверяет мобильное устройство на наличие финансовых приложений, предположительно, чтобы в будущем получить логин и пароль банковского счета пользователя. Таким образом вредоносное ПО функционирует в России. Английская версия сканирует мобильное устройство на наличие таких приложений как USAA Mobile, Citi Mobile, Amex Mobile, Wells Fargo Mobile, Bank of America Mobile Banking и других. После заражения устройства оно блокируется якобы уведомлением от ФБР, согласно которому необходимо оплатить штраф в размере 200 дол. через Green Dot

В настоящее время 91 % атак осуществляются при помощи этого трояна в США и Великобритании, остальные 9 % – в Индии, Германии и Швейцарии ***(Новый троян Svpeng функционирует в США и Великобритании // InternetUA (http://internetua.com/novii-troyan-Svpeng-funkcioniruet-v-ssha-i-velikobritanii). – 2014. – 18.06).***

***

Эксперты компьютерной безопасности из Marble Security утверждают, что мобильная платформа iOS подвержена угрозам не меньше, чем Android. Когда речь заходит о безопасности, ни одну из мобильных операционных систем нельзя назвать более защищенной, заявляют специалисты компании.

Marble Security признают, что установить вредоносное программное обеспечение на Android-устройства легче, однако и в iOS эта брешь есть, даже когда речь идет о телефонах без джейлбрейка. Еще один аспект, который приводит к повышенной уязвимости Android, – значительная фрагментация операционной системы. В Marble Security исследовали 11 800 устройств и пришли к выводу, что на них установлены «мириады версий» ОС от Google.

«В то время как Android-пользователи имеют больше возможностей установить программы не из официального магазина приложений, iOS-пользователям также доступны такие возможности», – цитирует Onliner исследователей Marble Security.

Атаки на обеих платформах отличаются незначительно, поскольку атакующие нашли способ публиковать вредоносные приложения, либо атаковать мобильных пользователей через SMS или точи доступа Wi-Fi как на iOS, так и на Android. Особой разницы между iPhone или iPad с джейлбрейком и Android-гаджета с root-доступом с точки зрения безопасности нет.

Угрозы, впрочем, на платформах различаются. К примеру, новые iOS-угрозы, такие как содержащие уязвимость конфигурационные профили, незашифрованные вложения в электронную почту и возможность похищение бэкапов, открывают хакерам возможности для эффективной атаки.

В Marble Security уверены, что заинтересованные лица без труда найдут способ получить доступ к данным вне зависимости от платформы, поэтому назвать iOS более безопасной, чем Android, нельзя ***(Мобильные платформы iOS и Android одинаково уязвимы // InternetUA (http://internetua.com/mobilnie-platformi-iOS-i-Android-odinakovo-uyazvimi). – 2014. – 19.06).***

***

Согласно данным, предоставленным FireEye и Google, некоторые пользователи Android-устройств стали жертвой очередной вредоносной кампании, развернутой в сети. В частности, речь идет о появлении приложения, выдававшего себя за Google Play.

Известно, что за последний месяц жертвами вредоносного ПО стали как минимум 200 человек. При этом, преимущественно, программа атакует корейских пользователей. Обнаружить вирус практически невозможно – только 3 из 51 антивирусного решения были способны найти на системе жертвы ложный Google Play с интерфейсом на корейском языке, уверяют в FireEye.

Иконка приложения выглядит почти так же, как и у Google Play, а располагается она на главной странице мобильного устройства. Благодаря этому повышаются шансы того, что пользователи будут заходить именно во вредоносное приложение, а не работать с подлинным клиентом. Активируется программа после первого клика, затем она похищает текстовые сообщения жертвы, сертификаты подписи, а также пароли, используемые для online-банкинга.

Стоит отметить, что внимание экспертов по ИБ привлекла одна из функций приложения. Согласно результатам проведенного исследования, опция Google App Stoy, якобы предназначенная для удаления программы, не удаляет его. Это означает, что вредоносное ПО запускается при каждом включении или перезагрузке системы ***(Приложение, выдающее себя за Google Play, похищает пароли online-банкинга // InternetUA (http://internetua.com/prilojenie--vidauasxee-sebya-za-Google-Play--pohisxaet-paroli-online-bankinga). – 2014. – 20.06).***

***

В сети зафиксирована активность очередного троянского вируса, предназначенного для рассылки спам-писем. Отличительной чертой вредоноса, по утверждениям ИБ-экспертов компании «Доктор Веб», является функционал антивируса.

Дело в том, что троянец, идентифицируемый как Trojan.Tofsee, сканирует систему жертвы на наличие других вредоносных программ. В случае их обнаружения вирус их удаляет.

Для распространения вируса злоумышленники используют Skype, различные социальные сети, а также съемные накопители. Здесь задействуется метод социальной инженерии – киберпреступники сообщают жертве о том, что в сети якобы опубликованы шокирующие фотографии или видеозаписи с ее участием.

Для выполнения вышеописанных действий вредоносу необходимо скачать специальный модуль. Последний отправляется с подконтрольного злоумышленникам сервера. «Отправляемые сообщения строятся по шаблону, который передается в конфигурационном файле. Сообщения пользователям социальных сетей отсылаются с учетом используемого ими национального языка», – сообщили в компании.

В сообщениях содержится ссылка, пройдя по которой пользователь якобы сможет просмотреть компрометирующие его/ее файлы. Правда, для

этого требуется также установить плагин для браузера – под его видом распространяется Trojan.Tofsee.

«Для отправки сообщений на сайты Twitter, Facebook и «ВКонтакте» вредоносный модуль использует данные сессии из файлов cookies браузеров Microsoft Internet Explorer, Mozilla Firefox, Opera, Safari, Google Chrome. В программу Skype сообщения отсылаются с помощью нажатия кнопок в окне самого приложения. Модуль также умеет распознавать защиту captcha на сайте социальной сети Facebook – для этого она отправляется на сервер, где распознается, после чего троянец получает текст для ввода в соответствующую экранную форму», – добавили ИБ-эксперты ***(Новый троянец выполняет роль антивируса // InternetUA (http://internetua.com/novii-troyanec-vipolnyaet-rol-antivirusa). – 2014. – 20.06).***

***

Пользователи из Австрии выразили недовольство тем, что Европа и США занимаются обменом личных данных пользователей Facebook.

Europe-v-Facebook, австрийская группа, представляющая некоторых пользователей Facebook, подала жалобу уполномоченному по защите персональных данных в Ирландии (Data Protection Commissioner, DPC) по поводу защиты пользовательских персональных данных в социальной сети. В ней утверждалось, что когда Facebook собирает пользовательские данные и экспортирует их в США, администрация сайта предоставляет Агентству национальной безопасности США (АНБ) возможность использовать их для массовой слежки за пользователями без достаточного основания. Как результат, Facebook нарушает европейские законы.

Тем не менее, DPC отказался расследовать жалобу Europe-v-Facebook, утверждая, что не было никаких оснований для расследования, поскольку передача данных пользователей Facebook покрывается соглашением между ЕС и США под названием Safe Harbour.

Не удовлетворенная ответом команда энтузиастов обратилась в Высокий суд Ирландии для рассмотрения дела. Однако дело было передано в суд Европейского союза (CJEU). Комиссия заявила, что персональные данные, переданные третьей стране, например, США, считаются защищенными надлежащим образом, если компании, которые их обрабатывают, придерживаются принципов соглашения Safe Harbour ***(Споры о безопасности личных данных в Facebook продолжаются // InternetUA (http://internetua.com/spori-o-bezopasnosti-licsnih-dannih-v-Facebook-prodoljauatsya). – 2014. – 20.06).***

***

Сайты знакомств match.com, PlentyOfFish, eHarmony, Christian Mingle, Chemistry.com, SeniorPeopleMeet, Zoosk, Lavalife и некоторые другие подверглись фишинговым атакам. Как сообщает Netcraft, мошенники

используют схемы, благодаря которым они воруют логины и пароли пользователей, зарегистрированных на сайтах знакомств.

Предположительно, кража данных пользователей совершается с помощью построения фиктивных отношений на расстоянии. Преступники крадут данные уже предоплаченных аккаунтов, что, чаще всего, позволяет им отправлять сообщениям реальным пользователям.

Мошенники втираются в доверие к жертве, общаются с ней на протяжении достаточно длительного времени. Затем они начинают просить пользователя переслать им деньги. Просьбу об отправке денег мошенники мотивируют такими причинами, как оплата медицинского лечения близкого человека или члена семьи, оплата расходов на путешествие и другое. В некоторых случаях преступники даже начинают шантажировать своих жертв. Например, грозятся переслать родственникам жертвы ее фотографии или видео интимного характера, которые ранее были получены мошенниками.

Один из многих случаев интернет-мошенничества на сайтах знакомств был зафиксирован в 2012 г. в США. Мать и дочь сумели получить посредством мошенничества более 1 млн дол. от 374 жертв, которые проживали в 40 странах. Мать и дочь претворялись человеком, получившим огромное наследство от друга-военнослужащего в Нигерии. Этот пользователь предлагал предоставить средства в долг за небольшой аванс. Жертвы так и не получали обещанных мошенницами средств. В 2013 г. суд в штате Колорадо приговорил мать и дочь к 12 и 15 годам тюремного заключения соответственно. Прокурор штата прокомментировал вердикт, заявив, что дуэт мошенниц не только нарушал закон, но и «разбивал сердца по всему миру» ***(Мошенники совершают фишинговые атаки на сайты знакомств // InternetUA (http://internetua.com/moshenniki-sovershauat-fishingovie-ataki-na-saiti-znakomstv). – 2014. – 20.06).***

***

Недавно в сети была зафиксирована новая вредоносная кампания с использованием вируса Zbot. В рамках компании распространялись уведомления для клиентов компании Berkeley Futures Limited. Имя предприятия настоящее, но сообщения ложные. В письме был прикреплен файл с расширением.zip, защищенный паролем. Пароль к файлу был указан в теле письма.

Это должно было стать предупреждающим знаком для пользователей сети. Файл расшифровывался после введения пароля. Так как файл защищен был паролем, антивирусные программы не могли просканировать его на наличие вредоносов.

Прикрепленный файл включает в себя еще два. Один из них с расширением .scr, другой – .pdf. Изначально файл отображается с расширением .zip, но на самом деле он имеет расширение .rar. Это можно обьяснить тем, что вирусописатели хотели обойти сканирование

антивирусной программой, так как вредоносное ПО с расширением .rar встречается намного реже.

Исполняемый файл с расширением .scr является трояном и обращается к российскому IP-адресу 62.76.43.110 и загружает файл «1.exe» размером 220 Кб, который имеет значок компании Amazon. Обнаруженный файл является вредоносным ПО Zbot, которое после запуска пытается соединиться с другим российским IP-адресом. Однако соединение установить не удается. Напомним, что основной целью вредоноса Zbot является похищение финансовых средств ***(В Сети зафиксирована вредоносная кампания с ипользованием Zbot // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/06/19/Zbot.html). – 2014. – 19.06).***

***

Компания Code Spaces, являющаяся хостинг-провайдером Subversion и Git и использующаяся организациями для управления и развития проектов, вынуждена прекратить свою деятельность из-за вредоносной активности хакера, получившего доступ к панели управления Amazon EC2.

Все началось с того, что 17 июня Code Spaces стала жертвой DDoS-атаки со стороны неизвестного злоумышленника, требующего за ее прекращение огромное вознаграждение. Это не первый случай в текущем месяце, когда на компанию совершается подобное нападение с целью получения выкупа.

Так, 10 июня атаке подверглись Evernote и Feedly. Тем не менее, в отличие от этих инцидентов, хакер, стоящий за атакой на Code Spaces, помимо прочего получил доступ к панели управления Amazon EC2, благодаря чему захватил полный контроль над всеми данными, хранящимися в Elastic Block Store (EBS) и облачном сервисе Amazon S3.

Code Spaces предприняла попытку вернуть себе контроль над панелью управления, изменив пароль. Тем не менее, злоумышленник был готов к этому и заранее открыл несколько окон входа. Видя, что администратор пытается вернуть контроль, он начинал в произвольном порядке удалять с панели артефакты. После того как компании, все-таки, удалось вырвать панель из рук хакера, он удалил все фотографии из EBS, бакеты в S3, все AMI и пр. Таким образом, большинство данных, резервных копий и конфигураций были частично или полностью удалены.

Для Code Spaces это означает невозможность продолжать работу, так как стоимость решения проблемы и предполагаемые затраты на возмещение убытков клиентам, которые остались без обслуживания, разрушительно скажутся как на финансовом состоянии компании, так и на ее репутации.

«Таким образом на данный момент нам ничего не остается, кроме как прекратить работу и сосредоточиться на помощи нашим пострадавшим клиентам вернуть сохранившиеся данные», – говорится на сайте Code Spaces ***(Неизвестный хакер уничтожил хостинг-провайдера Code Spaces //***

InternetUA (http://internetua.com/neizvestnii-haker-unicstojil-hosting-provaidera-Code-Spaces). – 2014. – 19.06).

***

В LinkedIn утверждают, что новый способ шифрования Secure Sockets Layer (SSL), который используется веб-сайтом, не влияет на безопасность личной информации пользователей.

Ранее эксперты компании Zimperium сообщали, что LinkedIn подвергла сотни миллионов своих пользователей возможной опасности по причине проведения злоумышленниками атаки «человек посередине» (Man-in-the-Middle) из-за способа использования веб-сайтом шифрования Secure Sockets Layer (SSL) в сети. Представители Zimperium заявляли о ситуации в LinkedIn шесть раз в течение прошлого года. Ответ от LinkedIn поступил только дважды.

Пресс-секретарь социальной сети Н. Леверич выступила от имени компании, заявив, что LinkedIn считает своим долгом обеспечивать безопасность своих пользователей. В декабре 2013 г. поисковик начал переход на протокол HTTPS и только на прошлой неделе объявил, что теперь все шифрование для пользователей в США и ЕС будет основываться на HTTPS-соединении. Данный способ шифрования Secure Sockets Layer (SSL) не влияет на безопасность подавляющего большинства пользователей LinkedIn, утверждает Леверич.

М. Шема, директор по инжинирингу компании Qualys заявил, что многие подобные сайты одинаково уязвимы, не говоря уже о всех тех веб-ресурсах, которые даже не беспокоятся об использовании HTTPS ***(LinkedIn ответил на критику со стороны Zimperium // InternetUA (http://internetua.com/LinkedIn-otvetil-na-kritiku-so-storoni-Zimperium). – 2014. – 22.06).***

***

Более 95 % всех инцидентов в сфере информационной безопасности вызвано человеческим фактором – такие данные предоставили аналитики службы безопасности IBM Managed Security Services.

Проанализировав инциденты, которые случились в компьютерных сетях почти 1 тыс. клиентов компании в 133 странах, специалисты установили, что огромное число инцидентов начинается с человеческой ошибки.

Наиболее популярный просчёт со стороны человека – переход на вредоносный сайт по ссылке в фишинговом сообщении.

Часто проблемы у пользователей возникают из-за неправильной конфигурации сервера, игнорирования вышедшего обновления системы, использования имени пользователя и пароля по умолчанию, потери ноутбука или другого устройства.

Аналитики отмечают, что большинство крупных организаций с числом сотрудников от 1 до 5 тыс. человек многократно сталкиваются с угрозами безопасности в течение года.

Среднее количество «событий» для каждой також компании за год превышает 91 млн, а среднее количество атак за год на крупные компании достигает 16 865.

Центр стратегических и международных исследований установил, что общий ущерб от хакерских атак достигает 400 млрд дол. в год. Половина всего ущерба от киберпреступности приходится всего на три страны: США, Китай и Германию ***(Почти 100 % проблем с кибербезопасностью провоцирует сам пользователь // InternetUA (http://internetua.com/pocsti-100--problem-s-kiberbezopasnostua-provociruet-sam-polzovatel). – 2014. – 21.06).***

***

Специалисты ESET зафиксировали распространение нескольких новых вариантов вымогательского ПО.

Наибольшее количество пользователей, пострадавших от вымогательского ПО Simplocker, находятся на территории России (48 %) и Украины (42 %). Такие данные предоставили ИБ-эксперты компании ESET, проанализировавшие информацию, полученную через LiveGrid.

Специалисты также говорят о том, что им удалось обнаружить несколько новых вариантов вируса. К примеру, в одном из случаев вредоносная программа содержит загрузчик программ-троянов. Последние, в свою очередь, скачивают ряд вредоносного ПО на зараженную систему. Подобный подход можно назвать типичным для Windows, однако в сфере Android это является неким нововведением.

Один из таких загрузчиков, например, предлагает пользователю качать фальшивое приложение для просмотра видео. Подобная практика является весьма удобной для злоумышленников, поскольку она позволяет уменьшить риск обнаружения вируса. Дело в том, что в таких случаях приложение просто открывает URL-адрес вне программы. Это действие не обозначается как вредоносное, поэтому загрузчик и не воспринимается как «плохой».

Проанализировав один из обнаруженных образцов, эксперты установили, что URL-адрес, содержащийся в приложении, не вел напрямую к Simplocker APK. Так, троян загружался после отправки соответствующей команды с подконтрольного злоумышленникам сервера.

Отметим, что речь идет о загрузчике, выдающем себя за подлинное приложение под названием USSDDualWidget ***(Наиболее активно Simplocker атаковал украинцев и россиян // InternetUA (http://internetua.com/naibolee-aktivno-Simplocker-atakoval-ukraincev-i-rossiyan). – 2014. – 23.06).***

***

В чипах Baseboard Management Controller (BMC) от Supermicro обнаружена уязвимость, которая предоставила злоумышленникам полный доступ к интерфейсу 32 тыс. серверов.

По информации ИБ-экспертов из CARInet, брешь присутствует в чипах линейки WPCM450, встроенных в материнские платы. Специалисты также говорят, что в платах Supermicro содержится бинарный файл, который хранит пароли для получения к серверам удаленного доступа. При этом данные никоим образом не зашифрованные, и их можно скачать посредством подключения к порту 49152.

Отметим, что BMC является центральной частью микроконтроллера, который располагается на серверной материнской плате или в блоке лезвийного сервера. BMC соединяется с главным процессором и другими элементами посредством обычной последовательной шины.

Для компрометации уязвимых серверов злоумышленнику необходимо подключиться к порту 49 152 и выполнить команду GET /PSBlock, после чего пароли будут доступны в открытом виде, без хэширования.

По информации специалистов из CARInet, всего в Сети есть 31 964 серверов, которые могут быть скомпрометированы. Они также подчеркивают, что в 10 % случаях на серверах использовались заданные по умолчанию пароли ***(Уязвимость в BMC раскрыла пароли 32 тысяч серверов // InternetUA (http://internetua.com/uyazvimost-v-BMC-raskrila-paroli-32-tisyacs-serverov). – 2014. – 23.06).***

***

Компания ESET предупреждает о появлении нового трояна Dyre, атакующего клиентов крупных коммерческих банков.

Вредоносная программа Dyre используется злоумышленниками для кражи аутентификационных данных пользователей банковских приложений. Анализ показал, что троян нацелен на интернет-банкинг CitiGroup, Bank of America, NatWest, RBS и Ulster Bank.

Dyre внедряет вредоносный код в браузер и перехватывает данные, когда жертва открывает сайт своего онлайн-банка. Троян совместим с Chrome, Firefox и Internet Explorer и может маскироваться под загрузку проигрывателя Flash Player. Зловред способен обойти SSL-шифрование и двухфакторную аутентификацию в системах интернет-банкинга.

ESET полагает, что Dyre распространяется по схеме crime-as-a-service («преступление как услуга» – в некотором смысле аналог SaaS): то есть, злоумышленники продают вредоносное ПО, оказывают услуги по его настройке и реализации кибератак.

Жертвы обычно получают вредоносный код в спам-письмах, предлагающих загрузить с того или иного файлообменного сервиса архив, якобы содержащий счета или информацию от налоговой службы. Главная опасность Dyre заключается в том, что трояну зачастую удаётся убедить

пользователя в том, что он подключается к своему банку через безопасное соединение, защищённое SSL-шифрованием. Это позволяет вредоносной программе перехватить конфиденциальную информацию и отправить её злоумышленникам ***(Новый банковский троян работает по «принципу SaaS» // InternetUA (http://internetua.com/novii-bankovskii-troyan-rabotaet-po--principu-SaaS). – 2014. – 24.06).***

***

Британские полицейские предупреждают пользователей компьютеров об участившихся случаях мошенничества, в результате которого пользователи теряли важную информацию вроде паролей для учётных записей и банковских данных, и другие ценные сведения.

Метод, которым воспользовались мошенники, оказался до неприличия прост и оригинален: они звонили на телефон потенциальной жертвы и представлялись сотрудниками компании Microsoft. Если человек, поднявший трубку, оказывался пользователем операционной системы Windows, то далее все действия выполнялись по одной и той же отработанной схеме. Якобы сотрудник Microsoft уведомлял пользователя об обнаружении на его компьютере вредоносного программного обеспечения или о какой-то критической ошибке, которую необходимо устранить в срочном порядке.

Жертва, не подозревая подвоха, предоставляла удалённый доступ к своей файловой системе согласно озвученным в телефонном разговоре инструкциям, надеясь избавиться от опасного вируса. Ну а как только мошенники получали доступ в чужую систему без необходимости совершать хакерские операции, они быстро находили ключи, пароли и прочие данные для доступа к финансовым счетам.

Иногда наглость мошенников выливалась в просьбу о материальном вознаграждении за оказанную «диагностику» и «удаление» троянцев из операционной системы.

С учётом того факта, что среди британских пользователей компьютерами есть люди достаточно преклонного возраста, которые никогда не слышали о подобного рода аферах, полиция выступила с заявлением. В нём она убедительно просила не предоставлять дистанционный доступ к своему ПК незнакомым лицам и напомнила о необходимых мерах предосторожности при подобных звонках от лже-сотрудников известных компаний. В списке превентивных мер оказалось прекращение разговора с аферистами и уведомление полиции о случившемся во избежание повторных инцидентов ***(Мошенники получали удалённый доступ к чужим системам, притворяясь сотрудниками Microsoft // InternetUA (http://internetua.com/moshenniki-polucsali-udal-nnii-dostup-k-csujim-sistemam--pritvoryayas-sotrudnikami-Microsoft). – 2014. – 24.06).***

***

Хакери використовують опубліковані торік проекти шпигунських пристроїв Агентства національної безпеки США, щоб їх відтворити. Про це пише mashable.com.

Окрім потужних технологій інтернет-стеження, АНБ створює різноманітні шпигунські пристрої, за допомогою яких можна зламувати комп'ютери чи мобільні телефони.

Деякі з таких засобів стали відомі після того, як торік Der Spiegel опублікував 48-сторінковий каталог, створений 2008 р. Агентством національної безпеки і який потім потрапив у розпорядження німецького журналу. Нині група хакерів намагається сконструювати ці пристрої АНБ, використовуючи компоненти, що є у відкритому доступі.

Група, що назвала свій проект NSA Playset, хоче показати іншим хакерам та майстрам, як створити шпигунські механізми та як від них захиститися.

«Для когось, хто не є експертом у цій галузі, потенційні можливості цього каталогу здадуться неправдоподібними або високотехнологічними, – каже один із хакерів проекту М. Османн. – Ми хочемо показати, що ці можливості є дуже досяжними та практичними. Показуючи, наскільки вони прості, ми сподіваємося підвищити обізнаність щодо питань безпеки комп'ютерних систем».

Ідея роботи над цим проектом належить досліднику питань безпеки Д. Пірсу, який хотів побачити, наскільки легко створити ці пристрої. М. Османн та інші приєдналися до ініціативи трохи пізніше. Через деякий час хакери зрозуміли, що більшість пристроїв з каталогу АНБ нескладно відтворити ***(Хакери створюють шпигунське обладнання за опублікованими у медіа проектами АНБ // Громадська організація «Телекритика» (http://osvita.mediasapiens.ua/material/31958). – 2014. – 24.06).***

***

Количество вредоносного ПО для пользователей смартфонов и планшетов под управлением ОС Google Android растет.

Популярность мобильной платформы Google Android продолжает расти, так же, как и разновидности программ-вымогателей, которые усложняют жизнь ее пользователям.

Первой угрозой стал троян-шифровальщик Android.Locker.2.origin. Вредоносное ПО заражало устройства, которые работали на базе ОС Android. Инфицировав систему, троян обнаруживает хранящиеся на сменных картах смартфона или планшета файлы с расширениями .jpeg, .jpg, .png, .bmp, .gif, .pdf, .doc, .docx, .txt, .avi, .mkv, .3gp. Далее он шифрует их, добавляя к каждому из них расширение .enc. После этого экран мобильного устройства жертвы блокируется до тех пор, пока владалец не заплатить выкуп за разблокировку.

Целью энкодера Android.Locker.5.origin является хищение и передача на сервер злоумышленников различной информации об инфицированном устройстве. Интересно, что троян Android.Locker.2.origin ориентирован на пользователей из Китая. Эксперты считают, что он был разработан, скорее, ради шутки, поскольку никакого особого вреда устройству не причиняет, а лишь блокирует доступ к нему на 24 часа, оставив владельцу уведомление о том, что подвергшийся блокировке телефон «немного отдохнет».

В этом месяце к предыдущей разработке присоединились новые ее версии Android.Locker.6.origin Android.Locker.7.origin. Эти трояны уже направлены на американских пользователей. Вредоносное ПО выдает себя за Adobe Flash Player и в ходе загрузки на мобильное устройство жертвы требует передать приложению права администратора. После этого трояны создают видимость сканирования устройства и блокирует экран, уведомляя жертву об обнаружении якобы незаконного контента. Разблокировка гаджета обойдется жертве в 200 дол. ***(Ассортимент блокировщиков и энкодеров под Android расширяется // InternetUA (http://internetua.com/assortiment-blokirovsxikov-i-enkoderov-pod-Android-rasshiryaetsya). – 2014. – 24.06).***

***

Злоумышленники осуществляют атаку DNS flood attack, достигающую 110 Гб/с.

Веб-сайт крупного представителя индустрии видео-игр стал жертвой масштабной DDoS-атаки. Об этом сообщил портал The Hacker News со ссылкой на электронное письмо от пресс-секретаря ИБ-компании Incapsula.

Атака началась в субботу, 21 июня, и в пиковые моменты достигала 110 Гб/с (90 млн пакетов в секунду). Для ее осуществления злоумышленники использовали ботнет из скомпрометированных систем. При этом большинство IP-адресов принадлежало пользователям в Индии и Китае.

По словам экспертов из Incapsula, злоумышленники использовали тип DDoS-атак под названием DNS flood attack, который сильно отличается от ранее популярного DNS amplification attack и является более мощным. Различие между этими двумя типами DDoS-атак заключается в методах осуществления и наносимом ущербе.

DNS amplification attack является ассиметричной атакой, в ходе которой злоумышленник устанавливает адрес источника запросов, используя поддельный IP-адрес жертвы. Это означает, что жертва получает ответы от всех используемых DNS-серверов.

DNS flood attacks является симметричной атакой, в ходе которой злоумышленник отправляет тысячи быстрых действительных DNS-запросов к целевому серверу, тем самым давая серверу больше трафика, чем он может обработать. В результате время ответа на легитимные запросы постепенно увеличивается ***(Злоумышленники используют тип более мощных DDoS-атак // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-tip-bolee-mosxnih-DDoS-atak). – 2014. – 25.06).***

***

Депутаты ЛДПР внесли в Госдуму законопроект, обязывающий российские и иностранные компании, осуществляющие обработку персональных данных граждан России, хранить эти данные в дата-центрах на территории Российской Федерации

В Госдуму внесен законопроект, согласно которому любые персональные данные россиян, включая данные из учетных записей в социальных сетях и электронной почты, с сентября 2016 г. должны будут храниться на серверах, размещенных на территории РФ. Текст законопроекта опубликован на сайте Госдумы.

Авторами законопроекта являются депутаты ЛДПР А. Луговой и В. Деньгин. Проект направлен председателю Госдумы С. Нарышкину.

Депутаты предлагают внести поправки в два федеральных закона: «О персональных данных» от 27 июля 2006 г. и «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.

В закон «О персональных данных», в частности, предлагается внести пункт со следующим содержанием: «При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, в базах данных информации, расположенных на территории Российской Федерации».

Также предлагается заставить операторов персональных данных сообщать уполномоченным органам по защите прав субъектов персональных данных о том, где именно находятся персональные данные граждан, и ограничить доступ к информации, обрабатываемой с нарушением законодательства РФ.

В свою очередь, в закон «Об информации, информационных технологиях и о защите информации» предлагается внести нововведения, которые позволят создавать реестры компаний, нарушающих права субъектов персональных данных.

Текст поправки выглядит следующим образом: «В целях ограничения доступа к информации в сети Интернет, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, создается автоматизированная информационная система “Реестр нарушителей прав субъектов персональных даннях”».

В этот реестр предлагается включать доменные имена, указатели страниц сайтов и сетевые адреса, содержащие информацию, обрабатываемую с нарушением законодательства РФ в области персональных данных. Также в реестре предлагается вести учет судебных постановлений относительно каждого ресурса и информацию об устранении нарушений.

«В настоящее время персональные данные россиян хранятся в основной массе за границей, – пояснил один из авторов законопроекта

В. Деньгин. – Такой информацией оперируют поисковики, она хранится на серверах. Наш закон направлен на то, чтобы такая информация не могла попасть в руки мошенников».

При этом депутат говорит, что крупным компаниям предлагаемых поправок опасаться не стоит. Например, «Яндекс», по его словам, уже строит свой дата-центр на территории одного из регионов в России, считает он. Деньгин добавил, что планируемые изменения заставят такие иностранные компании, как Facebook и Twitter, открыть представительства на территории РФ ***(Россия заставит интернет-гигантов хранить данные россиян внутри страны // InternetUA (http://internetua.com/rossiya-zastavit-internet-gigantov-hranit-dannie-rossiyan-vnutri-strani). – 2014. – 25.06).***

***

Представители компании Symantec зафиксировали спам-кампанию, нацеленную на пользователей электронных карт. Интересно, что спам-сообщение просто перенаправляет пользователя на сайт с предложением быстро разбогатеть.

Электронные письма этой кампании достаточно базовые. Сообщения отправляются с поддельного электронного адреса 123greetings.com, и содержат одну фразу и ссылку. Как оказалось, письма рассылаются с IP адреса Amazon.com. Эксперты предполагают, что, скорее всего – это попытка обмануть любого, кто читает заголовок. Тем не менее, IP-адрес на самом деле не относится к доменному имени, связанному с Amazon.

В теле писем, спамеры используют короткие ссылки для перенаправления жертв на свой сайт. Как правило, 123greetings не использует сокращения для обслуживания электронных карт клиентов. Вместо этого, сайт использует URL, который содержит соответствующее имя домена. Согласно записям на WhoIs, домен спамеров был зарегистрирован 17 июня в Панаме.

Фальшивая ссылка перенаправляет пользователей на разные веб-страницы несколько раз, которые запрашивают у пользователя контактные данные, прежде чем перенаправить его на сайт с предложением быстро разбогатеть. Злоумышленник связывается с жертвой путем SMS-сообщений или дополнительных писем в попытке убедить пользователя зарегистрироваться и заплатить для участия в розыгрыше денег. Также мошенник может использовать полученные контактные данные для отправки спама ***(Пользователям электронных карт рассылают спам с предложением быстро разбогатеть // InternetUA (http://internetua.com/polzovatelyam-elektronnih-kart-rassilauat-spam-s-predlojeniem-bistro-razbogatet). – 2014. – 25.06).***

***

«Лаборатория Касперского» (ЛК) обнаружила новые мобильные трояны для iOS и Android, входящие в состав платформы для слежки за

пользователями Remote Control Systems (RCS) от компании HackingTeam. Об этом на конференции Going Underground в Лондоне рассказали специалисты ЛК.

Вредоносные модули являются частью платформы RSC, также известной как Galileo. Компания HackingTeam продает лицензии на ПО Galileo государственным, в том числе, правоохранительным, органам.

По данным «Лаборатории Касперского», среди возможных пользователей платформы – структуры в 21 стране, включая Мексику, Польшу, Турцию, Италию, ОАЭ, Египет, Азербайджан, Узбекистан, Казахстан и др.

Вновь выявленные программы-трояны особенно активно заражают смартфоны iPhone, а среди жертв много журналистов, политиков и общественных активистов.

«Журналисты на удивление часто становятся объектами слежки. Примерно 21 из 25 новостных организаций являются целью государственных программ слежения», – сказал Морган Марки-Бур из исследовательской лаборатории Citizen Lab, участвовашей в расследовании.

Выявленные трояны могут передавать данные о местоположении жертвы, делать фотоснимки, копировать данные из календаря и информацию о новых sim-картах, а также перехватывать вызовы и сообщения из VIber, WhatsApp и Skype.

Операторы платформы создают индивидуальный вредоносный модуль для жертвы, на чье мобильное устройство он доставляется либо через уязвимость нулевого дня, либо во время синхронизации с компьютером по USB.

Особенно успешно у мобильного трояна Galileo удавалось заражать смартфоны iPhone, которые подверглись процедуре перепрошивки исходного программного обеспечения, установленного изготовителем. Кроме того, даже смартфоны Apple заводской сборки могут быть заражены через подключение к инфицированному компьютеру.

О существовании мобильных троянов для Android и iOS среди инструментов итальянского разработчика HackingTeam было известно и ранее. Однако до настоящего времени эксперты не могли их идентифицировать или заметить во время атак.

Шпионские функции начинают работать только после совершения некоторых действий – например, подключения к определенной сети, подзарядки аккумулятора или смены SIM-карты.

«Лаборатории Касперского» также удалось выявить местонахождение более 320 серверов, управляющих инфраструктурой Galileo, в более чем 40 странах. Большинство серверов размещается в США, Казахстане, Эквадоре, Великобритании и Канаде.

«Наличие серверов инфраструктуры RCS в той или иной стране еще не свидетельствует о том, что местные спецслужбы причастны к использованию Galileo. Однако организации, которые работают с RCS, должны быть

заинтересованы в том, чтобы их сервера располагались в местах, где у них был бы полный контроль над ними», – заявил С. Голованов, ведущий антивирусный эксперт «Лаборатории Касперского».

Ранее организация «Репортеры без границ» включила HackingTeam в число организаций – «врагов Интернета», помогающих властям контролировать сеть. В этот список, в том числе, входят компании Gamma, Trovicor, Amesys и Blue Coat, разработавшие специализированное ПО для слежки за интернет-пользователями ***(Выявлены новые шпионские программы для слежки за iPhone // InternetUA (http://internetua.com/viyavleni-novie-shpionskie-programmi-dlya-slejki-za-iPhone). – 2014. – 25.06).***

***

Російський сайт gazeta.ru був заблокований на території Росії та інших країн у результаті хакерської атаки.

Як повідомляє gazeta.ru, за попередньою версією, хакерська атака здійснювалася за допомогою анонімної мережі Tor.

Деякий час інтернет-користувачі, заходячи на сайт, бачили повідомлення Роскомнагляду. У ньому йшлося про те, що мережева адреса сайту занесена до так званого «Чорного списку» – Реєстру сайтів, що містять заклики до масових заворушень, здійснення екстремістської діяльності, участі в масових (публічних) заходах, що проводяться з порушенням встановленого порядку.

«Ми виявили, що сайт не відкривається і кинулися телефонувати в Роскомнагляд. Вони нам сказали, що нас не закривали. Генпрокуратура нам теж нічого не присилала і нас не закривала. Це хакерська атака. Зараз будемо обговорювати, як відбивати її», – розповіла виданню izvestia.ru головний редактор gazeta.ru С. Бабаєва.

У Роскомнагляді та Генпрокуратурі РФ заявили, що жодне з цих відомств не блокувало доступу до сайту ***(Російський сайт gazeta.ru атакували хакери // Громадська організація «Телекритика» (http://osvita.mediasapiens.ua/material/32049). – 2014. – 26.06).***

***

Исследователи из Duo Security сообщили об уязвимости, позволяющей обойти двухфакторную аутентификацию в PayPal. Более того, по их словам, брешь в системе Security Key существует уже несколько лет.

Уязвимыми являются мобильные приложения для iOS и Android, сообщающие об ошибке при входе пользователя в учетную запись, где активирована двухфакторная аутентификация. Эксперты обнаружили, что они могут манипулировать ответом сервера и создать видимость того, что данная функция в целевой учетной записи отключена. «Уязвимость напрямую связана с ошибкой аутентификации в веб-сервисе PayPal API

(api.paypal.com), который используется в официальных мобильных приложениях PayPal и некоторых сторонних компаний», – сообщил исследователь из Duo Security З. Ланье.

Как сообщает издание Forbes, уязвимость впервые была обнаружена Д. Солтманом из EverydayCarry, который сообщил он ней PayPal 29 марта текущего года в рамках программы по выплате вознаграждений за найденные бреши. Однако он не получил ответа от компании, поэтому обратился к исследователям из Duo Security, которые разработали концепт эксплоита. Эксперты создали скрипт, использующий API для доступа к учетным записям в PayPal и перевода средств с любого компьютера.

Стоит отметить, что PayPal заявила о намерении выпустить исправление уязвимости 28 июня нынешнего года ***(Двухфакторную аутентификацию в PayPal можно с легкостью обойти // InternetUA (http://internetua.com/dvuhfaktornuua-autentifikaciua-v-PayPal-mojno-s-legkostua-oboiti). – 2014. – 27.06).***

***

В первый день конференции разработчиков Google I/O 2014 было анонсировано множество продуктов, о которых написали многие технологические издания. В стороне остались вопросы безопасности, которые коснулись представители интернет-корпорации.

Выступая на мероприятии в Сан-Франциско, руководитель по разработке Android и Chrome OS в Google С. Пичаи сообщил, что менее 0,5 % пользователей Android хотя бы один раз сталкивались с вирусами в своих гаджетах. На первый взгляд эта цифра кажется небольшой, однако в мировом масштабе проблема достаточно велика.

По данным Google, свыше одного миллиарда человек пользуются Android-устройствами ежемесячно. Это значит, что 5 млн активных пользователей становились жертвами вредоносных программ. В это число не входят жители Китая и обладатели планшетов Kindle, в которых установлена модифицированная версия мобильной «операционки» от Google.

По данным F-Secure, около 97 % мобильных вирусных угроз, имевших место в 2013 г., предназначалось для Android-устройств, тогда как годом ранее показатель оценивался в 79 % (в 2011 г. – 66,7 %, в 2010 г. – 11,25 %).

С. Пичаи сообщил, что Google планирует обновлять систему безопасности Android каждые шесть недель, выпуская патчи в рамках обновлений для платформы Google Play Services ***(С вирусами сталкиваются 5 млн пользователей Android // InternetUA (http://internetua.com/s-virusami-stalkivauatsya-5-mln-polzovatelei-Android). – 2014. – 27.06).***

***

Новая версия Pony Loader, пресловутого семейства вредоносных программ, используемых для распространения трояна P2P Gameover Zeus,

получила новые возможности. Встроенные изменения позволяют вредоносному ПО заниматься хищением крипто-валюты.

Отметим, что предыдущая версия версия 1.9 в прошлом была опубликована в сети, благодаря чему любой желающий мог загрузить и использовать ее для кражи конфиденциальной информации, а также распространить дополнительные вредоносные программы на компьютере жертвы.

Тем не менее, исследователи из компании Damballa утверждали, что обнаружили факт продажи нового Pony Loader version 2. Эта версия содержит тот же список паролей, полученных от «нескольких взломов баз данных», как и его предыдущая версия 1.9, а это позволяет злоумышленникам еще легче проникнуть в учетную запись жертвы, сообщает специалист компании И. Палмер (Isaac Palmer).

В своем блоге И. Палмер утверждает, что новая версия может похитить средства с крипто-валютных кошельков следующих платформ: Electrum, MultiBit, Litecoin, Namecoin, Terracoin, Bitcoin Armory, PPCoin (Peercoin), Primecoin, Feathercoin, NovaCoin, Freicoin, Devcoin, Frankocoin, ProtoShares, MegaCoin, Quarkcoin, Worldcoin, Infinitecoin, Ixcoin, Anoncoin, BBQcoin, Digitalcoin, Mincoin, Goldcoin, Yacoin, Zetacoin, Fastcoin, I0coin, Tagcoin, Bytecoin, Florincoin, Phoenixcoin, Luckycoin, Craftcoin, Junkcoin и Bitcoin client.

Представители Bitcoin, тем временем, посоветовали установить более новую версию системы электронной валюты, которая защищена шифрованием с использованием фразы-пароля, хранящейся в кошельке.

Популярность платформ по обмену электронной валютой продолжает расти так же, как и число их конкурентов. Именно по этой причине Bitcoin и другие крипто-валютные кошельки становятся лучшей мишенью для киберпреступников ***(Новая версия Pony Loader совершает хищения с Bitcoin // InternetUA (http://internetua.com/novaya-versiya-Pony-Loader-sovershaet-hisxeniya-s-Bitcoin). – 2014. – 27.06).***

***

В Україні з’явилася ініціативна група, мета якої – привертання уваги до проблем кібербезпеки. До групи увійшли профільні фахівці з питань ІТ-технологій, громадські діячі та журналісти. На сьогодні група існує як спільнота в соціальній мережі Facebook. Низка подій останніх місяців продемонстрували неготовність державних структур протистояти кіберзлочинцям. Хакерська атака на ЦВК мало не зірвала президентські вибори в Україні.

А впливове видання The Financial Times написало про поширення російських вірусів, які є просунутими інструментами шпигунства або навіть дистанційного керування ІТ-системами.

Активну діяльність продовжує співтовариство «КіберБеркут», яке відкрито заявляє про свою протиправну діяльність, що полягає в цифровому вандалізмі.

У зв'язку з цими подіями ряд активістів, серед яких О. Ольшанський – президент Mirohost, О. Пилипенко – головний редактор видання PCWeek, О. Сич – керівник проекту Zilly, І. Головацький – фахівець з кібербезпеки, створили ініціативну групу, завдання якої привернути увагу громадськості до проблем уразливості українського інформаційного простору.

На думку О. Ольшанського, президента холдингу Internet Invest Group, «держава повинна приділяти набагато більше уваги напряму інформаційної безпеки. Активна інформатизація систем державного управління та «цифровізація» українського суспільства веде до все більших ризиків кібернападів.

Але тут треба розуміти, що держава може взяти в союзники лише громадян і приватний бізнес, оскільки всі компетенції знаходяться в приватних компаніях. Тому вихід лежить у пошуку справжнього порозуміння держави з бізнесом.

Без цього будь-які інвестиції у безпеку будуть абсолютно марними. Крім того, основними «робочими» органами у боротьбі мають стати саме приватні компанії. А СБУ і МВС скоріше повинні виконувати роль деяких координуючих органів».

В Україні надто довго не звертали увагу і відмахувалися від прихованих загроз. Однак деякі кроки в напрямі захисту інформаційного та кіберпростору все ж були зроблені: введення в дію рішення РНБО про інформаційну безпеку країни, активізація публічної діяльності CERT-UA, локальні затримання хакерів, які виконували DDoS-атаки на сайти держорганів.

Експерти вважають, що цих зусиль недостатньо, тому що паралельно з військовими діями традиційним способом ворог веде приховану кібервійну. Цей вид агресії здатний спровокувати порушення в управлінні державою, обурення в суспільстві з подальшою ескалацією насильства та інші негативні наслідки ***(В уанеті з'явилась Кібероборона, яка захищатиме від хакерських атак // InternetUA (http://internetua.com/v-uanet--z-yavilas-k-beroborona--yaka-zahisxatime-v-d-hakerskih-atak). – 2014. – 28.06).***

***

Уязвимость просуществовала столь длительный период времени в связи с традицией повторного использования кода.

В алгоритмах распаковки Lempel-Ziv-Oberhumer (LZO) и LZ4 исправлена уязвимость двадцатилетней давности. Брешь способна стать причиной повреждения областей памяти при распаковке специально оформленных сжатых данных. Согласно данным исследователей из Mouse Security, проблема вызвана целочисленным переполнением, проявляющимся при обработке Literal Run.

«Literal Run – это просто способ обнаружения и интерпретации бинарного кода. Атакуя этот функционал, злоумышленник может использовать данные для контролирования уязвимого приложения непредусмотренным способом, – подчеркивает глава компании Д. Бейли. – В результате, [злоумышленник] может удаленно скомпрометировать систему или повысить привилегии».

Уязвимость просуществовала столь длительный период времени в связи с традицией повторного использования кода. Именно поэтому брешь затрагивает весьма широкий круг продуктов: от открытых библиотек до мобильных устройств. Согласно утверждениям специалистов Mouse Security, уязвимость почти всегда можно проэксплуатировать удаленно.

По данным ИБ-экспертов, эксплуатация уязвимости позволяет осуществить DoS-атаку. Помимо прочего, брешь способна повредить структуры, которые влияют на процесс выполнения кода. Правда, это касается только случаев задействования LZO в многопоточных программах.

В связи с особенностями работы алгоритма LZ4 становится возможной атака с изменением указателя по заданному смещению. Кроме того, злоумышленник может внести изменения в часть структур, которые влияют на выполнение кода.

Наличие бреши ставит под угрозу такие программные продукты, как Linux, Juniper Junos, MPlayer2, Libav, FFmpeg, OpenVPN, а также встраиваемые платформы и устройства. Кроме того, сжатие при помощи LZO задействуется в таких файловых системах, как btrfs, squashfs, jffs2 и ubifs. LZ4, в свою очередь, используется в ZFS.

Обновления безопасности исправляют брешь в Linux 3.15.2, 3.14.9, 3.4.95 и 3.10.45. На текущий момент разрабатывается апдейт для дистрибутивов ***(В LZO и LZ4 нашли уязвимость 20-летней давности // InternetUA (http://internetua.com/v-LZO-i-LZ4-nashli-uyazvimost-20-letnei-davnosti). – 2014. – 28.06).***

***

Злоумышленники рассылают электронные письма, содержащие вирусы, от имени антивирусных вендоров. Об этом сообщили в компании «Доктор Веб». В письмах содержатся некие инструкции по противодействию вредоносным программам. Но под видом инструкции в прикреплённом файле содержится скрипт, загружающий на компьютер троян семейства BAT.encoder.

Компания «Доктор Веб» сообщила, что никогда не рассылала и не планирует рассылать подобные письма. Представители компании призывают ни в коем случае не открывать такое письмо, если вы его получили, и не запускать вложенные файлы.

Текст фальшивого письма от имени «Доктор Веб» выглядит следующим образом:

«В антивирусную лабораторию Dr.Web поступает множество жалоб от жертв вирусов-шифровальщиков. Наша аналитическая система установила, что на Ваш электронный адрес не так давно было выслано письмо, содержащее одну из подобных вредоносных программ. Если Вы пострадали от рук злоумышленников-шифровальщиков, изучите простые действия, которые помогут Вам избежать подобного в будущем. Мы подготовили простую инструкцию (во вложении), выполнение которой обезопасит Вас от многих уязвимостей, а также тестовый лицензионный ключ.

С уважением, Команда Dr.Web.»

Также появились сообщения и о рассылке фальшивых писем от имени компании Amazon. Эти письма сообщают о якобы поступившем заказе. Пользователю предлагают ознакомиться с детализацией покупки и счетом-фактурой. Сообщение написано на английском языке, его текст одинаков во всех известных случаях, различаются только дата и номер заказа. К письму приложен ZIP-архив, в котором также содержится файл вируса – BackDoor.Tishop.122.

Аналитики Check Point обратили внимание на то, что в 2013 г. широко распространилось более «умное» вредоносное ПО: 33 % организаций загружали как минимум один файл, зараженный неизвестным ПО, за период с июня по декабрь 2013 г. Более трети (35 %) таких файлов имели формат PDF. Новые инструменты, получившие название «криптеры», дали возможность создателям вирусов обойти системы противодействия вредоносному ПО ***(Хакеры рассылают трояны от имени антивирусной компании // InternetUA (http://internetua.com/hakeri-rassilauat-troyani-ot-imeni-antivirusnoi-kompanii). – 2014. – 29.06).***

***

Как сообщил порталу SecurityLab анонимный источник, в пятницу, 27 июня, пользователи Facebook стали жертвами ClickJacking-атаки. Атака заключалась в следующем: когда пользователи просматривали ролики на венгерском сайте heretacsko.hu, при нажатии кнопки воспроизведения видео от их лица в Facebook автоматически ставился лайк, а в учетную запись устанавливалось приложение app_240196472844332.

Особенностью этой программы является возможность публикации от имени жертвы. Отметим, что атака срабатывает автоматически, если пользователь авторизован в Facebook. В противном случае выводится окно авторизации.

Рекомендуется пользователям, авторизованным в соцсети, которые просматривали видеоролики на сайте heretacsko.hu, проверить наличие данного приложения в своей учетной записи ***(Пользователи Facebook стали жертвами ClickJacking-атаки // InternetUA (http://internetua.com/polzovateli-Facebook-stali-jertvami-ClickJacking-ataki). – 2014. – 29.06).***

***

Эксперты из «Лаборатории Касперского» (ЛК) сообщили о таинственном банковском трояне Luuuk, который всего за неделю принес злоумышленникам более 500 тыс. евро. По их словам, хакеры использовали данное вредоносное ПО для осуществления атаки «человек-в-браузере».

Жертвами трояна стали 190 клиентов одного из банков, работающих в Италии и Турции. Злоумышленники похищали их средства и переводили на заранее подготовленные счета. За неделю с каждого банковского счета жертв было снято 1,7–39 тыс. евро.

Троян похищал пароли, одноразовые пароли и имена пользователей для входа в сервисы online-банкинга с помощью вредоносной веб-инъекции. При этом он работал в фоновом режиме одновременно с легитимной сессией.

Luuuk был обнаружен 20 января нынешнего года, когда эксперты из ЛК обнаружили подозрительный сервер, содержащий несколько журналов. Помимо прочего, они нашли записи о соединениях, установленных ботами с веб-панелью управления C&C-сервера. Эксперты предположили, что отправляемые данные имели отношение к финансовому мошенничеству.

«К тому времени как были проанализированы все доступные данные, стало понятно, что данный командный сервер представлял собой серверную часть инфраструктуры, обслуживающей банковские троянские программы», – сообщается в уведомлении ЛК.

Примечательно, что, исследовав C&C-сервер, экспертам так и не удалось установить, какое именно ПО использовалось в ходе вредоносной кампании. Возможности, которыми обладает Luuuk, есть у различных вариантов Zeus – Citadel, SpyEye и IceIX. Вероятно, что Luuuk также является вариантом этого известного трояна ***(За 7 дней троян Luuuk принес злоумышленникам более полумиллиона евро // InternetUA (http://internetua.com/za-7-dnei-troyan-Luuuk-prines-zloumishlennikam-bolee-polumilliona-evro). – 2014. – 27.06).***

***

На днях стало известно о начале работы нового архива XSS-уязвимостей. По словам создателей проекта XSSposed, архив станет некой альтернативой и продолжением ранее существовавшего ресурса xssed.org.

XSSposed создавался по подобию своего предшественника. Так, это открытый некоммерческий каталог уязвимостей Cross-Site Scripting (XSS). Ожидается, что на сайте будут публиковать данные о брешах, найденных на всех доступных интернет-ресурсах.

Отметим, что каждый желающий сможет сообщить о наличии XSS-уязвимости на том или ином сайте. В архиве существует рейтинг пользователей по никам, а наиболее активные «источники информации» получают медали. Регулярно осуществляется очистка логов.

Для того чтобы сообщаемый код был включен в состав архива, его введение должно вызывать появление окна с текстом XSSPOSED на

странице того или иного ресурса. Известно, что в архиве, помимо прочего, будут доступны инъекции фреймов и открытые редиректы. Последний, если верить ресурсу XSSposed, был найден на сайте «Лаборатории Касперского».

Создатели ресурса подчеркивают, что модерация XSS-зеркал происходит очень быстро: уязвимости размещают в архиве сразу после проверки. Они также уверяют, что не намерены удалять данные об уязвимости из-за взятки или по каким-либо другим соображениям.

На момент написания заметки в архиве находилось 87 зеркал для 60 уязвимых сайтов, а информацию пока предоставили 30 пользователей ***(В Сети появился новый архив XSS-уязвимостей // InternetUA (http://internetua.com/v-seti-poyavilsya-novii-arhiv-hSS-uyazvimostei). – 2014. – 28.06).***

***

Эксперты по безопасности AdaptiveMobile обнаружили вредоносную программу под названием Selfmite, направленную на пользователей Android, которая рапространяется через SMS-сообщения.

В отличие от подавляющего большинства вредоносных программ для Android, Selfmite не является трояном. Это фрагмент вредоносной программы, распространяющейся с помощью SMS-сообщений, утверждает аналитик по безопасности из Adaptive Mobile Д. Масленников.

Жертвы получают сообщение со своим именем, содержащее сокращенную goo.gl ссылку, которая перенаправляет их на http://173.244.***.***/TheSelfTimerV1.apk, а затем предлагает загрузить и установить файл в формате apk, написал Д. Масленников в своем блоге. Если пользователь решит скачать предложенный файл, на рабочем столе компьютера появится иконка “автоспуск” (The self-timer). Запуск этой программы начнет сканирование адресной книги устройства жертвы и совершит рассылку сообщений 20 контактам, используя их имя в качестве приветствия.

Червь Selfmite использует рекламную платформу для перенаправления пользователя на веб-сайт, предлагающий скачать конкретную версию приложения Mobogenie и ее установку. Д. Масленников считает, что таким образом злоумышленники хотели увеличить количество установок Mobogenie с помощью вредоносного ПО ***(Атаки с использованием нового SMS-червя Selfmite на пользователей Android // InternetUA (http://internetua.com/ataki-s-ispolzovaniem-novogo-SMS-cservya-Selfmite-na-polzovatelei-Android). – 2014. – 29.06).***

***

Как сообщили эксперты из Trend Micro, все больше ботнетов и вредоносного ПО не только хранится в облачных хранилищах, но также удаленно управляется с облачных серверов. Таким образом хакеры выдают

вредоносные программы за обычный трафик, проходящий между корпоративными конечными точками и облачными сервисами.

«Преступники – умные деловые люди. Если что-то имеет смысл с точки зрения бизнеса, они перенимают это, – сообщается в блоге Trend Micro. – Как и многие представители малого бизнеса по всему миру, они поголовно переходят на облачные сервисы».

Эксперты отмечают, что практика использования облаков для осуществления атак не нова, и существует по крайней мере уже лет пять. Тем не менее, раньше злоумышленники при помощи облачных сервисов только хранили вредоносное ПО, которое потом загружалось на системы жертв. При этом программы для управления (C&C) им размещались на C&C-серверах, которые обычно было легко идентифицировать как подозрительные.

Теперь же хакеры управляют вредоносным ПО, используя популярные облачные сервисы. Большим преимуществом для них является то, что сетевой трафик между C&C и ботнетом или вирусом выглядит как обычный корпоративный трафик.

Эксперты из Trend Micro обнаружили первый образец ПО для управления вредоносами в DropBox. Однако, по их словам, подобные программы могут также размещаться и в других облачных сервисах ***(Хакеры управляют ботнетами с облачных серверов // InternetUA (http://internetua.com/hakeri-upravlyauat-botnetami-s-oblacsnih-serverov). – 2014. – 29.06).***