# СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*Огляд інтернет-ресурсів*
*(28.07–8.08)*

**2014 № 15**

# Соціальні мережі
## як чинник інформаційної безпеки

**Інформаційно-аналітичний бюлетень**
**Додаток до журналу «Україна: події, факти, коментарі»**
Огляд інтернет-ресурсів
(28.07–8.08)
№ 15

**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

Российские социальные сети теряют популярность в Украине. Согласно данным счетчика StatCounter, еще в июле 2013 г. 37 % страниц, просмотренных украинскими пользователями соцсетей, приходилось на сервис «ВКонтакте». В настоящее время его доля снизилась до 21,9 %. Менее активными стали и украинские пользователи «Одноклассников». Летом прошлого года на них пришлось 10 % просмотренных в соцсетях страниц, а сейчас – 3,6 %. Это самый низкий показатель за год, пишет «Капитал».

Одновременно за полгода возросла активность в американских социальных сетях. Доля Facebook, согласно этому же счетчику, увеличилась с 29 % до 41,5 %, Twitter – с 7 % до 14 %.

Меньше действий, больше пользователей

Объем аудитории пока позволяет «ВКонтакте» оставаться крупнейшей соцсетью в Украине. А по поводу снижения активности руководство соцсети пока не переживает. «Никаких негативных тенденций в Украине нет. Есть лишь традиционный сезонный спад, характерный едва ли не для всех интернет-ресурсов», – сообщил пресс-секретарь «ВКонтакте» В. Леготкин. С окончанием лета, по его словам, количество посещений обычно возвращается к норме и снова продолжает расти.

В. Леготкин предоставил данные, что с января количество уникальных посетителей «ВКонтакте» из материковой части Украины снизилось на 17 %, или почти на 2 млн. В Крыму оно остается стабильным – порядка 500 тыс. пользователей «ВКонтакте».

В «Одноклассниках» в настоящее время «сидит» более 5 млн украинцев. По данным исследовательской компании Gemius, с начала года соцсеть потеряла 170 тыс. наших соотечественников.

Агрессия и привычка

Опрошенные «Капиталом» эксперты говорят, что роль российских соцсетей в Украине по-прежнему лидирующая. Однако в связи с российской агрессией в отношении Украины и аннексией Крыма, многие пользователи отказались поддерживать сервисы из России. «Происходящие события в Украине играют свою роль в изменении интереса украинских пользователей к российским онлайн-сервисам», – констатирует директор по развитию бизнеса агентства Web-Promo А. Воронюк. По его информации, существенно уменьшилось количество поисковых запросов для российских соцсетей. Это особенно видно по «ВКонтакте»: об этом сервисе пользователи поисковиков сейчас спрашивают вдвое реже, чем год назад.

Рост активности в Facebook можно также связать с повышенным интересом его пользователей к новостям. Как ранее рассказывала пресс-секретарь агентства интернет-маркетинга Promodo М. Бергер, аудитория Facebook более взрослая и больше интересуется новостями, нежели

пользователи «ВКонтакте». Кроме политических событий, определенную роль играет насыщение уже существующей аудитории. «Социальные сети перестают быть новинкой и диковинкой. Многие люди приходят уже туда для того, чтобы связаться с конкретным человеком, а не просто провести время», – объясняет он.

Украинские конкуренты

С начала года в Украине появилось также несколько локальных соцсетей, которые планировали перебрать на себя часть аудитории российских сервисов. Но пока им удалось привлечь немногих. Количество пользователей наиболее массовых из новых проектов – Weua.info и Druzi.org.ua, – по данным этих сайтов, составляет 171 тыс. и 221 тыс. соответственно. Еще около 3,2 тыс. пользователей в соцсети Ukrface.com.ua ***(Украинцы отказываются от российских соцсетей и переходят в западные // IT Expert (http://itexpert.org.ua/rubrikator/item/37283-ukraintsy-otkazyvayutsya-ot-rossijskikh-sotssetej-i-perekhodyat-v-zapadnye.html). – 2014. – 30.07).***

***

Соціальною мережею Facebook принаймні раз на місяць користуються 1,32 млрд людей – за минулі три місяці аудиторія соцмережі збільшилася на 40 млн користувачів. Про це повідомляє портал Phonearena.

Однак темпи зростання аудиторії Facebook залишаються на тому ж рівні останні кілька кварталів. За попередній квартал Facebook додала 50 млн нових користувачів, до цього – також 40 млн.

399 млн користувачів заходять у соціальну мережу з мобільних пристроїв – це на 15 % більше, ніж у I кварталі цього року, і на 82 % більше показників минулого року.

Приблизно 654 млн користувачів заходять у Facebook з мобільних пристроїв щодня, а 1 млрд регулярно заходять у соціальну мережу як з мобільних пристроїв, так і з комп'ютерів.

Активне зростання мобільної аудиторії відповідає інтересам компанії. Розвиток мобільних технологій голова Facebook М. Цукерберг називає головним пріоритетом соцмережі. Крім додатків самої соцмережі, компанія Facebook володіє сервісами WhatsApp та Instagram, розвиває додатки Paper і Messenger.

Мобільний напрямок є ключовим і для бізнес-показників Facebook. У II кварталі 2014 р. на мобільну рекламу припало 62 % усього рекламного виторгу або 1,66 млрд дол. За прогнозом eMarketer, частка Facebook на глобальному ринку мобільної реклами зросте з 5,8 % до 7,8 % за підсумками поточного року.

Однак не виключено, що темпи зростання аудиторії Facebook можуть сповільнитися. Недавній експеримент Facebook над користувачами з метою дослідження можливості керувати їхніми емоціями за допомогою цілеспрямованої фільтрації повідомлень друзів викликав хвилю обурення

інтернет-співтовариства ***(Кількість користувачів мережею Facebook скоро може досягти 1,5 мільярда // ВІКНА (http://vikna.if.ua/news/category/world/2014/07/29/20226/view). – 2014. – 29.07).***

***

Instagram запустил новый мессенджер для обмена фотографиями под названием Bolt. Об этом сообщает издание Verge, пишет Marketing Media Review (http://mmr.ua/news/id/instagram-zapustil-fotomessendzher-bolt-40630/).

Новое приложение позволяет мгновенно отправлять фотографии и видео, которые исчезают сразу после прочтения. Verge также отметил, что Bolt имитирует аналогичное приложение Taptalk, представленное в апреле 2014 г. В настоящее время новый мессенджер доступен для скачивания в AppStore и Google Play Store только в Новой Зеландии, Сингапуре и Южной Африке.

«Мы планируем запустить приложение и в других странах, однако сейчас мы должны провести бета-тестирование на малой группе», – заявил пресс-секретарь Instagram.

Он также отметил, что в настоящее время у американского приложения Instagram около 65 % иностранных пользователей, которые вскоре тоже смогут воспользоваться новым мессенджером.

24 июля Instagram случайно анонсировал новое приложение для обмена фотографиями. Рекламу приложения со слоганом «обмен фотографиями в одно касание» увидели на своих устройствах некоторые пользователи фотосервиса.

Кроме того, в июне Facebook аналогичным образом запустила свой эфемерный мессенджер Slingshot за неделю до официального релиза. Slingshot также предназначен для обмена фотографиями и видеороликами, он стал прямым конкурентом популярного приложения Snapchat. Оба приложения относят к типу эфемерных мессенджеров, так как сообщения в них самоуничтожаются по истечении заданного времени ***(Instagram запустил фотомессенджер Bolt // Marketing Media Review (http://mmr.ua/news/id/instagram-zapustil-fotomessendzher-bolt-40630/). – 2014. – 30.07).***

***

Социальная сеть Facebook удалила из своих мобильных приложений для iOS и Android функцию обмена сообщениями. Для продолжения переписки с друзьями пользователей теперь просят установить отдельное приложение – Facebook Messenger.

Отделение сообщений от всего остального общения в соцсети было анонсировано Facebook в апреле. Тогда у части пользователей при попытке написать кому-то сообщение стал выводиться текст с предложением установить Facebook Messenger и продолжить переписку в нём.

Тем не менее, ещё несколько месяцев большинство пользователей могли общаться как в основном приложении Facebook, так и в отдельном мессенджере. Теперь же при нажатии на значок сообщений в главном приложении отображается кнопка, предлагающая загрузить Facebook Messenger.

Как сообщало ранее издание «Цукерберг позвонит», единственный способ продолжить общение в Facebook как раньше – использовать приложение социальной сети на смартфоне с устаревшей версией операционной системы Android, не поддерживающей Facebook Messenger ***(Facebook окончательно удалил функцию сообщений из основного приложения // InternetUA (http://internetua.com/Facebook-okoncsatelno-udalil-funkciua-soobsxenii-iz-osnovnogo-prilojeniya). – 2014. – 1.08).***

***

М. Петров – в прошлом главный инженер самого посещаемого портала Рунета – сообщил о возможной альтернативе «ВКонтакте».

Новая социальная сеть, по его словам, гарантирует безопасность и отсутствие какого-либо контроля со стороны государства, пишет sobesednik.ru.

На своей странице М. Петров заявил о доступности переписки не только сотрудникам ФСБ, но и мобильным операторам. Среди последних М. Петров выделил Мегафон, чье качество работы в этом году заметно ухудшилось.

Он предрекает осложнения в работе соцсети: «Существующее руководство ориентировано на снижение затрат любой ценой, или их осенью сменят. Но ставка на две вещи – новые сервера не понадобятся, так как видео и аудио станут платными».

К слову, стоит отметить недавний сбой в работе «ВКонтакте». У пользователей исчезли сообщения, фотографии, записи на «стене», возникали затруднения с «лайками» и комментариями. Некоторое время сайт Vk.com вовсе перестал отвечать на какие-либо запросы. Причина, как уверяет пресс-секретарь социальной сети Г. Лобушкин, – аномальная жара: «По предварительным данным неприятности начались в момент выхода из строя охлаждающего оборудования серверной одного из центров обработки данных “ВКонтакте” в Ленинградской области. После этого произошло аварийное отключение части серверов».

М. Петров обещает пользователям безопасную перспективу: будто бы его сводные братья Павел и Николай Дуровы осенью запустят новую социальную сеть. О ее предстоящем появлении бывший сотрудник «ВКонтакте» высказывается эмоционально и многообещающе: «Из подробностей: нет отслеживания следов точки входа – IP выделенных и статичных, нет ссылок на облако юзера и его файлов, невозможность прочитать переписку даже разработчикам сервиса. И вообще – наша новая соцсеть – это прототип будущего государства».

М. Петров не является участником проекта, но рекламирует его и не исключает дальнейшего сотрудничества. По его словам, новая социальная сеть станет революционной: «Смысл сети – мировая революция против существующего диктата власть предержащих над народом».

М. Петров отмечает, что новая социальная сеть будет «общественной», т. е. без акций и возможности торговли ими. Как пример – «Википедия».

Впрочем, сам П. Дуров в комментарии Tjournal опроверг информацию о возможном запуске сети этой осенью или даже ее разработки: «Михаил не имеет отношения к нашей с Николаем команде. Что касается новых проектов, то мы не начинали активную работу над ними, так как на повестке остаются серьезные задачи в рамках Telegram».

После своего ухода из «ВКонтакте», произошедшего 21 апреля 2014 г., П. Дуров в комментарии для блога TechCrunch заявил о своих планах начать разработку новой мобильной социальной сети. В настоящее время его главным проектом является Telegram – мессенджер с девизом «Верните обратно наше право на приватность».

25 апреля 2014 г. о своем уходе из «ВКонтакте» заявил М. Петров, раннее возглавлявший дата-центр «Ицвой», где находился видео и фотоконтент пользователей «ВКонтакте» ***(Сотрудник «ВКонтакте» рассказал, кто читает переписку пользователей // Хартия'97 (http://www.charter97.org/ru/news/2014/7/28/108806/). – 2014. – 28.07).***

***

У Рівному користувачі найпопулярнішої соціальної мережі «ВКонтакте» готові видалити свої профілі.

Портал «ЧаРівне.інфо» провів опитування, згідно з яким 25,4 % респондентів вказали, що «готові видалити свій акаунт, аби за ними не стежило ФСБ».

Натомість 23 % – «не готові це зробити, бо не володіють таємною інформацією». Ще 19, 6 % «у ВК хочуть залишитись, але при цьому оголосивши бойкот російським товарам».

До слова, в опитуванні брали участь особи до 18 років. Кількість осіб дорослiше 18 років становить 150. Усього голосувало 209 користувачів мережі «ВКонтакте».

Служба безпеки України попереджувала наших громадян про ймовірне втручання спецслужб Росії в особисте життя українців, та інших іноземців. Зокрема шляхом проникнення в соцмережі ***(За рекомендацією СБУ, рівняни готові видалитись із російської мережі ВКонтакте (опитування) // Інтернет-портал «ЧаРівне.інфо» (http://charivne.info/news/Za-rekomendatsiyu-SBU-rivnyani-hotovi-vidalitis-iz-rosiysko-merezhi-VKontakte-opituvannya). – 2014. – 3.08).***

***

Социальная сеть Facebook, принадлежащая одному из самых богатых и молодых миллиардеров М. Цукербергу (занимает 16-е место в рейтинге Forbes с капиталом 32,5 млрд дол.), предоставила жителям африканского государства Замбия возможность посещать Facebook и еще 11 сайтов со своих смартфонов без взимания платы за мобильный трафик.

Эта возможность была предоставлена в сотрудничестве с оператором Airtel и доступна только его абонентам, сообщили в компании.

Помимо мобильной версии веб-сайта Facebook (m.facebook.com), включая мессенджер (m.facebook.com/messages), абонентам предоставляется бесплатный доступ к локальной версии сайта оператора Airtel, сайтам AccuWeather, eZeLibrary, Facts for Life, Google, Go Zambia Jobs, Kokoliko, MAMA, Wikipedia, WRAPP и Zambia uReport.

Сайт eZeLibrary предназначен для ознакомления с законами Замбии и в настоящее время находится в разработке. Facts for Life посвящен здоровью детей, Go Zambia Jobs и Kokoliko – вакансиям местных компаний, MAMA (Mobile Alliance for Maternal Action) – проблемам материнства и планирования семьи, WRAPP (Women's Rights App) – защите прав женщин и Zambia uReport – борьбе с распространением ВИЧ-инфекций.

Получить доступ к указанным сайтам абоненты могут тремя способами: через приложение Internet.org, предварительно загрузив и установив его на Android-смартфон, через сайт Internet.org или через приложение Facebook для Android.

«Используя приложение Internet.org, люди смогут посещать ряд ресурсов, посвященных здоровью, трудоустройству и содержащих полезную информацию для местных жителей, без взимания платы за мобильный Интернет. Мы надеемся, что это увеличит число пользователей Интернета и поможет им найти полезную информацию, которая ранее не была доступна», – прокомментировали в Facebook.

Бесплатный доступ к 12 сайтам – первый шаг в рамках инициативы Internet.org, автором которой является Facebook. Социальная сеть заручилась поддержкой Nokia, Samsung, Ericsson, MediaTek, Qualcomm и Opera Software. Вместе партнеры рассчитывают сделать Интернет доступным большему числу жителей в развивающихся странах. В рамках инициативы Facebook также разрабатывает дроны, оснащенные средствами связи для «доставки» Интернета в отдаленные уголки планеты.

В Facebook пообещали, что в будущем возможность бесплатного доступа с мобильных устройств к избранным ресурсам получат жители в других регионах мира. В компании не уточнили, в каких именно и когда ***(Facebook начал раздавать бесплатный Интернет // InternetUA (http://internetua.com/Facebook-nacsal-razdavat-besplatnii-internet). – 2014. – 1.08).***

***

Если вы относитесь к той категории интернет-пользователей, которой нравятся функциональные особенности сервиса для работы с фотоснимками и изображениями в Google+, но у вас не вызывает симпатий сеть в целом, то для вас имеются хорошие новости от разработчиков.

Вслед за ставшим самостоятельным сервисом для мгновенного обмена сообщениями и организации видеоконференций – Google Hangouts – имеет все шансы отделиться от сети Google+ и стать частью нового проекта и фирменное фотохранилище Google Photos. В настоящее время в одной из крупнейших мировых корпораций планируют заняться разработкой нового детища – ещё одной социальной сети, в которой уже не найдётся места обязательного условия в виде привязки к Google+.

В новой разработке поискового гиганта сделают акцент на загрузку альбомов с фотографиями, их редактирование и прочие графические возможности. Что же касается судьбы функционирующего сегодня Google Photos в качестве главной составляющей сети Google+, то, вероятнее всего, в дальнейшем произойдёт смена названия первого исключительно в маркетинговых целях без потери каких-либо технических преимуществ.

Подобный шаг воспринимается как необходимая мера для привлечения новых людей в Google Photos, которые не хотят испытывать навязываемую компанией зависимость в рамках Google+ ***(Google запустит новую социальную сеть с уклоном в фотосервис // InternetUA (http://internetua.com/Google-zapustit-novuua-socialnuua-set-s-uklonom-v-fotoservis). – 2014. – 4.08).***

***

Соцсеть «Одноклассники» переехала на адрес ok.ru. Об этом «Ленте.ру» сообщил пресс-секретарь соцсети И. Грабовский.

Адрес ok.ru станет основным и будет выдаваться при запросах в интернет-поисковиках. При этом сайт Odnoklassniki.ru также будет продолжает работать. Новый адрес сделает «Одноклассники» официальным брендом соцсети.

«Теперь “Одноклассники” – это “ОК”. Короткое, ясно и удобное имя, которое мы уже постепенно начали использовать достаточно давно. Теперь же представляем “ОК” официально», – говорится в сообщении компании ***(«Одноклассники» переехали на ok.ru // InternetUA (http://internetua.com/odnoklassniki--pereehali-na-ok-ru). – 2014. – 7.08).***

***

В России у депутатов появилась своя социальная сеть – ресурс под названием «Парламентский портал», анонсированный в июле, работает в тестовом режиме. Разработчики надеются, что ресурс будет востребован хотя бы «в целях пиара», пишет «Московский комсомолец» в материале «Однодумники хотят быть “ВКонтакте”«.

По замыслу авторов, портал призван связать все уровни представительной власти России и дать им возможность обсудить свои инициативы с коллегами и экспертами. Свои странички здесь имеют право завести депутаты Госдумы, депутаты региональных законодательных собраний и депутаты муниципальные.

На первой странице портала есть рубрики «Новое» и «Популярное»: в первой при помощи модератора размещаются свежие публикации, предложенные депутатами, а во второй – те статьи и публикации, размещенные на портале, которые пользуются наибольшим интересом. Еще есть тематические рубрики («Безопасность», «Бизнес», «Государство», и т. д.). Материалы о своих инициативах и работе предлагают сами депутаты – это главное условие, поэтому портал предоставляет возможности для самопиара.

Странички депутатов Госдумы появились на портале без их участия – туда внесена информация и фотографии с официального думского сайта. «Сейчас стоит задача максимально привлечь к работе портала самих депутатов, прежде всего регионального и муниципального уровня», – сказали «МК» в аппарате Госдумы.

Площадка создается для того, чтобы депутаты всех уровней могли общаться друг с другом, говорят в Госдуме. Каждый из «членов клуба» сможет привлекать к обсуждению своих инициатив экспертов. Но пока их не зарегистрировано ни одного, отмечает «МК».

Обычный россиянин тоже может зарегистрироваться на портале, следить за ходом дискуссии по той или иной теме, не участвуя в ней, и даже задать вопрос депутату. Сообщение о вопросе сразу будет направлено депутату Госдумы, к примеру, на думскую электронную почту. Если депутат его не заметит – модератор напомнит. На портале можно будет быстро найти сведения о своем представителе любого уровня (в рубрике «Депутаты») ***(В России соцсеть для депутатов запустили без участия самих парламентариев // Утро.UA (http://www.utro.ua/ru/politika/v_rossii_sotsset_dlya_deputatov_zapustili_bez_uchastiya_samih_parlamentariev1407404743). – 2014. – 7.08).***

## СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Украинцы смогут наблюдать за Президентом в еще одной популярной социальной сети Instagram. 30 июля в Twitter П. Порошенко призвал соотечественников подписываться на его Instagram-аккаунт poroshenkopetro, хотя зарегистрирован он был еще в апреле, когда стартовала предвыборная кампания на пост главы государства.

Президент Украины, в отличие от российских чиновников, не публикует селфи и «лифтолуки» – его аккаунт носит сдержанный, как и подобает представителю власти. Зато не экономит на хэштегах.

Фотографии в Instagram Президента преимущественно дублируют те, что были опубликованы в других социальных сетях. Очевидно, как и в остальных социальных сетях, администрирует аккаунт не лично Президент, а его уполномоченные представители.

На сегодняшний день у П. Порошенко в Instagram почти 2,5 тыс. подписчиков. Сам Президент подписан только на один аккаунт. Пользователи активно лайкают и комментируют фотографии Президента. Больше всего украинцам нравятся семейные фото четы Порошенко, а также последние снимки из освобожденных от террористов городов.

П. Порошенко на сегодня, похоже, единственный среди представителей правительства Украины, кто зарегистрировался в Instagram ***(Петр Порошенко завел аккаунт в Instagram // IT Expert (http://itexpert.org.ua/rubrikator/item/37310-petr-poroshenko-zavel-akkaunt-v-instagram.html). – 2014. – 31.07).***

***

В сети Facebook появилась страница Ukraine Today (Украина Сегодня), основателем которой стал выпускник Дипломатической академии Украины при МИД Украины, профессиональный атлет и экономист В. Мигалчан.

Как сказал сам основатель: «Моей целью всегда было прославление Украины за рубежом и поднятия имиджа нашего государства. Так мои спортивные успехи привлекли внимание ко мне и к стране, которую я представляю. До, в течение и после революционных событий на Майдане, активным участником которых я был (не только как гражданин, но и как тот, кто может обеспечить защиту), я занимался переводами и посылал информацию в США и Канаду. Также информацию от меня получали в Великобритании, Испании, Португалии, Италии других странах ЕС, КНР, Индонезии и других странах Азии. Информацию я распространял через собственную страницу в Facebook. Поэтому я решил создать отдельный информационный ресурс, который будет поддерживаться на английском языке».

Ukraine Today (Украина Сегодня) в Facebook – это новый проект, направленный на то, чтобы донести до сведения мировой общественности реальное положение событий в Украине, особенно в контексте русской агрессии и войны. К каналу уже подписались граждане США, Канады, Великобритании, ЕС, стран Азии и Украины. Особый интерес к каналу общественность начала проявлять после трагедии Боинга 777, который был сбит российскими боевиками на территории Донецкой области. Канал является действенным инструментом противостояния в информационной войне, которую ведет Российская Федерация против Украины.

Напоминаем, что недавно в Интернете появилась информация о запуске в Украине телевизионного канала Ukraine Today. Трансляция первое время будет осуществляться в тестовом режиме, а до 24 августа эфирную сетку собираются покрыть уже в полном объеме. Трансляции будут вестись на английском языке. Финансировать новый проект будет медиа-холдинг «1 +1 Media».

Ссылка на страницу: https://www.facebook.com/pages/Ukraine-Today/259092467612804?fref=ts ***(Гребенюк В. В Facebook появилась страница Ukraine Today // Starlife (http://starlife.com.ua/posts/v-facebook-poyavilas-stranitsa-22412.html). – 2014. – 28.07).***

***

Команда украинской соцсети WEUA.info инициировала онлайн-петицию против присутствия П. Порошенко «на сайте враждебного государства», а именно в социальной сети «ВКонтакте». Сотрудников WEUA.info беспокоит то, что «ВКонтакте» якобы контролирует ФСБ, а еще данная соцсеть используется Россией в войне против Украины. Поэтому, пользуясь данным сайтом, Президент Украины спонсирует агрессию против своей страны, считают создатели WEUA.info.

«Социальная сеть "ВКонтакте" – финансово успешное предприятие, которое ежемесячно платит миллионы рублей в виде налогов в российский бюджет. Эти средства используются для вооружения армии оккупанта, следовательно регистрация и пользование этой сетью – поддержка оккупанта!» – сказано в заявлении команды WEUA.info.

Напомним, Президент Украины П. Порошенко зарегистрировался во «ВКонтакте» 15 июля. Ранее П. Порошенко заявил, что инициировал процесс объединения и перевода своих частных аккаунтов в публичные страницы, которые будет поддерживать его команда. Так у Президента Украины есть публичные страницы в Facebook, Twitter, Google+ и «ВКонтакте».

Разработчики WEUA.info обратились к Президенту Украины с просьбой удалить свой аккаунт из российской соцсети. Также они предложили украинским интернет-пользователям поддержать данную инициативу. «Ни для кого не секрет, что эта социальная сеть из популярной не национальной и аполитичной (спасибо за эти бывшие достижения ее бывшему владельцу господину П. Дурову) деградировала в форму дочернего предприятия Федеральной службы безопасности РФ и сегодня во всех возможных комбинациях используется для продолжение информационной войны против нас, украинцев», – сказано в петиции.

В WEUA.info убеждены, что регистрация «ВКонтакте» – это акт поддержки российского интернет-продукта и присутствие Президента Украины на сайте врага – непонятный маневр. «Мы просим Вас удалить свою официальную страницу с российского ресурса "ВКонтакте" и надеемся на ваше понимание того, что война идет не только на поле битвы, но и здесь, в Интернете», – подчеркнули создатели украинской соцсети.

А напоследок они призвали П. Порошенко поддерживать «национального производителя», вероятно, подразумевая регистрацию его официальной страницы на WEUA.info ***(Петра Порошенко и всех украинцев призвали удалиться из «ВКонтакте», чтобы не спонсировать терроризм // IT Expert (http://itexpert.org.ua/rubrikator/item/37239-petra-poroshenko-i-vsekh-ukraintsev-prizvali-udalitsya-iz-vkontakte-chtoby-ne-sponsirovat-terrorizm.html). – 2014. – 28.07).***

***

Просте повідомлення в соціальній мережі переросло у чисельний мирний мітинг

Сотні людей зібрались у Дніпропетровську, аби висловити свою підтримку мешканцям Ізраїлю та довести: в українців та євреїв єдина проблема – тероризм.

Сотні мешканців міста прийшли 28 липня на Фестивальний причал. З прапорами України та Ізраїлю, плакатами «Зупинимо тероризм» та вірою в те, що такий духовний порив принесе користь, люди співали гімни обох країн.

У те, що пост у соціальній мережі зможе зібрати сотні містян, організатори не вірили до останнього. Проте, коли побачили результат, впевнились: попри складну ситуацію в нашій державі, підтримки та розуміння українців вистачить на всіх ***(Просте повідомлення у соціальній мережі переросло у чисельний мирний мітинг // 11 канал (http://www.11channel.dp.ua/news//2014/07/29/24215.html). – 2014. – 29.07).***

***

Організація «Правий сектор» вирішила сховатися від переслідувань ФСБ Росії у мережі Facebook.

«Друзі та підписники! Всі ви, мабуть, знаєте про те, що з 1 серпня в Росії набирає чинності новий антитерористичний закон, що надає повне право на отримання ФСБ РФ практично всіх особистих даних користувачів інтернет-ресурсів.

У зв’язку з цим закликаємо всіх покинути ворожу мережу!» – ідеться в повідомленні групи «Правого сектору».

Організація просить усіх шукати їхню сторінку на Facebook. Також «настійливо рекомендує» всім членам ПС повидаляти свої акаунти в російській соцмережі, а адміністраторам районних осередків Івано-Франківської області наказує стерти свої сторінки. Натомість просить їх перейти на Facebook.

«Не забудьте про пароль! Він повинен відрізнятися від того, який ви використовуєте у vk.com», – додають у Проводі ПС Прикарпаття ***(Правий сектор видаляється з соцмережі «Вконтакте» // GALKA.IF.UA (http://galka.if.ua/praviy-sektor-vidalyayetsya-z-sotsmerezhi-vkontaktye/). – 2014. – 30.07).***

***

Нове керівництво УМВС в Івано-Франківській області «пішло» у мережу та робить наголос на відкритій, прозорій політиці та особистому спілкуванні з мешканцями області.

Про це на прес-конференції повідомив начальник відомства М. Семенишин, повідомляє кореспондент КУРСу.

Головний міліціонер області розповів, що в найбільших соціальних мережах УМВС в області завело власну офіційну сторінку «Міліція Прикарпаття». Відтак, правоохоронці сподіваються на відкритий діалог із прикарпатцями. «Свій робочий день ми починаємо з аналізу соціальних мереж», – говорить М. Семенишин ***(Прикарпатська міліція взялася за соцмережі // Версії.if.ua: Щоденна інтернет-газета (http://versii.if.ua/novunu/prikarpatska-militsiya-vzyalasya-za-sotsmerezhi/). – 2014. – 30.07).***

***

Для более тесного сотрудничества с населением, общественными организациями и представителями средств массовой информации начала функционировать персональная страница руководителя ГАИ в социальной сети Facebook.

На страницу А. Серенко гражданам предлагается обращаться с жалобами и предложениями касательно работы ГАИ и ее сотрудников.

«Я уверяю, что на каждое сообщение о нарушении законодательства в пределах компетенции службы будет обеспечено соответствующее реагирование, – отметил глава Департамента Госавтоинспекции А. Сиренко – От себя лично обещаю оживленное и открытое общение с гражданами».

Согласно заявлению, Госавтоинспекция обещает благодарность и оперативное реагирование на сообщения о нарушениях законов.

Так же на страничке руководителя ГАИ Украины ждут замечания и предложения относительно законодательства, если они позволят улучшить работу автоинспекции ***(Руководитель ГАИ Украины ждет жалобы и предложения на своей персональной страничке // DNEPR.INFO (http://dnepr.info/news/region/6546187-rukovoditel-gai-ukrainy-zhdet-zhaloby-i-predlozhenija-na-svoej-personalnoj-stranichke). – 2014. – 6.08).***

***

Государство давно взяло на вооружение социальные сети и на сегодняшний день у большинства министерств и других ведомств есть профили в ведущих социальных сетях. Самой популярной у органов исполнительной власти является Facebook, за ней следует Twitter, некоторые госорганы используют даже «ВКонтакте». Об этом сообщает ITExpert со ссылкой на Национальный центр электронного правительства.

Отдельные аккаунты существуют уже несколько лет, но настоящий интерес граждан к ним проявился только недавно. Мы решили собрать в

единый перечень все представительства государственных органов, доступные в социальных сетях.

• Урядовий портал. Офіційний портал органів виконавчої влади України – Facebook, Twitter

• Верховна Рада України – Facebook, Twitter, YouTube

• Міністерство оборони України – Facebook, Twitter, YouTube, «ВКонтакте»

• Міністерство економічного розвитку і торгівлі України – Facebook

• Міністерство закордонних справ України– Facebook, Twitter, «ВКонтакте», YouTube

• Міністерство інфраструктури України – Facebook

• Міністерство соціальної політики України – Facebook

• Міністерство фінансів України – Facebook

• Міністерство енергетики та вугільної промисловості України – Facebook

• Міністерство аграрної політики та продовольства України – Facebook, Twitter, YouTube

• Мінрегіон України – Facebook, Twitter

• Міністерство юстиції – Twitter, YouTube

• Міністерство доходів і зборів України – Facebook, Twitter, «ВКонтакте»

• Міністерство освіти і науки України – Facebook, Twitter, YouTube

• Міністерство охорони здоров'я України – Facebook, «ВКонтакте», YouTube

• Міністерство молоді та спорту України – Facebook

• Міністерство внутрішніх справ України – Facebook, YouTube

• Міністерство культури України – Facebook

• Міністерство екології та природних ресурсів України – Facebook, Twitter, YouTube, Google+, «ВКонтакте»

• Департамент ДАІ МВС України – Facebook, Twitter

• Державна служба України з надзвичайних ситуацій – Facebook, Twitter, YouTube

• Державна податкова служба України – Facebook, Twitter, «ВКонтакте»

• Державна прикордонна служба України – Facebook, Twitter, YouTube

• Державна санітарно-епідеміологічна служба України – Facebook, Twitter

• Державна пробірна служба України – Facebook

• Державна служба з питань інвалідів та ветеранів України – Facebook

• Державна служба фінансового моніторингу України – Facebook

• Державне агентство з енергоефективності та енергозбереження України – Facebook

• Державне агентство лісових ресурсів України – Facebook

• Державне агентство України з питань кіно – Facebook, Twitter

• Державне агентство України з туризму та курортів – Facebook
• Державне космічне агентство України – Facebook
• Державна екологічна інспекція України – Facebook
• Державна інспекція сільського господарства України – Facebook
• Державна інспекція України з безпеки на морському та річковому транспорті – Facebook, Twitter, YouTube
• Державна інспекція України з контролю за цінами – Facebook
• Державна інспекція України з питань захисту прав споживачів – Facebook, Twitter
• Державна інспекція України з питань праці – Facebook
• Державна інспекція ядерного регулювання України – Facebook
• Антимонопольний комітет України – Facebook, Twitter
• Фонд державного майна України – Facebook
• Національна гвардія – Facebook, Twitter, «ВКонтакте».
• Повітряні Сили – Facebook
• Національна комісія з цінних паперів та фондового ринку України – Facebook, Twitter, YouTube
• Держпідприємництво – Facebook
• Антикорупційний портал – Facebook, «ВКонтакте», YouTube
• Катастрофа Boeing 777 «Малайзійських авіаліній» (официальная страница комиссии по расследованию катастрофы) – Facebook ***(Facebook стала самой популярной у органов исполнительной власти соцсетью // IT Expert (http://itexpert.org.ua/rubrikator/item/37489-facebook-stala-samoj-populyarnoj-u-organov-ispolnitelnoj-vlasti-sotssetyu.html). – 2014. – 8.08).***

## БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Основатель крупнейшей социальной сети М. Цукерберг рассказал в своем последнем интервью о планах Facebook на разработку собственной платформы для электронной коммерции. Она должна стать станет надстройкой для Facebook Mesenger. Об этом пишет vesti.ru

М. Цукерберг отметил, что введение платежей планируется им не в краткосрочной перспективе – срок разработки услуги может достигать нескольких лет. Компания не собирается наживаться на встроенной рекламе – Facebook собирается получать определенную выручку с платежей.

Подобный шаг Facebook не стал для журналистов сюрпризом. Компания пытается экспериментировать с платежными системами в различных формах в течение последних лет. У Facebook Messenger насчитывается свыше 200 млн активных пользователей по всему миру, а некоторые конкурирующие мессенджеры уже имеют определенный функционал для совершения платежей, так что подобный шаг Facebook выглядит логичным ***(Цукерберг: Facebook Messenger займется денежными переводами // МедиаБизнес***

***(http://www.mediabusiness.com.ua/?option=com_content&task=view&id=40155&Itemid=). – 2014. – 28.07).***

***

«ВКонтакте» даст пользователям возможность зарабатывать на собственных роликах. Для этого владельцы соцсети намерены переработать свою видеоплатформу, пишут «Известия» со ссылкой на источники на медиарынке.

В настоящее время видеосервис «ВКонтакте» не позволяет отслеживать повторное размещение одних и тех же роликов, а его поиск не всегда работает удовлетворительно. Для решения этих проблем будет создан инструментарий, аналогичный тому, что используется на YouTube, рассказали источники.

Пользователи соцсети получат возможность создавать свои видеоканалы, где будут выкладывать собственные видео, на которые смогут предъявлять права. Для последнего видео нужно будет регистрировать в специальной системе FingerPrint, позволяющей сделать его цифровой отпечаток. Если кто-то будет пытаться загружать дублирующий ролик, система либо запретит загрузку, либо заменит видео на уже загруженный аналог.

Появится в «ВКонтакте», по данным издания, и собственная система видеоблогов. Для этого пользователям предложат зарабатывать на своем видео. Как будет действовать эта схема, пока неизвестно ***(Пользователи «ВКонтакте» смогут зарабатывать на видеороликах // InternetUA (http://internetua.com/polzovateli--vkontakte--smogut-zarabativat-na-videorolikah). – 2014. – 29.07).***

***

Интернет-компания Twitter по итогам II квартала получила выручку и прибыль выше ожиданий аналитиков на фоне расширения объемов продаваемой рекламы и роста пользовательской базы. После позитивных квартальных данных бумаги компании возросли почти на 35 % до 50 дол. за акцию.

Согласно данным Twitter, в отчетном квартале база пользователей компании достигла 271 млн человек, что на четверть больше, чем годом ранее. Аналитики отмечают, что в отличие от Facebook, Google+ и некоторых других соцсетей, Twitter за последние два года практически не сбавила темпов прироста базы пользователей. Аналитики прогнозировали, что отчетный квартал Twitter закроет с базой в 267 млн человек.

Продажи Twitter во II квартале возросли почти вдвое до 313,2 млн дол., превысив ожидания аналитиков в 282,8 млн дол.

Отметим, что два предыдущих квартала Twitter сообщала о замедлении темпов роста пользовательской базы, что вызывало определенные опасения инвесторов на рынке в связи с давлением на выручку компании.

Сегодняшний отчет Twitter вновь вселил в держателей акций компании значительный оптимизм.

29 июля акции компании в моменте поднимались в цене до уровня 52,48 дол. Ценовой пик бумаг Twitter был пройден 26 декабря, когда акции торговались на уровне 73,31 дол.

По итогам II квартала чистый убыток Twitter расширился до 144,6 млн дол. или 24 центов на акцию, против 42 млн дол. годом ранее. Операционная прибыль компании составила 2 цента на акцию, против убытка в 1 цент, ожидаемого аналитиками в Нью-Йорке. В текущем квартале Twitter ожидает выручку в 330–340 млн дол., против рыночной оценки в 323,1 млн дол. В текущем финансовом году компания планирует получить выручку в 1,31–1,33 млн дол.

Согласно отчету компании, на сегодня около 81 % рекламы в сети микроблоггинга – это мобильная реклама. За год этот показатель более чем удвоился. Аналитики говорят, что в текущем квартале Twitter может получить прирост результатов благодаря завершившемуся чемпионату мира по футболу в Бразилии, когда Twitter активно генерировала траффик ***(Twitter отчиталась выше прогноза по итогам второго квартала // InternetUA (http://internetua.com/Twitter-otcsitalas-vishe-prognoza-po-itogam-vtorogo-kvartala). – 2014. – 30.07).***

***

Акции американской социальной сети Facebook 30 июля прибавили в цене более 5 % на фоне опубликованной позитивной финансовой отчетности за II квартал 2014 г. После закрытия биржевых торгов в Нью-Йорке цена за бумагу составила рекордные для компании 75,30 дол.

Чистая прибыль компании, согласно обнародованным документам, увеличилась более чем в два раза по сравнению с показателями того же периода 2013 г. и составила 791 млн дол.

Выручка за отчетный период возросла на 61 %, составив 2,91 млрд дол. против 1,81 млрд дол. за аналогичный период 2013 г. При этом большая часть квартальной выручки пришлась на доходы от рекламы, которые возросли на 67 % и достигли рекордных 2,68 млрд дол. ***(Акции Facebook рекордно выросли // Перший Діловий Телеканал (http://fbc.net.ua/news/societu/aktsii_facebook_rekordno_vyrosli.html). – 2014. – 31.07).***

***

Каждый квартал социальные сети наращивают базу рекламодателей, которые покупают рекламу в приложениях, при этом эффективность мобильных объявлений едва ли заслуживает такого внимания.

30 июля Twitter сообщила, что ее продажи мобильной рекламы составили 224 млн дол. во II квартале этого года. Если сравнивать с 2013 г.,

то в этом же квартале доходы от мобильной рекламы Twitter были на 36 % ниже.

Facebook все еще более невероятно. Мобильная реклама приносит компании 800 млн дол. А если сравнивать доходы II квартала 2014 г. с IV кварталом 2013 г., то рост равен 34 %.

Однако в компаниях SocialFlow, Direct Agents и SocialRank уверены, что мобильная реклама еще не так эффективна, чтобы тратить на нее такие средства, пишет Adweek.

«Сегодня еще сложно достичь аудитории на мобильных девайсах, и ленты Facebook и Twitter представляются для рекламодателей лучшим вариантом решения проблемы. Но есть другой путь: сначала внимание пользователей, затем деньги», – говорит Д. Андерсон, генеральный директор SocialFlow ***(Facebook и Twitter надувают пузырь в мобильной рекламе // Marketing Media Review http://mmr.ua/news/id/facebook-i-twitter-naduvajut-puzyr-v-mobilnoj-reklame-40672/). – 2014. – 1.08).***

***

Instagram проводит тестирование с Mercedes-Benz, которое позволяет бренду эффективно таргетировать пользователей Facebook, которые ранее видели одно из рекламных сообщений Instagram, пишет Marketing Media Review http://mmr.ua/news/id/facebook-i-instagram-testiruet-novyj-sposob-targetirovat-polzovatelej-s-pomoschju-reklamy-40658/).

Facebook отказался комментировать, но представитель Mercedes-Benz подтвердил о наличии теста.

Бренды возможно вскоре смогут использовать Instagram и Facebook, чтобы пройти свой путь по воронке продаж. Руководитель медиа агентства, имеющий отношение к рекламе Instagram, отметил, что Instagram разрабатывает возможность для рекламодателям показать рекламные сообщения пользователям Instagram на основе рекламных сообщений, которые они видели в Facebook.

Одна из целей эксперимента позволить Mercedes, который начал показывать рекламу в Instagram в этом месяце – провести A/B тестирование рекламы в Facebook и Instagram и получить инсайт о том, какие изображения демонстрируют более хорошие результаты на каждой из платформ ***(Facebook и Instagram тестируют новый способ таргетировать пользователей с помощью рекламы // Marketing Media Review http://mmr.ua/news/id/facebook-i-instagram-testiruet-novyj-sposob-targetirovat-polzovatelej-s-pomoschju-reklamy-40658/). – 2014. – 31.07).***

***

Twitter купила стартап Mitro, предоставляющий возможность использовать один пароль нескольким лицам, назначенным пользователем, не раскрывая им само кодовое слово. Об этом сообщил ресурс Mashable.

На сайте стартапа сообщается, что коды для клиентской и серверной части проекта становятся открытыми по лицензии GPL. Она позволяет разработчикам использовать предоставленные программные коды, изменять их и использовать в бесплатных и коммерческих продуктах, если они также распространяются на условиях GPL. Команда Mitro переезжает в офис Twitter в Нью-Йорке.

Сумма сделки не сообщается. Ранее А. Хлисс, основавший стартап в 2012 г., получил от инвесторов 2,4 млн дол.

Это уже второй стартап, приобретенный компанией за последние сутки. Ранее Twitter купила стартап Madbits, занимающийся поиском изображений ***(Twitter купил сервис для совместного использования паролей // InternetUA (http://internetua.com/Twitter-kupil-servis-dlya-sovmestnogo-ispolzovaniya-parolei). – 2014. – 2.08).***

***

Социальная сеть LinkedIn, предназначенная для поиска и установления деловых контактов, объявила о квартальных финансовых показателях, которые оказались выше прогнозов Уолл-стрит. Однако американская компания начала работать в убыток.

По итогам II квартала 2014 г. чистый убыток LinkedIn достиг 1,03 млн дол., тогда как годом ранее была зафиксирована чистая прибыль в размере 3,73 млн дол. При этом скорректированная прибыль заметно возросла – с 38 до 51 цента в расчете на одну акцию. По прогнозам аналитиков, скорректированная прибыль должна была составить 39 центов на акцию.

Выручка соцсети увеличилась на 47 % в годовом исчислении – до 533,9 млн дол. Прогноз рыночных экспертов подразумевал доход на уровне 511 млн дол.

За отчетный период на продаже премиум-аккаунтов LinkedIn заработала 105 млн дол., увеличив показатель годичной давности на 44 %. Рекламный бизнес, за который отвечает подразделение Marketing Solutions, также показал 44 % прирост выручки – до 106 млн дол. Сервис платных объявлений работодателей и соискателей вакансий принес компании доход в 322 млн дол., что на 49 % больше по сравнению со второй четвертью 2013 г. Число пользователей соцсети превысило 300 млн человек ***(Деловая соцсеть LinkedIn стала убыточной // InternetUA (http://internetua.com/delovaya-socset-LinkedIn-stala-ubitocsnoi). – 2014. – 2.08).***

***

Социальные сети становятся все более востребованным каналом коммуникации. Застройщики активно используют этот инструмент общения с клиентами и говорят о его высокой эффективности.

В современных условиях застройщикам приходится все более внимательно следить за потоком информации, который может повлиять на его репутацию. Чтобы не оказаться в стороне, а самому регулировать информационные волны, девелоперы все чаще в свою стратегию продвижения включают работу в социальных сетях, говорит А. Лепехина, директор по продвижению NAI Becar.

По словам А. Отрощенко, директора по связям с общественностью ООО «Главстрой-СПб», сегодня соцсети являются одним из наиболее популярных и оперативных каналов коммуникации не только для собственников квартир и потенциальных клиентов, но и для профессионального сообщества. «Застройщики стараются использовать все инструменты работы с аудиторией социальных сетей: создание официальных страниц компании и объектов, работа в существующих сообществах и форумах и т. д. Это все позволяет не только транслировать информацию о компании и проектах, но и вести диалог с существующими и потенциальными клиентами», – рассказывает А. Отрощенко.

По данным участников рынка, самой популярной соцсетью, которой пользуются в том числе и клиенты строительных компаний, является «ВКонтакте». Далее идут Facebook, «Одноклассники», Twitter, YouTube, Google plus и Instagram.

«Группа, сообщество или страница в любой из социальных сетей, хорошо проработанная и наполненная актуальным контентом, фактически является вторым сайтом компании. Также любое сообщество отлично индексируется поисковыми системами, и для этого не нужно затрачивать много усилий и денег, как, например, для SEO-продвижения. Главное здесь – возможность быстрой обратной связи: вопрос-ответ, – поясняет Н. Суслова, генеральный директор коммуникационного агентства “Репутация”. – На сайтах тоже работают онлайн-консультанты, но любому покупателю жилья всегда интересно почитать отзывы о компании-застройщике людей, которые уже живут в доме или ждут его сдачи. Сарафанное радио – лучшая реклама, тем более когда наружная, телевизионная, печатная реклама частенько воспринимается как информационный шум».

Все опрошенные «Строительным Еженедельником» эксперты говорят о высокой эффективности работы в соцсетях. «Основная проблема, которую решают соцсети, – это возможность прямого общения с клиентом, – продолжает А. Лепехина. – Информация проходит не через призму СМИ, рекламы, а идет напрямую к человеку, задающему вопрос. И открытость компании в общении, в том числе и в соцсетях, на современном рынке является преимуществом».

К тому же грамотная работа в социальных сетях, по мнению А. Отрощенко, позволяет снизить риск возникновения непроверенных слухов и распространения некорректной информации.

С. Цинбарев, специалист отдела маркетинга и продаж EKE Group, добавляет, что социальные сети являются эффективным инструментом постпродажного обслуживания. С ним согласна К. Никитина, руководитель PR-службы O2 Development: «Ведение групп в соцсетях помогает решить проблемы покупателей, связанные с поиском и выбором жилья, потребностью получать актуальную информацию о ходе строительства до сдачи дома в эксплуатацию и поддержку во время эксплуатации».

При этом работа в соцсетях не требует от застройщика больших затрат. «Оплата такой работы за месяц может быть сопоставима в среднем с выходом одного рекламного объявления в крупном издании или с арендой пары билбордов в месяц, а результат того стоит», – говорит Е. Валуева, директор по маркетингу компании Mirland Development Corporation.

По оценкам Н. Сусловой, затраты на работу специалиста и оплату таргетинговой рекламы для сообществ или постов в месяц могут составить от 30 тыс. до 150 тыс. р. для одной социальной сети. «Первые результаты от продвижения группы станут заметны через 2–3 месяца. Главное – помнить: если вы не создадите официальную группу вашей компании, кто-то это обязательно сделает за вас», – резюмирует Н. Суслова ***(Застройщики идут в соцсети // Advis.ru (http://advis.ru/php/view_news.php?id=5DC121D2-001D-A44F-B19D-84028AF1D10C). – 2014. – 4.08).***

***

SMM-агентство Shareablee предоставило данные, где говорится о том, что компании, хотя и не покупают активно рекламу в Instagram, являются постоянными пользователями этой социальной сети, пишет Marketing Media Review (http://mmr.ua/news/id/instagram-operezhaet-facebook-po-aktivnosti-brendov-40716/).

Насколько похожи Instagram и Facebook, когда дело доходит до активности брендов? Намного больше, чем мы думаем. Вот интересные цифры о том, как бренды в США ведут себя в этих социальных сетях. Статистика за II квартал 2014 г. (напомним, что Facebook появился на четыре года раньше, чем Instagram):

Facebook генерирует 2,5 млн постов брендов, что больше, чем в прошлом году, на 22 %;

В Instagram тем временем опубликовано 493 тыс. постов, что на 49 % больше прошлогоднего результата;

В Facebook всего за II квартал 2014 г. было зарегистрировано 6 млрд активностей (лайки, комментарии, шейры);

В Instagram произошло 3,4 млрд активностей (лайки, комментарии);

На каждый пост бренда в Facebook приходится 2,396 активностей, в Instagram – 6,932.

По этому поводу есть четыре вывода:

Во-первых, Instagram прибавил 56 % в числе активностей на фоне присоединения к Facebook. Во-вторых, рост активности брендов в Instagram действительно происходит гораздо быстрее, чем в Facebook. В-третьих, будущее платной рекламы в Instagram пока неясно. В-четвертых, активность пользователей по отношению к брендам в Instagram намного выше, чем в Facebook ***(Instagram опережает Facebook по активности брендов // Marketing Media Review (http://mmr.ua/news/id/instagram-operezhaet-facebook-po-aktivnosti-brendov-40716/). – 2014. – 5.08).***

***

В мире социальных сетей живет множество мифов, легенд, слухов, а также массовых заблуждений. С момента появления Facebook мы думаем, что знаем, как нужно написать пост, чтобы он привлек наибольшее количество внимания и вовлеченности пользовательской аудитории. С тех пор как у нас появился аккаунт в Twitter, мы убеждены, что понимаем, как можно и как нельзя им оперировать для успеха нашей бизнес-кампании, пишет Marketing Media Review (http://mmr.ua/news/id/5-faktov-kotorye-zastavjat-vas-po-drugomu-vzgljanut-na-socialnye-seti-40752/).

Все это просто чудесно, но насколько наше поведение в соцсетях соотносится с некоторыми реалиями Интернета? Давайте рассмотрим пять фактов, которые, возможно, изменят ваш подход к работе с социальными медиа:

1. Коэффициент окупаемости инвестиций email-маркетинга – 4300 %.

Статистика по email-маркетингу? А вы думали, что мы будем говорить о социальных сетях, верно? Дело вот в чем: эта шокирующая статистика имеет непосредственное отношение к тому, как вы работаете в социальных медиа.

И вот самый главный факт: коэффициент окупаемости email-маркетинга просто огромен, больше, чем у любой кампании в соцсетях. Просто сравните окупаемость в 4300 % с тем же показателем социальных сетей, плетущимся где-то позади. Даже труда не стоило, правда?

У органического поиска и контекста самые высокие проценты приобретения новых клиентов. Главный конкурент у них – email-маркетинг, из-за его коэффициента окупаемости.

Самый главный плюс email-маркетинга в том, что его процент приобретения клиентов растет огромными темпами: за четыре последних года увеличился в четыре раза. Показатели его эффективности превосходят любую социальную сеть, а рост далеко их опережает.

2. У YouTube самый высокий показатель вовлеченности и самый низкий показатель отказов.

Когда мы слышим слово «соцсети», мы автоматически думаем о Facebook, Twitter, Google+ и им подобных.

Но как же YouTube? Давайте взглянем только на некоторые показатели:

Среднее время на сайте: 227 секунд

Глубина просмотра: 2,99 страниц

Показатель отказов: 43,19 %

В исследовании Shareaholic сказано, что YouTube является бесспорным чемпионом по всем показателям.

3. Трафик из Facebook больше, чем из любой другой соцсети.

Хотите знать, какая социальная сеть предоставляет вам больше всего трафика? Так вот, это Facebook.

В течение нескольких месяцев специалисты из Shareaholic анализировали реферальный трафик на сайты из различных соцсетей. Абсолютным чемпионом стал Facebook, подтвердив, что у него самый высокий показатель реферального трафика на планете.

4. Каждый пин в Pinterest стоит 78 центов

Плюсом этой соцсети является все тот же реферальный трафик. Разумеется, он гораздо ниже, чем у Facebook, но зато выше, чем у Twitter, YouTube, Google+ и LinkedIn.

Стоит вспомнить и об окупаемости инвестиций. Она, как выяснилось, у Pinterest есть, но в долгосрочной перспективе. Владельцу аккаунта придется довольно долго ждать какого-либо отклика после создания своего пинборда, не говоря уже о доходе. В отличие от Twitter, где «период полураспада» длится очень недолго, а подписчики добавляются так же быстро, как и исчезают, в Pinterest эти процессы занимают гораздо больше времени. Можно сравнить аккаунт в Pinterest с вином: чем старше, тем лучше.

Не рассчитывайте получить доход от Pinterest раньше, чем через два месяца. Подписчики тратят много времени, изучая пинборды других пользователей, а затем подбирая материалы для своих пинов. «Среднестатистическим» пином делятся примерно 10 человек, но долго приходится ждать репостов этого пина с их страниц.

5,65 % пользователей Twitter ожидают получить ответ в течение двух часов.

Ваши потенциальные клиенты используют Twitter как «горячую линию» компании. Если вы не отвечаете в течение нескольких минут, вы пропали.

Если вы не ответите на протяжении этого времени:

38 % потребителей станут негативно относиться к бренду и, в результате, перестанут пользоваться услугами компании.

60 % предпримут активные действия, чтобы выразить свое неудовольствие, оставляя негативные отзывы в соцсетях. 74 % пользователей полагают, что это приведет к улучшению работы компании.

Как выигрывают бренды, отвечающие своим потенциальным клиентам незамедлительно?

34 % потребителей будут продолжать сотрудничать с компанией.

43 % порекомендуют бренд своим родственникам и друзьям.

38 % будут гораздо активнее реагировать на рекламу бренда.

42 % пользователей будут активно рекомендовать бренд в соцсетях.

Вы много получите, если будете отвечать своим клиентам в Twitter быстро, и также много потеряете, если не будете этого делать ***(5 фактов, которые заставят вас по-другому взглянуть на социальные сети // Marketing Media Review (http://mmr.ua/news/id/5-faktov-kotorye-zastavjat-vas-po-drugomu-vzgljanut-na-socialnye-seti-40752/). – 2014. – 7.08).***

***

LinkedIn запустил скрытый Спонсированный контент – версию рекламной программы «Спонсированные обновления». Новые объявления будут публиковаться не на странице бренда, а в ленте новостей подписчиков. Рекламодатели могут настраивать, тестировать рекламные объявления и улучшать их для своей целевой аудитори, пишет Marketing Media Review (http://mmr.ua/news/id/linkedin-zapustil-skrytyj-sponsirovannyj-kontent-40576/).

LinkedIn – не первая социальная сеть, применившая «скрытые» сообщения, которые не опубликованы на странице бренда. Facebook предложил их более года назад. Как и в Facebook, «Спонсируемый контент» LinkedIn дает компаниям возможность таргетировать и проверять сообщения, не прибегая к рассылке спама.

Сообщения «Спонсируемого контента» не должны быть организованы менеджером страницы, так как контент не размещается на странице компании. При согласии администратора страницы несколько заинтересованных сторон могут проверить контент для своих аудиторий.

Новое рекламное предложение доступно в менеджере кампаний LinkedIn и «Спонсируемых обновлениях». О поддержке «Спонсируемого контента» заявили компании Unified и AdStage. AdStage дает возможность управлять всеми «скрытыми» сообщениями одновременно, а также настраивать внешний вид контента и отслеживать переходы. Об участии в пилотном проекте заявили Comcast Business и NewsCred.

По данным LinkedIn, на «Спонсируемый контент» приходится 19 % выручки от маркетинговых решений компании.

Программа «Спонсируемые обновления» была запущена год назад для размещения рекламных сообщений вверху ленты новостей на домашней странице пользователей ***(LinkedIn запустил скрытый спонсированный контент // Marketing Media Review (http://mmr.ua/news/id/linkedin-zapustil-skrytyj-sponsirovannyj-kontent-40576/). – 2014. – 28.07).***

# СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

## Інформаційно-психологічний вплив мережевого спілкування на особистість

Использование социальных сетей увеличивает положительный заряд от хорошей новости

Исследователи изучили 300 студентов из Университета Висконсина, Мэдисон. Участники вели дневник, фиксируя в нем то, какие эмоции вызвала у них та или иная новость, и какие эмоции возникли у них после того, как они ей поделились. После этого ученые давали новостям оценку по специальной шкале (от хороших до плохих). Таким образом, они закодировали эмоциональное состояние студентов.

Исследователи обнаружили, что, помимо живого общения, 70 % участников делятся новостями с помощью телефонных звонков, SMS-сообщений или социальных сетей. В основном, люди использовали больше одного способа поделиться, независимо от характера новостей. Однако ученые выяснили: плохие и хорошие новости сообщаются разными способами, передает CBS News.

Для обмена хорошими новостями большинство предпочитает Twitter или SMS-сообщения. Это происходит из-за того, что посредством данных видов связи можно быстро и ненавязчиво поделиться с другими людьми. Если случается что-то хорошее, мы сразу же хотим сообщить об этом. Когда речь идет о плохих новостях, люди стремятся рассказать их по телефону. «Многие считают: телефонный звонок предвещает плохие новости. Оказывается, часто это действительно так», – говорит автор исследования К. Тома.

Использование социальных сетей увеличивало положительный заряд от хорошей новости. При сообщении плохих новостей, эмоциональное состояние ухудшалось. «Когда мы делимся, новость кажется нам более реальной», – объясняет К. Тома. Наименьший отрицательный эффект наблюдался, когда участники делились плохими новостями по телефону ***(Социальные сети больше подходят для хороших новостей // Багнет (http://www.bagnet.org/news/health/243441). – 2014. – 29.07).***

***

Несколько интересных выводов после семинара Майдан Мониторинг в Виннице по использованию соцсетей и ведению информационной войны:

Нужно все свои наблюдения, изменения в мышлении по-максимуму описывать в соцсетях. Таким образом мы невольно заставляем людей задуматься, способствуем обсуждению, изменению мышления и развитию

своего окружения, а значит и изменению страны, мира и т. д. Мы недооцениваем этот вклад.

Нужно стараться все интересные события, которые происходят вокруг, описывать в соцсетях. В последнее время часто именно сообщения обычных людей становятся топ-новостями. Поэтому, нужно обзаводиться смартфоном, Интернетом и, кто знает, может быть однажды ваша информация изменит мир.

С той же целью нужно не лениться комментировать, «тежить» друзей. Таким образом доступность нашей информации будет повышаться.

Много интересного было сказано о Twitter. Оказывается, Twitter имеет неограниченные возможности для анализа собственной деятельности и связей. Другого ресурса с такими возможностями нет.

Кроме этого, сделав репортаж про событие из нескольких твитов можно в пару нажатий легко создать статью.

И, оказывается, анализ соцсетей – это уже научная дисциплина! Во как.

Три основных вывода по поводу информационной войны:

– Закрыть все аккаунты в зоне ру. Именно потому, что теперь по ним очень легко проследить всю вашу деятельность и связи.

– Важно учиться мыслить критически и побуждать к этому своё окружение.

– Перестать смотреть источники негатива ***(Ляшенко Н. Семинар в Виннице: Все интересные события, наблюдения и мысли нужно описывать в соцсетях // МАЙДАН (http://maidanua.org/2014/08/semynar-v-vynnytse-vse-ynteresnyie-sobyityya-svoy-nablyudenyya-y-myisly-nuzhno-opysyivat-v-sotssetyah/). – 2014. – 5.08).***

***

Индийские информатики раскрыли секрет распространения ложных сведений по соцсетям

В последние годы ученые и политики по всему миру начали осознавать, что соцсети – мощный механизм влияния, который можно гораздо эффективнее использовать для манипуляции общественным мнением, чем традиционные медиа – телевидение, радио и печатные издания. В 2011 г. айтишники из MIT раскрыли в журнале Science особую методику передачи и распространения информации через Twitter, которая помогла им победить в конкурсе «Сетевой вызов» DARPA в 2009 г. Авторы публикации открыто утверждали, что подобный прием можно использовать для координирования действий активистов во время революции или для дезинформации противника.

К. Кумар и его коллега Г. Гитакумари из Института технологий и науки имени К. Бирлы в Хайдерабаде (Индия) решили выяснить, как дезинформация и ложные сведения распространяются в социальных сетях, и попытались найти способы противостоять подобной информационной угрозе. В качестве материала для анализа индийские айтишники взяли

реальное событие в недавней истории Азии – вспышки свиного гриппа 2009 г. и связанный с ними поток дезинформации.

Авторы статьи обратились в Facebook, Twitter и в региональные социальные сети и собрали огромный пакет данных с сообщениями, которые оставляли пользователи во время эпидемии. Они изучили содержимое твитов, постов в Facebook и в блогах, построили гигантские «деревья» социальных связей между пользователями и попытались найти закономерности в том, как происходила передача дезинформации и почему люди верили таким сообщениям и делились ими с друзьями.

Подобный анализ невозможно осуществлять вручную – К. Кумару и Г. Гитакумари пришлось разработать автоматизированные алгоритмы статистического анализа, которые сравнивали содержимое постов в соцсетях с учетом социального и экономического положения их авторов, их возраста, времени публикации и множества других факторов. Каждая из этих программ была основана на одной из дюжины наиболее популярных сегодня моделей того, как распространяется информация в сообществах из множества связанных друг с другом узлов. Ученые попытались найти некие общие факторы, влияющие на этот процесс.

Результаты такого сопоставления оказались довольно неожиданными – на распространение дезинформации о вспышках гриппа в разных уголках Азии больше всего влияло эмоциональное содержимое сообщения и его семантическая структура, а не сила социальных связей между пользователями или какие-то другие факторы. В пользу этого говорит то, что друзья в Twitter ссылались друг на друга, распространяя слухи, лишь в 22 % случаев, и цепочки передачи таких некорректных сведений редко содержали в себе более четырех взаимных фолловеров. Число прямых и косвенных ретвитов практически не зависело от того, насколько популярным был пользователь, выступавший источником слухов, и как много друзей у него было.

Как считают авторы статьи, привлекательные дезинформирующие сообщения, способные быстро и широко распространяться по соцсетям, возникали не сами по себе и не были случайными, их авторы осознанно пытались распространить слухи и ложную информацию и практически всегда добивались успеха.

По словам ученых, эту проблему практически невозможно решить при помощи существующих сегодня методов управления и мониторинга за работой социального сегмента Интернета. Для отражения семантических атак, как называют такие дезинформирующие сообщения авторы статьи, необходима особая система защиты, работающая примерно так же, как современные антивирусы и файерволлы в информационном пространстве. В качестве заключения К. Кумар и Г. Гитакумари призывают администрацию Facebook, Twitter и других социальных сетей начать ее разработку ***(Телишев А. Сети дезинформации // Русская Планета (http://rusplt.ru/world/seti-dezinformatsii-11714.html). – 2014. – 1.08).***

Совет национальной безопасности и обороны (СНБО) предупреждает о появлении фейковой страницы пресс-центра АТО в Facebook.

«Появилась фейковая страница, один к одному, которая создана российскими спецслужбами», – сказал спикер Информационно-аналитического центра СНБО А. Лысенко на брифинге в Киеве.

По его словам, отличить настоящую страницу от фейковой можно по наличию англоязычной версии ***(В Фейсбуке россияне создали фейковую страницу пресс-центра АТО, – СНБО // Новости Донбасса (http://novosti.dn.ua/details/230937/). – 2014. – 29.07).***

***

Распространенная 27 июля рядом СМИ и в соцсетях информация о том, что украинская власть якобы готовит масштабные провокации в Павлограде с большим количеством жертв среди мирного населения, – очередной фейк от террористов.

Об этом сообщили в пресс-службе Управление СБУ в Днепропетровской области, передает Цензор.НЕТ со ссылкой на Укринформ.

«Установлено, что сообщение является пропагандистским шагом террористов и их российских кураторов, целью которого является распространение панических настроений среди населения и снижение авторитета органов государственной власти», – отметили в пресс-службе, уточнив, что первоисточником указанного фейка являются российские интернет-ресурсы и группы в социальных сетях.

Служба безопасности принимает меры для установления лиц, причастных к распространению ложных слухов, в украинском сегменте Интернета.

Как стало известно, террористы обвинили губернатора Днепропетровской области, бизнесмена И. Коломойского в подготовке к масштабной провокации в г. Павлоград. Вроде бы подготовлены группы русскоязычных боевиков, которые, прикидываясь «ополченцами» «ДНР» и «ЛНР», должны были устроить в Павлограде провокации, в результате которых должны были быть убиты сотни мирных жителей, якобы из мести за погибших в так называемых «Луганской» и «Донецкой республиках» ***(Террористов поймали на лжи о провокации в Павлограде, – СБУ // Цензор.НЕТ (http://censor.net.ua/n295734). – 2014. – 28.07).***

***

Хакеры из группы «Анонимный интернационал», которые недавно выложили в сеть переписку российских военных, взломали электронную почту депутата Госдумы РФ Р. Шлегеля. Судя по переписке, которая попала в сеть, депутат координировал работу троллей на украинских и иностранных

форумах, руководил «вбросами» и всячески содействовал сепаратистам. Например, в одном из писем он дает указание своему помощнику напечатать бюллетени для «народного референдума» о федерализации Украины. Еще в одном – пишет П. Дурову с требованием заблокировать аккаунты «Правого Сектора».

В отличие от предыдущей «фабрики троллей», бюджет шлегельского штаба оказался намного скромнее – на оплату труда «пропагандистов» выделялось около 3 тыс. дол. Более того, в штабе депутата предпочитали сотрудничать с теми, кто был готов славить В. Путина и разоблачать США забесплатно. В переписке можно отыскать видео о том как, здорово, что Крым присоединился к России, заготовки записи в ЖЖ о героических парнях из «Беркута», колонки прокремлевских колумнистов и многие другие материалы, посвященные Украине.

Очень подробный анализ переписки выложил ЖЖ пользователь под ником ntv. AIN.UA отобрал несколько интересных материалов, которые иллюстрируют работу депутата над «украинским вопросом». Так, в одном из писем депутат просит своего помощника изготовить бюллетени для поддержки сепаратистов.

Сказано – сделано. Вскоре после этого «бюллетени» отправились на восток Украины.

Кроме того, россиянин просил П. Дурова заблокировать «ВКонтакте» группы «Правого сектора», в которых «осуществляются экстремистские и русофобские призывы». Свою просьбу он мотивировал якобы обращениями граждан в Госдуму РФ.

Напомним, что в конце июня этого года россияне потребовали убрать из файлообменника Ex.ua архив с перепиской некоего И. Осадчего, поскольку размещение переписки в свободном доступе нарушает российские законы. А пользователя, разместившего архив, требовали заблокировать. СМИ связывают И. Осадчего с компанией «Конкорд» предпринимателя Е. Пригожина, а также – с неким «Агентством интернет-исследований».

Согласно информации, которую выложили в сеть хакеры, это агентство координирует деятельность так называемых «кремлевских троллей» – людей, которые издевательскими, критическими или угрожающими комментариями заполняют страницы с критикой политики российских властей – причем даже на сайтах зарубежных зданий ***(Взломана почта российского депутата: в сеть попали подробности информационной войны против Украины // InternetUA (http://internetua.com/vzlomana-pocsta-rossiiskogo-deputata--v-set-popali-podrobnosti-informacionnoi-voini-protiv-ukraini). – 2014. – 6.08).***

## Зарубіжні спецслужби і технології «соціального контролю»

Сайт «Одноклассники» видалив спільноту «Західна Україна для всіх! Україна – це Європа!», у якій налічувалося понад 43 тис. учасників. Про це через свій канал на YouTube повідомляє модератор спільноти В. Старущак. Хлопець є людиною з особливими потребами, він інвалід 1 групи. Прикутий до ліжка, намагався бути потрібним для своєї країни і внести вклад для консолідації і єднання, як українців, так й інших людей. Багато часу та сил він приділяв модерації і ось в один день, не зміг зайти на свій акаунт в «Одноклассниках», сторінка була знищена, а разом з нею і комунікаційний майданчик спільноти «Західна Україна для всіх! Україна – це Європа!» Слід зауважити, що це зробили без будь-якого попередження чи зауваження з приводу того чи іншого записа В. Старущака.

Хлопчина закликав користувачів переходити на інші соціальні мережі, такі як WEUA (weua.info), ДРУЗІ (druzi.org.ua) або Facebook (https://www.facebook.com). А сайту «Одноклассники» (www.odnoklassniki.ru) зробити всесвітній бойкот.

Відомий музикант, фронтмен гурту «Тартак» С. Положинський прокоментував це на сторінці у Facebook: «Я своєю сторінкою на однокласниках користуюся мінімально – часом заходжу перевірити, чи не з'явився хтось із колись загублених близьких людей. Тепер хочу видалити сторінку. Якщо не розберуся – спитаю у вас як. А поки давайте підтримаємо ініціативу, хто як може» ***(Сайт «Однокласники» видалив 43-тисячну спільноту, яку створив інвалід I групи // UAINFO (http://uainfo.org/yandex/363073-sayt-odnoklasniki-vidaliv-43-tisyachnu-splnotu-yaku-stvoriv-nvald-grupi-vdeo.html). – 2014. – 25.07).***

***

Мэрии российского г. Красноярск запретили пользоваться социальными сетями Facebook и Twitter и поисковиком Google, сообщает интернет-издание «Красноярский блокнот» со ссылкой на «Седьмой канал».

С 25 августа будут блокироваться не только три этих портала, но и все почтовые сервисы и социальные сети не на русских доменах. Соответствующее распоряжение выпустило управление информатизации и связи. В документе сказано, что зарубежные системы служат основой для активного противодействия политике государственной власти. Ограничение объяснили вопросами информационной безопасности.

Ранее кировским учителям рекомендовали не пользоваться Google для служебной переписки. Весной в Совете Федераций прозвучало предложение создать российский Интернет – сеть «Чебурашка», а в мае запустился российский государственный поисковик «Спутник» ***(Российским чиновникам запретили пользоваться Google, Facebook и Twitter // IT***

***Expert (http://itexpert.org.ua/rubrikator/item/37221-rossijskim-chinovnikam-zapretili-polzovatsya-google-facebook-i-twitter.html). – 2014. – 27.07).***

***

Депутат Госдумы от фракции КПРФ В. Соловьёв предложил запретить российским солдатам публиковать в соцсетях фотографии и видео, сделанные во время учений и на территории военных частей. Об этом, ссылаясь на слова самого депутата, 30 июля сообщает газета «Известия».

По данным издания, В. Соловьёв уже начал работу над соответствующим законопроектом и готовит его к внесению в Государственную думу.

Предполагается, что запрет будет распространяться как на солдат, проходящих в армии срочную службу, так и на контрактников.

Если законопроект будет успешно внесён и утверждён парламентом, военнослужащим запретят размещать в социальных сетях фото и видеоролики, снятые во время нахождения в частях, в ходе учений, а также «изображения специальной техники и вооружения» и другую «внутреннюю армейскую информацию».

Как рассказал В. Соловьёв в комментарии «Известиям», на переписку и обмен сообщениями в соцсетях запрет распространяться не будет.

«Мы считаем нужным ограничить разрешение на пользование Интернетом для военнослужащих в целях недопущения попадания во всемирную сеть любой информации военного характера, поскольку она может быть использована западными СМИ в провокационных целях. Переписка в личных целях запрету не подлежит», – заявил В. Соловьёв.

По мнению депутата, ограничения на пользование соцсетями в армии востребованы, так как Россия находится «в условиях информационной войны» с неприятелем, использующим против неё «самые незначительные детали». О какой информационной войне и каком именно неприятеле идёт речь, В. Соловьёв не уточнил.

Информация о готовящемся законопроекте появилась в прессе спустя несколько дней после скандала вокруг фотографии артиллерийских оружий на границе с Украиной, размещённой во «ВКонтакте» российским солдатом-срочником В. Григорьевым.

Фото появилось в аккаунте В. Григорьева 23 июля и сопровождалось подписью «всю ночь долбили по Украине». Вскоре комментарий был отредактирован, а затем и вовсе удалён. Спустя некоторое время из соцсети исчезла и вся страница срочника.

24 июля в интервью телеканалу «Россия 24» В. Григорьев объяснил появление снимка на своей странице «взломом». По словам солдата, сам он во «ВКонтакте» не был уже «очень давно».

Похожие фото – снимки с подготовительных сборов, полигонов и даже карты перемещения военных частей из Ингушетии на границу с Донецкой областью – можно было обнаружить и на страницах других российских

солдат в Интернете. После попадания этих изображений в СМИ, все аккаунты, как и страница В. Григорьева, были удалены ***(Депутат Госдумы предложил запретить российским солдатам публиковать фото в соцсетях // InternetUA (http://internetua.com/deputat-gosdumi-predlojil-zapretit-rossiiskim-soldatam-publikovat-foto-v-socsetyah). – 2014. – 31.07).***

***

Радник міністра внутрішніх справ України А. Геращенко повідомив, що українські правоохоронні органи працюють над технічним питанням блокування акаунтів терористів у соціальних мережах – про це він розповів у програмі «Свобода слова» на ICTV, пише Українська правда.

«Щодо питання, пов'язаного з тим, щоб блокувати сторінки панів-терористів в Інтернеті. Це непросте питання технічно. У деяких країнах на це йшло кілька років. Ми зараз намагаємося це зробити за кілька місяців», – сказав А. Геращенко.

У який спосіб буде відбуватись блокування А. Геращенко не повідомив. Технічно це зробити майже не можливо, не маючи доброї волі з боку власників соцмереж. Адже блокувати по прямому посиланню конкретний акаунт не можливо, оскільки весь обмін інформації з соцмережами відбувається, як правило, через захищене з'єднання. Тобто лише соцмережа знає, які посилання відкриває користувач ***(Дмитренко О. Українські правоохоронні органи розробляють систему для блокування екаунтів терористів в соціальних мережах // UkrainianWatcher (http://watcher.com.ua/2014/07/29/ukrayinski-pravoohoronni-orhany-rozroblyayut-systemu-dlya-blokuvannya-ekauntiv-terorystiv-v-sotsialnyh-merezhah/). – 2014. – 29.07).***

***

В социальных сетях и средствах массой информации появилась информация о том, что 17 агуста в Новосибирске пройдет «Марш за федерализацию Сибири» под лозунгом «Хватит кормить Москву!». Об этом на своей странице в Facebook сообщил известный российский журналист А. Соломонов.

Кремль от таких заявлений пришёл в панику. Иначе не объяснить массовое закрытие доступа к этой информации Роскомнадзором. С 3 августа интернет-СМИ начали получать уведомления от своих провайдеров и хостинговых компаний о том, что на основании требования Генеральной прокуратуры Российской Федерации страница с новостью про сибирский марш и сибирскую республику ограничивается операторами связи на территории Российской Федерации. А ряд российских интернет-СМИ, кроме того, получили требования от Генпрокуратуры РФ удалить эту «вредную информацию».

По мнению российских прокуроров, информация содержит «призывы к массовым беспорядкам, осуществлению экстремистской деятельности или

участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка».

Предупреждения из-за Сибирского марша вынесены в общей сложности 14 СМИ, сообщил «Коммерсанту» пресс-секретарь Роскомнадзора В. Ампелонский. Список изданий, попавших под санкции, он не назвал. По данным NR Baltia, Роскомнадзор вынудил это сделать редакцию Slon.ru, Грани и др.

Под ограничения попали не только российские СМИ. Так известный оппозиционый сайт Беларуси «Хартия 97» сегодня написал, что американская хостинговая компания Amazon сообщила им о требовании российского Роскомнадзор ограничить доступ к «сибирской» статье. Редакция «Хартии 97» заявила, что «требование удалить новость является грубейшим нарушением Конституции Республики Беларусь».

Об этом же сообщает и украинское СМИ ТСН.

Между тем 4 августа в сетях появился новое подобное объявление только из Калининградской области. На фоне флаге Литвы «Калиннградская народная республика» объявляет сход на 15:00 под лозунгом «Хватит кормить Москву!»

Также NR Baltija стало известно о проведение 17 августа протестного марша по инициативе «Уральской республики». В закрытой анонимной сети TOR вовсю идёт обсуждение о призыве к уральцам «вспомнить времена Росселя и послать Кремль к чёрту».

Частные лица используют TOR для получения доступа к информации, заблокированной интернет-цензурой. Журналисты используют TOR для безопасного общения с информаторами и дисидентами ***(В сети начался процесс синхронизации протестных акций в России. Кремль в панике // «ХЕРСОН Онлайн» (http://khersonline.net/novosti/politika/27321-v-seti-nachalsya-process-sinhronizacii-protestnyh-akciy-v-rossii-kreml-v-panike.html). – 2014. – 4.08).***

***

Суд в США потребовал от интернет-гиганта Microsoft передать пользовательскую электронную переписку под контроль правительства страны. В настоящее время электронные письма хранятся на сервере компании в Ирландии.

Как отметила в своем вердикте председатель процесса, принципиальным для правительства является не место хранения, а возможность контроля над информационным потоком.

Решение суда не вступает в силу немедленно, оставляя Microsoft время на апелляцию.

При этом представители ряда других американских IT-компаний в ходе процесса приняли сторону интернет-гиганта.

«Нет ничего более важного, чем защита личной информации каждого пользователя вне зависимости от страны проживання», – заявил журналистам вице-президент телекоммуникационной корпорации AT&T У. Уоттс.

По словам экспертов в области информационных технологий, корпорации опасаются потерять миллиарды долларов на зарубежных рынках, если их клиенты заподозрят, что информация может попасть в руки правительству США и воспользуются услугами неамериканских фирм ***(Власти США хотят получить контроль над почтой Microsoft // InternetUA (http://internetua.com/vlasti-ssha-hotyat-polucsit-kontrol-nad-pocstoi-Microsoft). – 2014. – 1.08).***

***

В Крыму Сакский горрайсуд приговорил 30-летнего жителя к 1,5 годам лишения свободы условно, обвинив в «пропаганде нацизма в социальной сети».

Как сообщает «прокуратура» АРК, крымчанин признан виновным в совершении преступления, предусмотренного ч. 1 ст. 282 Уголовного кодекса Российской Федерации (возбуждение ненависти или вражды по признакам национальности, совершенные публично).

«Установлено, что тридцатилетний житель Сакского района, будучи приверженцем национал-радикальных взглядов, разместил на своей личной странице в социальной сети “ВКонтакте” текстовые и визуальные файлы, содержащие информацию, направленную на возбуждение ненависти и вражды к группе лиц, объединенных по признакам национальности, а также нацистскую атрибутику и символику», – говорится в сообщении.

При этом в так называемой прокуратуре не уточнили, какие именно это были материалы.

Примечательно, что главная линия российской пропаганды – приход к власти в Украине сторонников нацизма и националистов. Статью за пропаганду нацизма прокуроры-самозванцы могли использовать для разбирательств с неугодными жителями полуострова.

Глава Службы безопасности Украины В. Наливайченко советует соотечественникам быть более сдержанными в социальных сетях из-за вступления в силу в России так называемого закона о блогерах ***(Псевдовласти осудили крымчанина за пост ВКонтакте // InternetUA (http://internetua.com/psevdovlasti-osudili-krimcsanina-za-post-vkontakte). – 2014. – 1.08).***

***

Прокуратура Закарпатья сообщает об осуждении на три года условно местного жителя В. Сверлович, который в социальной сети Facebook распространял призывы к сепаратизму. Об этом передает «Укринформ».

«Состоялся суд над жителем Закарпатья В. Сверлович, который в социальной сети Facebook распространял призывы к сепаратизму.

Подсудимый вину полностью признал и заключил соглашение с прокурором, что таких действий он не будет делать. Согласно решению суда, он получил три года условно с отсрочкой приговора на один год», – сообщили в пресс-службе прокуратуры.

Осужденный является членом пророссийской так называемой «русинской» организации. Вместе с тем, следственным отделом Службы безопасности Украины в Закарпатской области закончено досудебное расследование уголовного производства в отношении еще одного жителя Закарпатья, который публично призвал к насильственному свержению конституционного строя и захват государственной власти в Украине.

«Обвинительный акт в указанном уголовном производстве направлено в Ужгородский горрайонный суд для рассмотрения», – сообщили в СБУ. Напомним, в городе Берегово (Закарпатская область) милиция задержала бывшего жителя Горловки (Донецкая область), который распространял идеи сепаратизма в видеохостинге YouTube ***(Член «русинской» организации Закарпатья получил три года условно за распространение сепаратизма в Facebook // IT Expert (http://itexpert.org.ua/rubrikator/item/37375-chlen-rusinskoj-organizatsii-zakarpatya-poluchil-tri-goda-uslovno-za-rasprostranenie-separatizma-v-facebook.html). – 2014. – 4.08).***

***

Компания The Tor Project, занимающаяся разработкой программного обеспечения Tor, позволяющего интернет-пользователям скрывать свое местонахождение, на 47 % увеличила расходование бюджетных средств США на свои нужды, сообщает CNews.RU.

В 2013 г. Tor Project в общей сложности получил правительственные гранты на сумму 1,82 млн дол. по сравнению с 1,24 млн дол. в 2012 г.

Из этой суммы 882,3 тыс. дол. были выделены Госдепартаментом США, 830,3 тыс. дол. – Министерством обороны США, 100,3 тыс. дол. – Национальным научным фондом при правительстве США и 10 тыс. дол. – Агентством США по международному развитию.

В 2012 г. основным источником финансирования стало Министерство обороны (876,1 тыс. дол.), при этом Госдепартамент выделил 353,6 тыс. дол. Таким образом, в 2013 г. Госдепартамент увеличил расходы на Tor в 2,5 раза. В общей сложности на федеральные власти США пришлось 60 % всего финансирования проекта за 2012 г.

Принцип работы сети Tor заключается в прокладывании запутанного маршрута от интенет-ресурса к компьютеру пользователя. На протяжении маршрута информация проходит через несколько ретрансляторов. При этом на каждом ретрансляторе находится только адрес предыдущего узла и адрес последующего узла – ни на одном ретранслятор не находится полная информация о маршруте и, таким образом, перехватчик не может отследить исходный и конечный пункты передачи данных.

Проект Tor был запущен в 1990-х годах Научно-исследовательской лабораторией ВМС США с целью разработки технологии защиты каналов правительственной связи. В 2001 г. благодаря усилиям двух студентов Массачусетского технологического института технология стала доступна гражданам. В 2005 г. правительство США выделило первый грант проекту, стремясь сделать технологию доступной широким массам. А с 2006 г. проект был преобразован в некоммерческую организацию.

В правительстве США заявили, что заинтересованы в развитии проекта, так как он способен сохранить жизни интернет-пользователей в таких странах, как Иран и Сирия, чтобы они могли без опаски высказывать свое мнение о действующем политическом режиме.

Технология Tor используется в качестве основы в операционной системе Tails, которую использует для конфиденциальной работы Э. Сноуден, бывший системный администратор АНБ и ЦРУ, раскрывший информацию о деятельности американских спецслужб ***(США на 47 % увеличили расходы на анонимную сеть Tor // InternetUA (http://internetua.com/ssha-na-47--uvelicsili-rashodi-na-anonimnuua-set-Tor). – 2014. – 31.07).***

***

За первые шесть месяцев текущего года правительство США направило Twitter на 48 % запросов раскрыть информацию пользователей больше, чем за аналогичный период 2013 г. Соответствующие данные содержатся в «Отчете прозрачности» (Transparency Report) компании.

В Twitter говорят, что все запросы были отправлены в связи с ведущимися криминальными расследованиями.

Наибольшее количество запросов (61 %, что на 2 % больше, чем годом ранее) было отправлено в отношении пользователей из США. На втором месте оказалась Япония с показателем в 9 % (на 6 % меньше, чем в первой половине 2013 г.). Вслед за ними в документе отмечаются Бразилия и Великобритания с одинаковым показателем в 4 %.

По информации Twitter, количество запросов в отношении пользователей из Бразилии, Турции и Испании возросло более чем в два раза. Более того, по сравнению со вторым полугодием 2013 г. показатель Бразилии увеличился в три раза.

В компании увеличившееся количество запросов объясняют тем фактом, что платформа микроблогов становится все более популярной по всему миру.

В 72 % случаев запросов касательно американских пользователей Twitter предоставила «некоторую информацию». В Великобритании этот показатель составил всего 46 % ***(Количество правительственных запросов в отношении Twitter возросло на 48 % // InternetUA (http://internetua.com/kolicsestvo-pravitelstvennih-zaprosov-v-otnoshenii-Twitter-vozroslo-na-48). – 2014. – 3.08).***

***

В Великобритании ряд вузов займется подготовкой кибершпионов. Центр правительственной связи (ЦПС) страны выдал соответствующую аккредитацию шести учебным заведениям. Об этом сообщает BBC News.

Секретарь Кабинета министров Ф. Мод заявил, что кибербезопасность стала важнейшей частью плана правительства для британской экономики. По его словам, специалисты в области кибероборонs и обеспечения безопасности данных помогут сделать Великобританию «одной из самых безопасных в мире страной для онлайн-бизнеса».

«Работа ЦПС совместно с другими государственными ведомствами, частным сектором и научными кругами, позволит противостоять угрозам и гарантировать, что вместе мы сильнее и лучше осведомлены», – добавил Ф. Мод.

В список аккредитованных учебных заведений вошли Оксфордский университет, университет Ланкастера, Лондонский университет и Эдинбургский университет. Также читать курсы по информационной безопасности и кибероборонe разрешили в Крэнфилдском и Суррейском университетах ***(В вузах Великобритании займутся подготовкой кибершпионов // InternetUA (http://internetua.com/v-vuzah-velikobritanii-zaimutsya-podgotovkoi-kibershpionov). – 2014. – 3.08).***

***

Специалисты российской организации «Лига безопасного Интернета» разработали механизм предварительной фильтрации Интернета.

Организация предлагает проверять все сайты на предмет «нежелательного содержания» прежде, чем допустить пользователя к просмотру страницы. Об этом говорится в сообщении на сайте «Лиги безопасного Интернета», пишут «Подробности».

«Мы предлагаем ввести предустановленную фильтрацию Интернета, которая позволяет автоматически, в режиме реального времени определять содержимое страницы, запрашиваемой пользователем. Система оценивает содержимое страницы и определяет категорию, к которой относится информация. В случае, если категория является запрещенной, система автоматически блокирует интернет-страницу», – рассказал исполнительный директор организации Д. Давыдов.

В настоящее время контроль Интернета в России осуществляется путем внесения сайтов с нежелательным содержанием в «черный список» Роскомнадзора ***(Российские специалисты уже научились фильтровать интернет // From-UA (http://www.from-ua.com/news/317529-rossiiskie-specialisti-uzhe-nauchilis-filtrovat-internet.html). – 2014. – 5.08).***

***

Всего несколько дней назад Tor объявила о том, что личности многих пользователей сервиса, посещавших скрытые страницы, могли быть

взломаны. Теперь издание Wired сообщает, что ФБР уже давно проводит кампанию по идентификации пользователей Tor, устанавливая вредоносное ПО на их компьютеры.

Как пишет бывший хакер К. Поульсен, проблему стоит рассматривать с разных сторон. С одной стороны, трудно спорить с тем, что делает ФБР. Так называемые «сетевые методы расследования», применяемые бюро, чтобы получить несанкционированный доступ к компьютерам пользователей, их местоположению и истории веб-поиска, бесспорно включают в себя использование вредоносных программ. ФБР использует сайты с высоким трафиком для того, чтобы заразить вредоносным ПО большее количество компьютеров.

Тем не менее, ФБР до сих пор придерживалась вышеупомянутой политики с целью найти людей, которые торгуют детской порнографией на многих сайтах, не индексируемых поисковыми системами. Так, К. Поульсен сообщает, что дела более десятка предполагаемых пользователей сайта с детской порнографией на базе Tor теперь направлены в суд.

Неясно, подпали ли под суд невинные пользователи, однако вполне вероятно, что ФБР продолжит использовать данную технику для поимки нарушителей в сети ***(ФБР заражает компьютеры пользователей Tor // InternetUA (http://internetua.com/fbr-zarajaet-kompuateri-polzovatelei-Tor). – 2014. – 7.08).***

***

Загальнодоступні сайти в Росії, у тому числі соціальні мережі, повинні підключити обладнання, за допомогою якого спецслужби і правоохоронні органи здійснюють оперативно-розшукову діяльність.

Така вимога міститься в постанові, яку 31 липня підписав прем'єр-міністр Росії Д. Медведєв. Інтернет-ресурси будуть зобов'язані впроваджувати обладнання згідно з планом заходів, розроблених ФСБ. Адміністраціям сайтів забороняється розкривати «організаційні та технічні прийоми проведення оперативно-розшукових заходів», повідомляють «Грани».

Ідеться про програмне забезпечення, яке дає змогу спецслужбам отримувати інформацію про дії користувачів сайтів. За цією схемою працює Система технічних засобів для забезпечення функцій оперативно-розшукових заходів (СОРЗ), яку зобов'язані за свій рахунок встановлювати російські оператори зв'язку.

У постанові також повідомляється, що «функціонування технічних засобів і програмного забезпечення забезпечує організатор поширення інформації».

За допомогою системи СОРЗ, встановленої у російських провайдерів, спецслужби вже зараз можуть отримати інформацію про все, що користувачі роблять в Інтернеті. Однак через операторів зв'язку йде занадто великий обсяг інформації, у зв'язку з чим процес пошуку конкретного відправника

через цю систему ускладнюється. На думку експертів, встановлення СОРЗ у соціальних сервісах полегшить спецслужбам пошук людей, які написали той чи інший текст.

Інтернет-компанії не знали про підготовку постанови. У «Яндексі» РБК повідомили, що документ був присутній у первісному переліку підзаконних актів, але його текст не обговорювався з галуззю і ніде не публікувався.

У Mail.ru Group підтвердили, що обговорення постанови не проводилося. За словами керівника юридичного департаменту Mail.Ru Group А. Мальгінова, документ викликає у компанії питання про те, що тепер потрібно робити, і в яку суму обійдеться компанії взаємодія із спецслужбами та правоохоронними органами ***(Російські сайти і соцмережі повинні встановити обладнання для прослуховування // Ipress.ua (http://ipress.ua/news/rosiyski_sayty_i_sotsmerezhi_povynni_vstanovyty_obladnannya_dlya_prosluhovuvannya_78786.html). – 2014. – 7.08).***

***

Правительство Китая обяжет пользователей популярных средств мгновенного обмена сообщениями использовать реальные имена для регистрации. Помимо этого, журналисты, желающие размещать политические новости, будут обязаны проходить процесс предварительного одобрения. Об этом сообщает сразу ряд китайских источников.

В 2013 г. правительство Китая усилило контроль за Интернетом. Среди принятых государством мер значилось блокирования тысяч учетных записей пользователей Weibo – китайского аналога социальной сети Twitter.

Новые ограничения затронут пользователей мобильных приложений для мгновенного обмена сообщениями. В качестве примера можно привести WeChat разработки Tencent Holdings, которым пользуются 400 млн человек.

Пользователи, не получившие одобрения, более не смогут размещать на своих страницах политические новости, а также делиться ими. Чтобы получить разрешение, потребуется обратиться к команде разработчиков приложения.

Помимо этого, в пользовательские соглашения будет добавлен пункт, согласно которому пользователи обязуются «соблюдать действующие законы и социалистические устрои, защищать национальные интересы и законные права граждан, придерживаться общественной морали и обеспечивать подлинность размещаемой информации».

Новые правила могут отрицательно повлиять на развитие сервисов обмена сообщениями. Когда в прошлом году Китай ввел ограничения в отношении сервиса Weibo, количество пользователей социальной сети резко сократилось.

По мере роста популярности приложений наподобие WeChat Коммунистическая партия Китая стремится достичь все большего контроля над ними. В качестве аналога можно привести действия правительства РФ, с каждым годом пытающегося усилить свой контроль над Рунетом ***(В Китае***

***ввели новые ограничения для средств мгновенного обмена сообщениями // InternetUA (http://internetua.com/v-kitae-vveli-novie-ogranicseniya-dlya-sredstv-mgnovennogo-obmena-soobsxeniyami). – 2014. – 7.08).***

***

Спустя несколько минут после того как борт MH-17 Malaysia Airlines упал в Донецкой области, аналитик Разведывательного управления Минобороны США, который просматривал сообщения в социальных медиа, нашел ценную информацию, пишет The Wall Street Journal.

«Этот аналитик, владеющий русским языком, увидел в российской сети "ВКонтакте" пост пророссийских сепаратистов в Украине, где утверждалось, что они сбили украинский военно-транспортный самолет», – пишет журналист Д. Барнс.

«Первые признаки, указывающие на то, кто его сбил, чем он был сбит, где и когда он был сбит, появились исключительно в социальных сетях, – заявил генерал-лейтенант М. Флинн, глава РУМО, описавший в интервью работу его отдела – Центра Европы и Евразии. – Это произошло буквально через несколько минут».

По словам генерала М. Флинна и других американских официальных лиц, за последние полтора года США вложили много средств в способы сбора и изучения постов в Facebook, Twitter и зарубежных региональных соцсетях. По их словам, эти методы смогут произвести революцию в сборе разведданных в открытых источниках.

Чиновники говорят, что их компьютеры могут агрегировать материалы из множества социальных медиа и просматривать огромные массивы информации, находящейся в публичном доступе, чтобы выявлять тенденции и связи.

М. Флинн добавил, что данные соцсетей помогают отслеживать кризис в секторе Газа, террористические группировки и приказы африканских полевых командиров (они отдают распоряжения в публичных постах).

Инструменты нового поколения позволяют США выискивать тенденции и тревожные признаки потенциальных кризисов в области национальной безопасности. Разведки сосредотачиваются на постах, выложенных в заданный период времени из заданного географического района (от участка в несколько квадратных миль до целой страны или континента), передает издание.

Аналитики также могут выявить связи автора некой записи с другими пользователями соцсети, а также установить физическое местонахождение его контактов.

«Социальные медиа – новая форма радиотехнической разведки», – заключил генерал М. Флинн.

РУМО также разработало программу, которая находит в социальных медиа изображения конкретных людей. Как утверждает автор, был взят снимок «военного в российской форме на базе ВМФ в Новороссийске в

сентябре 2013 г.». «Затем на протяжении 8 дней серия публичных постов в социальных медиа продемонстрировала, как этот военный перемещался по Краснодарскому краю, а в марте появился в Крыму», – говорится в статье ***(Пентагон мониторит «ВКонтакте» для поиска террористов // InternetUA (http://internetua.com/pentagon-monitorit--vkontakte--dlya-poiska-terroristov). – 2014. – 8.08).***

## Проблема захисту даних. DDOS та вірусні атаки

Официальный сайт Президента Украины подвергся DDoS-атаке. Об этом сообщили в Государственной службе специальной связи и защиты информации.

В ведомстве обещали обнародовать более подробную информацию об инциденте позднее.

В течение как минимум последнего часа сайт Президента не загружается.

В то же время в социальной сети Facebook появилась информация некой организации «Киберберкут», которая сообщает о своей причастности к блокировке президентского веб-ресурса. В своем сообщении они поблагодарили сотрудников Госспецсвязи за содействие.

При этом в Госспецсвязи опровергли сотрудничество с организацией ***(Хакеры атакуют сайт Президента Украины // Главком (http://glavcom.ua/news/223210.html). – 2014. – 29.07).***

***

28 липня на сайт Тернопільської ОДА було здійснено вірусну атаку. Як наслідок, адміністрування сайтом стало неможливим.

Як пише Тернопільінфо, очевидними є наміри зловмисника – не давати можливості розповідати про діяльність ОДА. На думку видання, мета злому сайту – видалення інформації про діяльність попередніх голів ОДА, тобто знищення архіву публікацій ***(Владу Тернопільщини атакували віруси // За Збручем (http://zz.te.ua/vladu-ternopilschyny-atakuvaly-virusy/). – 2014. – 28.07).***

***

Україна стала полем віртуальних атак армії кремлівських кіберсолдатів – Le Figaro

22 червня 2014 р. питання, задане Le Figaro своїм читачам про відповідальність Росії за крах малазійського літака, викликав небувалий потік відповідей з Росії та України, при цьому користувачі Інтернету переважною більшістю проголосували за їх версією подій. Питання в тому, хто головні дійові особи в цій ілюстрації розгортання українського конфлікту

в мережі. Про це йдеться в аналітичній статті під назвою «Кіберпропаганда: Україна стала полем віртуальних бойових дій», опублікованій у французькій газеті Le Figaro, де О. Моренкова-Пер'є, доктор політичних наук, описує стратегію розвитку пропаганди 2.0, яку використовує Москва.

Кібер солдати Кремля?

Після приголомшливого провалу російських засобів комунікації під час «п'ятиденної війни» між Росією і Грузією у 2008 р., уряд Росії усвідомив, наскільки важливо керувати думками в Інтернеті, у тому числі на міжнародному рівні. У липні 2014 р. у розпал української кризи, анонімна російська група розповіла про існування «Агентства інтернет-досліджень». Як свідчить листування власника цього агентства, отримане в результаті хакерської атаки, близько 600 блогерів і коментаторів, які отримують зарплату, щодня працюють у соціальних мережах і в електронних засобах масової інформації, у тому числі західних країн, впливаючи на думки користувачів Інтернету. З початку української кризи журналісти насправді помітили, що кількість проросійських коментарів, які написані за одним і тим же зразком, набагато збільшилася. Модератори сайту The Guardian, наприклад, обробляють по 40 тис. проросійських коментарів на день, щоб відфільтрувати повідомлення тролів. Якщо навіть цю інформацію підтвердять результати дослідження, яке проводить незалежна «Нова газета» про «Армії тролів Кремля», і якщо російська влада ніколи не спростовували інформацію про існування кібербригад, все ж мобілізацію такого типу не завжди починають і направляють зверху. У випадку з Le Figaro, наприклад, мобілізація була ініційована користувачами соціальної мережі «ВКонтакте» і лідерами «Антимайдану» у Twitter.

Війна хакерів

Ця інформаційна війна ведеться одночасно з кібервійною між проукраїнськими і проросійськими хакерами. Варто згадати, що дві перші великомасштабні кібератаки на сайти естонських та грузинських інституцій здійснили у 2007 і 2008 р. за участі Росії. Сьогодні дві головні мережі хакерів, що беруть участь в українському конфлікті, Кіберсотня з української сторони та Кіберберкут з російської, символізують протистояння між активістами Майдану (яких називають «Небесна сотня») та загоном «Беркут», який займався розгоном демонстрантів за наказом В. Януковича.

У той час як проукраїнські хакери відзначилися тим, що атакували сайт «Російської газети», офіційної газети російського уряду, у березні 2014 р., проросійські хакери заблокували в березні близько 150 українських сайтів, а також сайти НАТО і деяких приватних американських охоронних агентств, таких як Academy.

Діапазон дії проросійських хакерів дуже широкий (DDoS-атаки, хакерські атаки і публікація електронного листування і телефонних розмов), їхня тактика не змінилася з 2008 р. Вона полягає в тому, щоб за допомогою патріотичних промов спонукати новачків брати участь у кібервійні, надаючи їм шкідливі програми, щоб допомогти їм здійснювати анонімні атаки, що дає

змогу постійно збільшувати кількість «кіберсолдат» і забезпечувати їх усім необхідним.

Наскільки залучена насправді російська влада в цю війну? Навіть якщо Д. Карр, експерт із кібербезпеки, під час своїх досліджень мережі російських хакерів у 2008 р. не знайшов доказів прямої чи непрямої участі російської влади, цілком ясно, що Кремль не перешкоджає діям хакерів. Хоча атаки здійснюються за ініціативою приватних осіб, уряд їх підтримує, але тримає дистанцію, достатню для того, щоб можна було заперечувати свою участь, користуючись при цьому стратегічною перевагою, яку він отримує ***(Україна стала полем віртуальних атак армії кремлівських кіберсолдатів – Le Figaro // Інформаційний портал «Стик» (http://styknews.info/novyny/polityka/2014/07/28/ukraina-stala-polem-virtualnykh-atak-armii-kremlivskykh-kibersoldativ-le-). – 2014. – 28.07).***

***

Неизвестные злоумышленники взломали облачный сервис Amazon Cloud и загрузили на его серверы троянца Mayday, выполняющего DDoS-атаки на определенные сайты. Это стало возможно благодаря использованию уязвимости в устаревшей версии Elasticsearch, установленной на серверах Amazon.

Elasticsearch – поисковое ПО, позволяющее приложениям выполнять полнотекстовый поиск различных документов. Благодаря своей распределенной архитектуре программа пользуется большим спросом среди облачных сервисов. Поисковик можно успешно развернуть на таких платформах, как Amazon Elastic Compute Cloud (EC2), Microsoft Azure, Google Compute Engine и подобных им.

Начиная с версии 1.1.x, Elasticsearch получил поддержку активного использования скриптов через вызовы API в конфигурации по умолчанию. Эта функция представляет собой угрозу безопасности, поскольку ее использование не требует аутентификации и скриптовый код не исполняется в безопасном окружении.

Уже сообщалось, что злоумышленники могут эксплуатировать скриптовые возможности Elasticsearch для выполнения произвольного кода на основном сервере. Разработчики программы выпустили обновление 1.2.0, исправляющее уязвимость CVE-2014-3120 и отключающее динамический скриптинг. Несмотря на это, Amazon отказались перейти на обновленную версию Elasticsearch.

По данным К. Баумгартнера из «Лаборатории Касперского», существует новый вариант Mayday. Троянец, направленный на пользователей Linux, используется для DDoS-атак и поддерживает несколько технологий для их совершения, включая DNS-амплификацию. Эта модификация Mayday была обнаружена на одном из серверов Amazon EC2.

По словам К. Баумгартнера, преступники получили доступ к серверам EC2, используя уязвимость CVE-2014-3120. Хоть она и была исправлена в

Elasticsearch 1.2.x и 1.3.x, некоторые организации до сих пор используют устаревшие версии 1.1.x.

Исследователям из «Лаборатории Касперского» удалось понаблюдать за ранними стадиями атак на серверы под управлением EC2. По их словам, взломщики использовали находящийся в открытом доступе код, эксплуатирующий уязвимость CVE-2014-3120, чтобы установить на уязвимые серверы бэкдор-скрипт, позволяющий злоумышленникам удаленно выполнять команды через сеть.

Модифицированный вариант Mayday, заразивший EC2-сервера, не использовал DNS-амплификацию. Вместо этого использовалось наполнение UDP-трафиком. Это привело к тому, что подверженные атаке жертвы (среди которых был крупный региональный банк в США и японский производитель электроники) сменили свои IP-адреса и подключили защиту от DDoS-атак.

«Поток оказался достаточно мощным для того, чтобы Amazon оповестил своих клиентов о происходящем. Вероятно, другие облачные сервисы испытывают те же трудности», сказал К. Баумгартнер.

Пользователям Elasticsearch 1.1.x рекомендуется как можно скорее установить обновление 1.2 или 1.3, которое исправляет эту уязвимость. Для тех, кто планирует и дальше использовать скриптовые функции программы, разработчики выпустили рекомендации безопасности ***(Хакеры внедрили DDoS-ботов на Amazon Cloud, эксплуатируя уязвимость в Elasticsearch // UVO.SU (http://uvo.su/biblio/inform_zachita/hakery-vnedrili-ddos-botov-na-amazon-cloud-ekspluatiruya.html). – 2014. – 29.07).***

***

В анонимной сети Tor обнаружена уязвимость, позволяющая полностью деанонимизировать любого пользователя.

Уязвимость выявили в начале июля 2014 г. два независимых эксперта из Университета Карнеги Мелон, США, А. Волынкин и М. Маккорд.

Все детали уязвимости пока что держатся в тайне, поскольку администрация Tor ещё не устранила данную брешь.

Над исправлением ошибки работает один из создателей Tor Р. Дингледин. Согласно его заявлению, обнаруженная брешь – это «проблема, но не конец света».

Ранее Министерство внутренних дел РФ объявило закрытый конкурс на исследование возможности получения технической информации о пользователях анонимной сети Tor.

Соответствующая заявка появилась на российском сайте госзакупок. На взлом государство готово выделить 3,9 млн рос. р. – около 112 тыс. дол. Заявки для участия в конкурсе будут приниматься до 13 августа, а итоги будут подведены 20 августа 2014 г.

Исследователи установили, что за минувший год украинские пользователи начали активнее использовать анонимную сеть Tor, чтобы обеспечить себе инкогнито в онлайне ***(Коваль М. В Tor нашли опасную***

***уязвимость, угрожающую анонимности // Блог Imena.UA (http://www.imena.ua/blog/tor-july-danger/). – 2014. – 28.07).***

***

Представители анонимной сети Tor заявили 30 июля, что личности многих пользователей сервиса, посещавших скрытые страницы, могли быть обнаружены финансируемыми правительством исследователями.

В записке на сайте некоммерческой организации лидер проекта Tor Р. Динглдайн сказал, что сервис определил в своей сети компьютеры, которые вносили изменения в трафик Tor в течение пяти месяцев в попытке разоблачить пользователей, подключающихся к «скрытым сервисам». Последние включают в себя подпольные сайты по продаже наркотиков, такие как заблокированный веб-ресурс Silk Road, а также SecureDrop, который предназначен для безопасного обмена информацией между СМИ и информаторами.

Р. Динглдайн сказал, что, скорее всего, это кибернападение было совершено с компьютеров, изъятых из сети 4 июля 2014 г. Они находились под управлением двух исследователей из Института технологий разработки программного обеспечения (Software Engineering Institute), который финансируется Департаментом обороны США.

Остается неясным, какое количество личных данных смогли собрать ученые и как они используют эту информацию ***(Tor предупреждает пользователей о кибернападении // InternetUA (http://internetua.com/tor-preduprejdaet-polzovatelei-o-kibernapadenii). – 2014. – 31.07).***

***

Как сообщил эксперт из компании Offensive Security М. Ахарони изданию Network World, в антивирусном продукте Symantec Endpoint Protection обнаружены три уязвимости нулевого дня. Эксплуатация брешей позволяет авторизованному пользователю повысить привилегии на системе и получить более высокий уровень доступа.

Уязвимости были обнаружены в ходе тестирования безопасности одной из финансовых компаний. Во вторник, 29 июля, эксперты из Offensive Security опубликовали видеоролик, демонстрирующий успешную эксплуатацию брешей. Подробности о них будут раскрыты на конференции хакеров Black Hat, которая состоится в следующем месяце в Лас-Вегасе.

По словам М. Ахарони, уязвимости позволяют авторизованному пользователю получить более широкий доступ к системе, что дает возможность осуществления других атак, таких как дамп хэшей или идентификации кэша учетных данных администраторов домена.

В процессе тестирования на проникновение эксперты не были нацелены на Endpoint Security, однако подчеркнули, что бреши могут привести к катастрофическим последствиям для финансовой компании.

Эксперты уведомили о брешах Компьютерную группу реагирования на чрезвычайные ситуации (Computer Emergency Response Team, CERT). В Symantec пока никак не прокомментировали факт обнаружения уязвимостей ***(В антивирусном продукте Symantec Endpoint Protection обнаружены уязвимости нулевого дня // InternetUA (http://internetua.com/v-antivirusnom-produkte-Symantec-Endpoint-Protection-obnarujeni-uyazvimosti-nulevogo-dnya). – 2014. – 31.07).***

***

В Интернете завелся новый вирус, который выдает себя за видео, якобы выложенное от имени друзей в Facebook. От действия хакеров пострадали уже более 800 тыс. пользователей.

Ссылка на вирус приходит в электронном письме или личном сообщении в Facebook, уведомляющим, что кто-то отметил человека на видео. После перехода по незнакомому URL-адресу пользователя просят скачать «плагин» для браузера, чтобы можно было посмотреть ролик. После того как вредоносное ПО попадет на компьютер, злоумышленники получают доступ к любой информации, хранящейся в браузере, в том числе аккаунтам и паролям в Facebook, Twitter и других соцсетях.

Избавиться от «расширения» не так легко, т. к. оно блокирует доступ к настройкам браузера и запрещает переходить на сайты антивирусных компаний. По мнению исследователей, которые судят по комментариям в коде, вирус создали хакеры из Турции.

Распространяется он довольно быстро – со скоростью 40 тыс. атак в час, и успел заразить свыше 800 тыс. человек, пользующихся Chrome. Компания Google, разработчик браузера, осведомлена об атаке и уже заблокировала «плохой» плагин. Facebook также занимается чисткой ссылок на вирус ***(Новый компьютерный вирус «поразил» более 800 тысяч пользователей Facebook // InternetUA (http://internetua.com/novii-kompuaternii-virus--porazil--bolee-800-tisyacs-polzovatelei-Facebook). – 2014. – 30.07).***

***

Исследование публично доступных веб-серверов, принадлежащих крупнейшим мировым организациям, показало, что только 3 % машин были полностью защищены от уязвимости в OpenSSL, также известной как Heartbleed.

Специалисты компании Venafi Labs проверили 550 тыс. серверов, принадлежащим 1639 компаниям, значащимся в списке 2000 крупнейших предприятий. Оказалось, что 99 % проверенных компаний применили обновление, исправляющее критическую уязвимость Heartbleed.

Но лишь на 15 000 серверов были изменены личные ключи, отозваны старые сертификаты SSL и выданы новые. Учитывая то, что Heartbleed можно использовать для извлечения личных ключей из памяти уязвимого

компьютера, можно считать, что ключи и сертификаты серверов также были скомпрометированы.

«Устранять последствия инцидента не так просто, как кажется, – говорит К. Бочек, вице-президент стратегии безопасности и отслеживания киберугроз Venafi Labs. – Одной лишь установкой обновления в данном случае не обойтись».

К. Бочек отметил, что брешь в OpenSSL активно эксплуатировалась в течение двух лет перед тем, как ее обнаружили в апреле 2014 г. В течение этого времени злоумышленники могли получать не только пароли, но и ключи шифрования и данные сертификатов.

По словам специалиста, еще хуже дела обстоят среди закрытых серверов, поскольку в большинстве случаев на них даже не устанавливали исправление, устраняющее уязвимость ***(Только 3 % web-серверов полностью защищены от последствий Heartbleed // InternetUA (http://internetua.com/tolko-3--web-serverov-polnostua-zasxisxeni-ot-posledstvii-Heartbleed). – 2014. – 30.07).***

***

Исследователь безопасности М. Ахмед обнаружил критическую уязвимость в приложении Instagram для Android, позволяющую атакующему взломать учетную запись пользователя, получить контроль над управлением и публикацией фотографий, а также редактировать и удалять комментарии.

Приложение соединяется с сервером через незашифрованный протокол HTTP, который может быть изменен злоумышленником с целью перехвата. М. Ахмед использовал программу на своем смартфоне, осуществляя при этом мониторинг трафика с помощью анализатора WireShark. Эксперт обнаружил, что соединение уязвимо к перехвату пользовательской сессии, осуществляемой с помощью атаки «человек посередине».

Повторное использование перехваченных HTTP cookie сессии на другой системе или браузере позволяет злоумышленнику взломать сессию в учетной записи жертвы в Instagram.

«Как только я вошел в учетную запись в Instagram на своем телефоне, WireShark перехватил незашифрованные данные, проходящие через HTTP. Эти данные включали в себя фотографии, просматриваемые жертвой, cookie сессии, имя пользователя и ID», – сообщил М. Ахмед.

Эксперт уведомил Facebook, владеющую Instagram, о бреши. Представители компании сообщили о переводе сервиса на протокол HTTPS, однако пока неизвестно, как скоро это произойдет ***(Обнаружена критическая уязвимость в приложении Instagram для Android // InternetUA (http://internetua.com/obnarujena-kriticseskaya-uyazvimost-v-prilojenii-Instagram-dlya-Android). – 2014. – 29.07).***

***

Исследователи из Китайского университета Гонконга сообщили о возможности осуществления потенциальных атак на Android-устройства с помощью встроенного модуля голосового помощника Google Voice Search и динамика. В качестве доказательств своей теории эксперты создали вредоносное приложение, получившее название VoicEmployer.

Использование голосового помощника для осуществления атак действительно очень удобно. Так, если для прослушки и скриншотов с помощью микрофонов и камер вредоносному ПО необходимо специальное разрешение, то голосовой помощник такового не требует. Как известно, запрос на разрешение намного повышает риск для вредоноса быть обнаруженными.

По словам исследователей, атака осуществляется следующим образом: при низком уровне громкости VoicEmployer посылает Voice Search команду «набрать номер» (определенный заранее). Затем телефон, независимо от вмешательства пользователя, набирает номер и передает конфиденциальную информацию лицу на другом конце, которое задает такие вопросы, как «где я нахожусь?» и т. д. Злоумышленник также может использовать голосовые команды для отправки почты, текстовых сообщений, прослушивать голосовую почту и пр.

Вредонос можно использовать в «тихом режиме» для того, чтобы избежать обнаружения пользователем. При этом уязвимыми к подобным атакам могут быть практически все Android-устройства, использующие Google Services Framework ***(Атаки на Android-устройства можно осуществлять с помощью голосового помощника // InternetUA (http://internetua.com/ataki-na-Android-ustroistva-mojno-osusxestvlyat-s-pomosxua-golosovogo-pomosxnika). – 2014. – 1.08).***

***

На образах популярных героев сегодня зарабатывают не только издательства и лицензионные компании, но и хакеры. Мошенники используют поисковые системы в преступных целях: через популярные «термины» поиска – цепляющие слова – привлекают внимание жертвы: светские сплетни, праздники, популярные хиты и, конечно же, супергерои.

Эксперты компании McAfee выяснили, какие супергерои являются самыми опасными в этом году.

Используя рейтинги McAfee® SiteAdvisor®, они определили, какие герои чаще всего приводят пользователей на опасные сайты. Результаты показали, что поиск по запросам «Супермен», «Супермен загрузить бесплатно с торрента», «Супермен смотреть», «Супермен бесплатные приложения», а также «Супермен онлайн» с вероятностью 16,5 % может закончиться посещением сайта с такими угрозами, как шпионские программы, спам, фишинг, вирусы и др.

Вторым по «опасности» является Тор (Thor), следом за ним – Чудо Женщина (Wonder Woman) и Аквамэн (Aquaman), Росомаха (Wolverine), Спайдермен (Spiderman), Бэтмен (Batman) и другие.

Чтобы защитить себя от мошенников, эксперты McAfee рекомендуют, в первую очередь быть бдительными: «Если поиск выдает ссылку с доступом к бесплатному контенту или к слишком хорошему предложению, чтобы быть правдой, не открывайте. Дважды проверьте веб-адрес: будьте внимательны к неправильному написанию адреса или других элементов, которые могут подсказать, что сайт небезопасен» ***(Эксперты: Фильмы про супергероев могут заразить ваш компьютер // InternetUA (http://internetua.com/eksperti--filmi-pro-supergeroev-mogut-zarazit-vash-kompuater). – 2014. – 1.08).***

***

Устройства с USB-разъемом – флешки, мышь, клавиатура – могут использоваться для взлома компьютера, утверждают специалисты по безопасности из SR Labs. И дело вовсе не в том, что на флеш-носителе будет записано вредоносное ПО. Новый потенциальный класс атак, против которого бесполезны существующие средства защиты, обнаружили К. Нол и Я. Лелл из берлинской SR Labs, сообщает Iksmedia.

Проблема здесь более глубокая, связанная с самим принципом работы USB-устройств, рассказали эксперты. Имеющиеся в них контроллеры – микросхемы, управляющие их работой, – могут быть перепрограммированы, а вредоносный код скрыт, после чего он будет заражать компьютеры, к которым подключат эти устройства, поясняют исследователи. Речь идет о любых мобильных и настольных операционных системах. Что существенно, на самих микросхемах исходно не предусмотрены никакие средства защиты кода. «Вы не сможете определить, откуда взялся вирус, – говорит К. Нол. – Это почти магический трюк».

Исследователи из SR Labs провели опыты с такими атаками, записав собственный вредоносный код (они назвали его BadUSB) на USB-микросхемы для флешек и смартфонов. Будучи подключено к компьютеру, перепрограммированное USB-устройство может эмулировать клавиатуру, выполнять команды от имени пользователя, например, удалять файлы или устанавливать программы. Записанный на нем вредоносный код может, в свою очередь, заражать другие устройства, которые будут подключены к тому же компьютеру. Наконец, он способен изменить настройки DNS компьютера, перенаправляя на внешний сервер поступающий на него трафик.

Исследователи собираются сделать доклад о новой угрозе, представив доказательства фундаментального нарушения безопасности USB, на предстоящей конференции Black Hat в Лас-Вегасе (их презентация будет называться Bad USB – On Accessories that Turn Evil).

По словам К. Нола, он бы не удивился, узнав, что разведывательные организации, к примеру National Security Agency, уже выяснили, как организовать такие атаки. Год назад, пишет Reuters, К. Нол представил на Black Hat результаты изучения методов удаленного взлома SIM-карт мобильных телефонов. А в декабре из данных, обнародованных Э. Сноуденом, выяснилось, что разведка использовала для слежки сходную технику.

Эффективной защиты против USB-атак пока нет, считают в SR Labs. Такие средства защиты, как антивирусы, сканируют только ПО, записанное в памяти компьютера, и не имеют доступа к прошивке, управляющей работой USB-устройств. Межсетевых экранов, блокирующих определенный класс устройств, пока не существует. Очистить зараженную систему также будет очень непросто.

В исследовании К. Нола и Я. Лелла есть один момент, полагают эксперты, который заставляет прислушаться к их выводам, не считая их просто рассуждениями теоретиков. Дело в том, что заражение может быть направлено в обе стороны: как от USB к компьютеру, так и обратно. Каждый раз, когда устройство включается в USB-порт компьютера, фирменное ПО на нем может быть переписано вредоносным кодом, находящимся на ПК, и владельцу устройства будет непросто это детектировать. Точно так же любое USB-устройство сможет заразить любой компьютер. «Это работает в обе стороны, – говорит К. Нол. – Доверять нельзя никому» ***(Хакеры научились взламывать компьютеры, заражая мыши и клавиатуры с USB-интерфейсом // InternetUA (http://internetua.com/hakeri-naucsilis-vzlamivat-kompuateri--zarajaya-mishi-i-klaviaturi-s-USB-interfeisom). – 2014. – 1.08).***

***

Новая особо опасная разновидность ransomware – вредоносных программ, целью которых является вымогательство денег под угрозой порчи важной информации – открыта фирмой Kaspersky Lab.

Получившее название Onion это ПО зашифровывает данные пользователей и использует анонимную сеть Tor для осуществления неотслеживаемого перевода электронных денег Bitcoin. По информации экспертов Касперского, в настоящее время вредоносная активность Onion ограничивается пользователями Windows из России и других восточноевропейских стран.

Ransomware это относительно новый тренд. Строго говоря, данное ПО нельзя рассматривать как вирус – это лишь программа, запускающаяся на чужом компьютере без ведома его владельца. Прежние его варианты отображали полноэкранную заставку с инструкциями по переводу денег, препятствующую запуску других программ и сохраняющуюся даже после перезагрузки. Разработчики антивирусов быстро нашли пути

противодействия такому ransomware, а власти блокировали большинство источников его поступления.

Возвращение ransomware происходит на новом качественном уровне, и представляет более серьезную угрозу. Атака обычно инициируется нажатием на ссылку в спамовом электронном письме, и запускает серию процессов, не оставляющих жертве особого выбора. Всплывающее окно информирует о том, какие файлы зашифрованы, а также о том, что при невыплате выкупа ключ расшифровки будет уничтожен, и возможность восстановления информации окончательно потеряна.

Использование сети Tor делает практически невозможным отслеживание организаторов таких атак, а нестандартная схема шифрования не позволят найти решение даже перехватив сетевой трафик.

Анализ кода Onion позволяет специалистам Kaspersky Lab предположить, что родным языком программистов является русский. Они также предупреждают, что выход этой угрозы за пределы постсоветского пространства это лишь вопрос времени.

МВД России предложило контракт стоимостью 3,9 млн р. (примерно 110 тыс. дол.) для изучения возможности получения технической информации о пользователях и оборудовании анонимной сети Tor.

На сегодняшний день, однако, единственный реальный способ противодействия усовершенствованному ransomware заключается в создании резервных копий своих файлов на съемных носителях ***(Вредоносное ПО Onion, по мнению экспертов, почти неуязвимо // InternetUA (http://internetua.com/vredonosnoe-po-Onion--po-mneniua-ekspertov--pocsti-neuyazvimo). – 2014. – 1.08).***

***

Более 2800 предприятий, значительная часть которых связана с энергетикой и машиностроением, пострадали от глобальной кампании кибершпионажа Crouching Yeti (также известной как Energetic Bear) – предположительно похищена конфиденциальная информация, составлявшая коммерческую тайну, в том числе некоторых украинских предприятий. Специалисты Kaspersky Lab провели расследование, в ходе которого установили, что злоумышленники, стоящие за Crouching Yeti, участвовали в организации ряда других сложных целевых атак. Одной из особенностей кампании является нацеленность на индустриальные ИТ-инфраструктуры и системы.

Первые действия в рамках кампании были предприняты еще в 2010 г., и ежедневные атаки продолжаются до сих пор. В числе жертв – предприятия отрасли машиностроения, энергетики, промышленного производства, строительства, фармацевтические организации, ИТ-компании и образовательные учреждения. Большая часть из них находится в США и Испании, но были также обнаружены атаки на предприятия в Германии, Франции, Италии, Турции, Ирландии, Польше и Украине. Ранее сообщалось,

что кампания была направлена на энергетические структуры, но список жертв, идентифицированных Kaspersky Lab указывает, что интересы киберпреступников гораздо шире. Специалисты Kaspersky Lab допускают, что речь идет не об узкоспециализированной операции, а о широкой кампании шпионажа, затрагивающей различные секторы.

Crouching Yeti не относится к ряду технически сложных кампаний. Злоумышленники не использовали уязвимости нулевого дня – ими были применены распространенные эксплойты. Однако это не мешало проводить операцию в течение многих лет без привлечения внимания. В общей сложности эксперты смогли собрать доказательства использования троянцев и бэкдора для кражи ценной информации из зараженных систем. Самым распространенным из них является троянец Havex – было найдено 27 различных версий этого зловреда, в том числе дополнительные модули, нацеленные на сбор данных из индустриальных систем. Один из них искал в локальной сети OPC-серверы, обычно использующиеся совместно с множеством индустриальных систем автоматизации, и собирал чрезвычайно подробную информацию об их работе.

Для управления использовалась широкая сеть взломанных веб-сайтов, находящаяся большей частью на территории США, России и Германии. На них хранилась украденная информация, а также дополнительные вредоносные модули, которые доставлялись на зараженные системы. Среди этих модулей – инструменты для кражи паролей и почтовых контактов, снятия снимков экрана и поиска текстовых документов, таблиц, баз данных, носителей информации, защищенных файлов, электронных ключей и прочих ценных данных ***(От глобальной кампании кибершпионажа пострадали более 2800 предприятий, включая украинские // InternetUA (http://internetua.com/ot-globalnoi-kampanii-kibershpionaja-postradali-bolee-2800-predpriyatii--vkluacsaya-ukrainskie). – 2014. – 1.08).***

***

Американский программист и хакер М. Солник утверждает, что способен удаленно взломать и получить управление над любым смартфоном на расстоянии 10 м от него. Об этом не узнает ни его владелец, ни телефонная компания, а хакер получит полный контроль над гаджетом. Захочет – превратит в микрофон, работающий в реальном времени, или при желании получит доступ к списку контактов, личным сообщениям и другой информации пользователя.

Хакеры могут делать все, что хотят. Даже если они пожелают установить на чужом устройстве Angry Birds, они сделают это.

М. Солник, 28-летний консультант по безопасности Accuvant Inc., работающей с компаниями из списка Fortune 500 и с американским правительством.

Умения М. Солника определяют новый рубеж в информационной безопасности, ведь компьютер специалиста теперь может буквально замаскироваться под смартфон любого пользователя.

Смартфоны постоянно подключены к Интернету, прошивка в них обновляется не слишком часто, а обеспечить их безопасность довольно сложно. То есть, для мошенников они представляют собой хорошие мишени, с помощью которых можно получить нужные фотоснимки и имена и даже прослушать разговоры.

Большинство пользователей не осознает масштабы данной проблемы. Вы храните массу информации на своих устройствах, которые постоянно подключены к сети.

Смартфоны будут основной темой обсуждения в рамках конференции по компьютерной безопасности Black Hat, что пройдет в Лас-Вегасе на следующей неделе. В ее рамках М. Солник проведет презентацию и расскажет о технике разработанной им хакерской атаки. Четыре студента из Технологического университета Джорджии получили задание продемонстрировать новые способы взлома самой последней модели iPhone. Исследователи из Bluebox Security, работающей в сфере мобильной безопасности, покажут, как приложения могут воровать пользовательские данные со смартфонов на базе созданной Google операционной системы Android. Кстати, Google уже в курсе проблемы и даже выпустила патч для ее решения.

М. Солник сообщает, что научился выдавать себя за оператора сотовой связи и проникать в смартфон через лазейку в радиосистемах. Его находку можно использовать против современных смартфонов на базе ПО от BlackBerry, включая и модель Z10, с ОС Android на борту и даже старых версий iOS. Также с ее помощью можно взломать многие гаджеты в сетях LTE, хотя данная технология, считается самой современной и, соответственно, самой защищенной от кибератак.

Для связи с беспроводными сетями операторов смартфоны используют так называемый чип радиомодема. У пользователей нет доступа к этой системе, а эксперты по безопасности еще должны попотеть, чтобы пройти через ее защиту.

М. Солник использует фальшивые вышки-ретрансляторы мобильной связи, чтобы «обмануть» смартфон и заставить систему считать его сотовым оператором. Такие имитации вышек, по словам эксперта, можно купить меньше чем за 1000 дол. И затем на расстоянии менее 10 м эта фальшивая вышка размером со стандартный ноутбук может загрузить в любой смартфон вредоносный код.

В некоторых случаях взломщик может контролировать и другие функции смартфона, включая его микрофоны, камеры и даже приложения. По словам М. Солника, он сам и его коллега М. Бланшу воплотили в жизнь эту технику с целью доказать, что это, в принципе, возможно.

Их технология работает с микросхемами, производимыми Qualcomm, а ведь эта компания поставляет чипы радиомодема практически для всей индустрии смартфонов. Представители Qualcomm подтвердили, что программисты из Accuvant нашли лазейку в системе защиты их чипов. Однако это поможет теперь оперативно исправить проблему с безопасностью. По словам пресс-секретаря Qualcomm, уязвимость, выявленная М. Солником, работает только с программами от сторонних компаний, и только в устаревших версиях радиосистемы.

В BlackBerry заявляют, что активно сотрудничают с Accuvant, а представители Google и Apple подтвердили, что приняли неприятное открытие во внимание.

А. Людвиг, глава отдела безопасности Android, утверждает, что Google интегрирует систему безопасности в свое программное обеспечение. Так, подразумевается, что приложения должны работать изолировано друг от друга, это исключит кражу личных данных. По его мнению, система радиомодема, в принципе, угрожает уязвимостью любому смартфону, в котором она используется.

Такая особенность работы системы радиосвязи усложняет процесс защиты смартфона с помощью единой антивирусной программы. Ведь на мобильных устройствах антивирусы работают не так, как на компьютерах. К тому же сами пользователи еще не научились самостоятельно предпринимать какие-то меры безопасности, пользуясь смартфонами.

Хакеры и разведывательные службы уже давно ищут способы взлома и проникновения в смартфоны без ведома их владельцев или сотовых операторов. Некоторые подрядчики Министерства обороны США даже инвестируют средства в разработку технологий взлома систем радиомодемов. Это подтверждают источники, которые осведомлены в данном вопросе.

Инвестиционная компания Francisco Partners Management LLC в этом году приобрела за 110 млн дол. израильскую компанию NSO Group, которая помогает правительственным ведомствам шпионить за личными смартфонами граждан. Это также подтверждают осведомленные источники. В своих учетных записях в профессиональной соцсети LinkedIn бывшие и нынешние инженеры NSO Group сообщают о взломе систем безопасности мобильных систем Google и Apple. В Francisco Partners пока не комментируют эту информацию.

Чем круче становятся наши гаджеты, тем меньше сил разного рода спецслужбам и мошенникам надо затрачивать для получения нужных сведений. А если вспомнить о социальных сетях, поисковых системах и прочих фишках Интернета, благодаря которым, по сути, каждый активный пользователь упомянутых сервисов является открытой книгой для тех, у кого есть доступ к соответствующим данным. А он есть, чтобы там ни говорило правительство или силовые ведомства.

Все, что создано человеком, может быть им же и взломано. Уверен, что всплывающие то тут, то там методы взлома тех или иных сервисов и устройств уже давно известны особым людям и организациям и активно ими используются. Просто «непосвященным» посчастливилось наткнуться на эти методы в ходе своих экспериментов, и они начали поднимать шум. Пошумят, ответственные люди сделают вид, мол, все исправили, и на этом все закончится, а мы, простые пользователи, все так же будем «под колпаком» ***(Смартфоны – это новый вызов кибербезопасности // InternetUA (http://internetua.com/smartfoni---eto-novii-vizov-kiberbezopasnosti). – 2014. – 3.08).***

***

Австрийская правозащитная организация Europe-v-Facebook обратилась к пользователям с предложением присоединиться к ее исковому заявлению против крупнейшей социальной сети. Как следует из сообщения юристов, компания Facebook обвиняется в нарушении политики конфиденциальности и злоупотреблении личными данными владельцев учетных записей.

Учредитель австрийской организации М. Шремс инициировал судебное разбирательство в Хозяйственном суде Вены, Австрия, (по месту своего жительства). Сторонников своей инициативы он ищет при помощи специально созданного сайта fbclaim.com.

Ответчиком по делу выступает ирландское подразделение социальной сети Facebook Ireland, в обязанности которого входит работа с клиентами за пределами США и Канады. Согласно законодательству ЕС, потребители могут подать в суд на какую-либо бизнесорганизацию в соответствующий суд в их стране. Кроме того, по словам представителей Europe-v-Facebook, стоимость судебного разбирательства в Австрии значительно ниже, чем в Европе.

Социальную сеть призывают к ответственности за «очевидные нарушения закона», совершенные в результате участия компании в американской правительственной программе Prism, отслеживания действий пользователей на сторонних сайтах, невыдачи информации по запросами на доступ к данным Facebook и т. п.

Сумма возмещения ущерба составляет 500 евро для каждого, кто подключился к судебному разбирательству. По словам М. Шремса, сумма специально была установлена на столь низком уровне, поскольку основной целью правозащитников является отстаивание прав потребителей ***(Австрийская правозащитная организация подала в суд на Facebook // InternetUA (http://internetua.com/avstriiskaya-pravozasxitnaya-organizaciya-podala-v-sud-na-Facebook). – 2014. – 3.08).***

***

Свыше 17 тыс. человек присоединились к иску студента из Австрии против Facebook, обвиняющего соцсеть в нарушении приватности личных данных пользователей. Об этом со ссылкой на инициатора иска сообщает Reuters.

По словам 26-летнего М. Шремса, который подал иск в суд Вены на прошлой неделе, отклик на призыв к пользователям Facebook присоединиться к обвинению оказался значительно выше ожидаемого. Большинство пользователей, подписавшихся под коллективным иском, живут в Европе, многие из них решили оказать финансовую поддержку, отметил он ***(Более 17 тысяч человек поддержали иск австрийского студента к Facebook // InternetUA (http://internetua.com/bolee-17-tisyacs-cselovek-podderjali-isk-avstriiskogo-studenta-k-Facebook). – 2014. – 6.08).***

***

Китайские власти исключили «Лабораторию Касперского» из списка компаний-поставщиков защитного ПО для правительства КНР. Об этом сообщило китайское информагентство агентство «Синьхуа».

Помимо «Касперского», места правительственного поставщика лишился американский разработчик Symantec, производящий обширный перечень защитных программных продуктов, в частности, Norton AntiVirus, DLP-решения, решения для резервного копирования и пр.

Как сообщает агентство, право на поставку ПО для обеспечения информационной безопасности в правительственных учреждениях Китая сохранили только пять местных разработчиков защитных программ: Qihoo 360, Venustech, CAJinchen, Beijing Jiangmin и Rising.

В «Лаборатории Касперского» на момент выхода этого материала (в воскресенье 3 августа 2014 г.) не прокомментировали информацию, распространенную «Синьхуа». Представитель «Касперского» заявила CNews, что занята выяснением подробностей о сложившейся ситуации.

Известно, что «Лаборатория Касперского» считает китайский рынок, где она присутствует с 2003 г., одним из важнейших. Согласно открытым источникам, В 2009 г. гендиректор и основатель компании Е. Касперский был награжден орденом Дружбы КНР за вклад в развитие индустрии информационной безопасности в Китае. В 2013 г. китайский интернет-поисковик Baidu выпустил при участии «Лаборатории Касперского» собственный антивирус.

В последние месяцы было замечено несколько действий китайских властей, направленных на отказ от использования зарубежных аппаратных и программных продуктов в правительственных учреждениях и местной финансовой сфере.

Так, по данным «Синьхуа», в мае 2014 г. центральная служба обеспечения правительства запретила использование в правительственных структурах новых ПК на платформе Microsoft Windows 8.

Тогда же стало известно о требовании китайского правительства местным банкам отказаться от серверов, выпущенных американской корпорацией IBM, и заменить их аналогами китайских производителей ***(Китай изгоняет «Касперского» из правительственных учреждений // InternetUA (http://internetua.com/kitai-izgonyaet--kasperskogo--iz-pravitelstvennih-ucsrejdenii). – 2014. – 4.08).***

***

Symantec и Kaspersky Lab отрицают тот факт, что Китай запретил использование антивирусов на территории своей страны. Заявление было сделано на фоне сообщений СМИ о том, что Китай прекращает сотрудничество с зарубежными компаниями по безопасности, а также ограничивает использование зарубежных технологий своими гражданами.

Обе компании не входят в число утвержденных компаний-производителей антивирусной продукции, которые контролируются агентством правительственных закупок. Это и побудило СМИ сделать выводы, что Китай исключил Symantec и Kaspersky из перечня доверенного антивирусного ПО с целью минимизировать использование иностранных технологий в стране ***(Symantec и Kaspersky отрицают введение Китаем запрета на использование антивирусов // IT Expert (http://itexpert.org.ua/rubrikator/item/37416-symantec-i-kaspersky-otritsayut-vvedenie-kitaem-zapreta-na-ispolzovanie-antivirusov.html). – 2014. – 5.08).***

***

Специалисты «Лаборатории Касперского» провели анализ накопленной статистики по различным показателям активности киберзлоумышленников во II квартале 2014 г. Об этом IT Expert сообщила пресс-служба компании.

Антивирусные эксперты отметили не только 4-кратное усиление темпов развития банковских троянцев, но и новые приемы хакеров. Также они столкнулись с первой мобильной программой-шифровальщиком и обнаружили модули для слежки за мобильными устройствами Apple. Несмотря на то, что украинские пользователи еще не успели пострадать от этих новых угроз, они ежедневно сталкиваются с множеством других опасностей. В частности, Украина вышла на третье место по количеству атак банковскими троянцами и на четвертое по риску онлайн-заражения.

По всему миру за II квартал с онлайн-ресурсов было произведено 354,5 млн атак, что на 1,3 млн превышает аналогичный показатель первых трех месяцев. Среди стран-источников веб-атак на первое место, опередив США, вышла Германия – ее доля возросла на 12 пунктов и составила 22,4 %.

Что касается мобильных зловредов, то они заметно пополнили коллекцию KasperskyLab: 65 тыс. новых образцов, среди которых первый мобильный шифровальщик Pletor, увеличили базу данных до 300 тыс. экземпляров. Большинство из них по-прежнему нацелено на Android, однако злоумышленники, применяя ряд инструментов для похищения AppleID,

начали целиком блокировать устройства на базе iOSи требовать с пользователей выкуп за восстановление доступа к смартфону или планшету. Эта находка совпала с выпуском отчета о «новинках» итальянской компании HackingTeam, которая занимается разработкой и продажей правоохранительным органам программ для слежки – теперь они предоставляют модули для Android, iOS, WindowsMobileи Blackberry.

Рост числа классических вредоносных программ также не замедляется: за II квартал в коллекцию Kaspersky Lab попало 60 млн новых опасных объектов, а 145 млн ссылок были признаны вредоносными, что на 77 % выше показателя прошлого квартала.

При этом защитные продукты компании пресекли более 927 тыс. попыток запуска банковских троянцев. Примечательно, что в мае этот показатель увеличился на 36,6 % по сравнению с апрелем. Большая часть атак затронула пользователей Бразилии, России, Италии и Германии. Также было обнаружено более 2 тыс. новых банковских троянцев – таким образом, с начала года число известных образцов этого типа вредоносного ПО увеличилось в четыре раза. Растут и финансовые потери – в рамках одной только операции с помощью троянца Luuukза одну неделю было похищено 500 тыс. евро у 190 жертв ***(Шаповал В. Украина вышла на третье место по количеству атак мобильными банковскими троянцами IT Expert (http://itexpert.org.ua/rubrikator/item/37408-ukraina-vyshla-na-trete-mesto-po-kolichestvu-atak-mobilnymi-bankovskimi-troyantsami.html). – 2014. – 5.08).***

***

Спеціаліст із кібербезпеки і зламу систем Р. Сантамарта, який працює консультантом в IOActive, заявив, що йому вдалося знайти спосіб проникнення в систему супутникового зв'язку пасажирських літаків. Злам здійснюється за допомогою бортової Wi-Fi мережі та розважальні системи, які доступні звичайному пасажиру.

Завдяки вразливості, хакери можуть взяти під контроль передачу даних із супутників навігації і змінювати їх, що може призвести до того, що літак зіб'ється з курсу. Дана вразливість була виявлена в багатьох зразках програмного забезпечення, яке використовується для контролю над комунікаційним обладнанням. Як зізнається сам Р. Сантамарта, механізм тестувався виключно в лабораторних умовах.

Варто зазначити, що ряд виробників частково підтвердили таку можливість, але заявили, що реальний рівень ризику нижчий, ніж його подає хакер.

Детальний опис механізму зламу фахівець збирається розповісти на щорічній конференції Black Hat, на якій хакери і фахівці з кібербезпеки діляться результатами своїх досліджень. У разі пред'явлення хакером реальних даних, як вважають фахівці, авіакомпанії можуть запровадити нові правила, а також змусити виробників програмного забезпечення закрити уразливість і провести повну перевірку всіх систем ***(Хакер попередив про***

***можливість кібератаки на пасажирські літаки // ТСН (http://tsn.ua/nauka_it/haker-popered iv-pro-mozhlivist-kiberataki-na-pasazhirski-litaki-361913.html). – 2014. – 5.08).***

***

Майже три чверті від усіх пристроїв з категорії «Інтернету речей» можуть піддаватися хакерським зламам та пошкодженням. Про це йдеться в нещодавньому дослідженні, опублікованому компанією Hewlett-Packard (HP), пише mashable.com.

Під час дослідження вивчалися 10 поширених смарт-пристроїв, включно з веб-камерами та термостатами. Як стверджують експерти, кожен із приладів мав приблизно 25 вразливостей. Багато з них стосувалися ненадійних паролів або слабко захищеного програмного забезпечення.

Вісім з десяти пристроїв для нормальної роботи потребують сильнішого паролю. Таке ж співвідношення приладів, що піддаються ризику перехоплення персональної інформації за допомогою хмаркових сервісів.

«Торік ми багато чули про "Інтернет речей" про його безпеку, але не бачили загальної картини», – пояснюють необхідність свого дослідження в HP.

Тож у компанії вирішили вивчити проблему та ознайомити людей з основними проблемами безпеки таких пристроїв.

Дослідна компанія Garner передбачає, що до 2020 р. у світі буде 26 млрд індивідуальних об'єктів категорії «Інтернету речей». При цьому у 2009-му р. їх було продано лише 9 млн.

До «Інтернету речей» можуть належати будь-які приєднані до Інтернету прилади, так звані «розумні пристрої»: від холодильника до зубної щітки ***(70 відсотків «розумних пристроїв» вразливі до хакерських атак – дослідження // MediaSapiens (http://osvita.mediasapiens.ua/material/33312). – 2014. – 4.08).***

***

Лаборатория Zillya! провела исследование вирусной активности в Украине за первое полугодие 2014 г. и обнаружила очень интересный факт: компьютеры многих украинцев стали жертвами вируса, которые втайне от пользователя изменяет результаты интернет-поиска. Вирус применяется в «черном SEO», когда вместо стандартной поисковой выдачи, на первых местах поиска оказываются нужные заказчику или владельцу вируса сайты. Это позволяет повысить посещаемость указанных сайтов и, следственно, увеличить продажи рекламируемых товаров и услуг, пишет AIN.UA (http://ain.ua/2014/08/04/535309).

Эксперты из Zillya! составили график, на котором видно, что около 30 % всех веб-угроз в марте месяце относились именно к вирусу Adware.BetterSutf.Win32. Подтверждает результаты исследований отчет

«Лаборатории Касперского» за I квартал 2014 г., которая определила вирус как № 3 в списке вредоносных объектов за этот период.

Как работает Adware.BetterSutf.Win32?

Вирус устанавливается на компьютер пользователя в виде плагинов для основных интернет-браузеров Chrome, Internet Explorer и Firefox. В Zillya! взяли несколько образцов вирусов и установили их на чистых машинах ради эксперимента. В Chrome-браузере образец вируса зашифровался под непонятную программу Video Player 1.1. Обнаружен вирус для черного SEO, который подделывает результаты поиска для украинцев

В данном случае рекламный модуль используется для сбора данных пользователя, чтобы затем отправлять ему спам. Аналогичные результаты были получены и по другим запросам. В дополнение к «фейковым» результатам поиска начали появляться всплывающие окна с предложением установить ПО непонятного происхождения.

Эксперты из Zillya! считают, что вирус используют многие украинские SEO-специалисты. О том, кто и как занимается подменой поисковой выдачи украинцев говорить пока рано, но работа в этом направлении уже ведется. «Информационная война в Украине продолжается и, чем глубже и дольше в Украине будет наблюдаться кризис, тем чаще мы будем детектировать подобного рода угрозы. Не стоит забывать, что подобные модули могут использоваться, как еще один вид “вооружения” в “информационной войне”», – считает технический директор компании О. Сыч.

Недавно на AIN.UA публиковалась карта зараженности Украины вирусами. Как выяснилось, самыми уязвимыми для кибератак регионами в Украине оказались Закарпатская, Ровенская, Кировоградская области, а также Крым. Самой «здоровой» областью оказалась Черниговская ***(Обнаружен вирус для черного SEO, который подделывает результаты поиска для украинцев // AIN.UA (http://ain.ua/2014/08/04/535309). – 2014. – 4.08).***

***

Создатели известного вредоносного ПО CryptoWall провели новую хакерскую атаку, жертвы которой потеряли биткоинов на общую сумму в несколько сотен тысяч долларов. По данным ИБ-экспертов из PhishMe, точные масштабы инцидента установить невозможно, но потери могут составить даже несколько миллионов долларов.

Известно, что с атакой, реализуемой при помощи фишинга, связаны два Bitcoin-кошелька. Владельцем одного из них является пользователь под ником Leo1, владеющий 710 виртуальными монетами стоимостью в 415 тыс. дол. В другом кошельке находилось 38 биткоинов на 22 тыс. дол.

По информации специалистов, CryptoWall использует фишинговые электронные письма, содержащие сокращенную ссылку Google. Узнав о наличии проблемы, эксперты поискового гиганта сразу же удалили URL-адрес.

Согласно данным PhishMe, на сокращенный URL нажали 281 раз – после каждого раза на систему скачивался вредоносный zip-файл, содержащий новый вариант CryptoWall. Примечательно, что антивирусные решения практически не способны обнаружить наличие вируса ***(Новый вариант CryptoWall позволил похитить биткоинов на сотни тысяч долларов // InternetUA (http://internetua.com/novii-variant-CryptoWall-pozvolil-pohitit-bitkoinov-na-sotni-tisyacs-dollarov). – 2014. – 6.08).***

***

Компания Dr.Web создала отчет за июль о выявлении угроз и вирусной активности в общем. В прошлом месяце были выявлены такие вредоносные ПО как Trojan.BPlug.100, Trojan.BPlug.48, Trojan.BPlug.46, Trojan.BPlug.102, Trojan.BPlug.28, Trojan.BPlug.79 и прочее. Разница между ними заключается в особенностях реализации.

Наиболее распространенной угрозой месяца июля можно по праву считать троянца – установщика зараженных приложений Trojan.Packed.24524. Частота его установки от общего количества всех угроз составляет 1,59 %. Среди лидеров по частоте распространения вредоносного ПО также находятся рекламные троянцы семейства Trojan.InstallMonster.

Почтовый трафик июля содержал в себе множество вредоносов, перенаправляющих жертву на различные вредоносные сайты. Среди них – Trojan.Redirect.195 и Trojan.Redirect.197. Одним из опаснейших троянов оказался BackDoor.Tishop.122, который занимался рассылкой вредоносных программ, которые загружались на незащищенный ПК жертвы.

Ботнеты, созданные злоумышленниками с использованием файлового вируса Win32.Rmnet.12 (250 тыс. обращений к управляющим серверам в сутки), продолжают свое действие. На втором и третьем месте по используемых ботнетами вирусам занимают Win32.Sector и вредоносный модуль Trojan.Rmnet.19, которые инфицировали 65 тыс. узлов и создали 1100 ежесуточных обращений к командным серверам, соответственно. В свою очередь, троянская программа BackDoor.Flashback.39, управляемая ОП Mac OS X на сегодняшний день заразила порядка 14 тыс. узлов.

Наиболее актуальной угрозой для пользователей ПК эксперты Dr.Web признали вредоносные программы семейства Trojan.Encoder. Энкодеры массово рассылают ссылки на вредоносные веб-сайты через социальные сети или электронную почту.

Среди мобильных угроз была обнаружена опасная вредоносная программа Android.BankBot.21.origin, занимающаяся кражей данных об используемой банковской карте владельца смартфона или планшета под управлением ОС Android ***(Наиболее распространенная угроза в июле – троянец-установщик приложений // InternetUA (http://internetua.com/naibolee-rasprostranennaya-ugroza-v-iuale---troyanec-ustanovsxik-prilojenii). – 2014. – 5.08).***

***

ИБ-эксперт П. Раскагнерес сообщил о редкой разновидности вредоносного ПО, которое инфицирует системы и похищает данные без установки файлов. Оно локализируется исключительно в реестре компьютера, поэтому вредонос весьма сложно обнаружить.

Заражение происходит через открытие вредоносного документа Microsoft Word. Сначала создается скрытый зашифрованный ключ реестра, а затем выполняются шелл-код и полезная нагрузка. «Вся активность происходит в реестре. Никакие файлы не создаются, – сообщил П. Раскагнерес. – Таким образом злоумышленники могут обойти классические технологии сканирования файлов и, проникнув в глубокий слой [машины], могут осуществлять любые действия даже после перезагрузки системы».

По словам эксперта, для того, чтобы предотвратить подобные атаки, антивирусные решения должны перехватить вредоносный документ Microsoft Word еще до того, как он попал в электронный почтовый ящик пользователя, и не допустить его выполнения.

Windows Regedit не может прочитывать или открывать входы, которые осуществляются с помощью ключа, зашифрованного не в ASCII. Microsoft использует эту особенность для предотвращения копирования исходного кода. Тем не менее, ранее эта функция была взломана. Для того чтобы обезопасить себя, пользователи могут использовать инструменты безопасности, способные обнаружить эксплоит, а также проверять реестр на наличие подозрительной активности ***(Эксперт рассказал о вредоносном ПО, которое локализируется в реестре и не создает файлы // InternetUA (http://internetua.com/ekspert-rasskazal-o-vredonosnom-po--kotoroe-lokaliziruetsya-v-reestre-i-ne-sozdaet-faili). – 2014. – 6.08).***

***

Эксплойт под уязвимость CVE-2010-2568, обнаруженную еще в 2010 г. вместе с печально известным червем Stuxnet, до сих пор широко распространен и представляет опасность для пользователей. Как выяснили эксперты Kaspersky Lab в ходе специального исследования уязвимостей ОС Windows, за восемь месяцев с ноября 2013 г. по июнь 2014 г. с этой угрозой столкнулось 19 млн пользователей по всему миру.

Уязвимость CVE-2010-2568 вызвана ошибкой в механизме обработки ярлыков в ОС Windows, что позволяет загружать произвольную библиотеку без ведома пользователей. Уязвимость затронула системы Windows XP, Vista, 7, а также Windows Server 2003 и 2008. Самой известной вредоносной программой, использовавшей эксплойт под эту уязвимость, стал червь Stuxnet, предположительно ответственный за физическое разрушение оборудования для обогащения урана на ядерных объектах в Иране. Несмотря на то что Microsoft выпустила обновление безопасности, закрывающее эту уязвимость, еще осенью 2010 г., системы детектирования Kaspersky Lab до

сих пор регистрируют миллионы срабатываний на эксплойты под CVE-2010-2568.

Большинство срабатываний были зарегистрированы на компьютерах пользователей из Вьетнама (43 %), Индии (12 %), Индонезии (9 %), Бразилии (6 %) и Алжира (4 %).

Наибольшее число срабатываний на уязвимость CVE-2010-2568 пришлось на ОС Windows XP – 64 %. Самая популярная среди пользователей Windows 7 оказалась на втором месте с долей 28 %. На серверные же версии Windows Server 2008 и 2003 пришлось по 4 % и 2 % срабатываний соответственно.

Эксперты Kaspersky Lab хотели бы почеркнуть, что большое количество срабатываний в данном случае не свидетельствует о большом количестве атак. Из-за особенностей использования уязвимости CVE-2010-2568 невозможно точно определить, в каких случаях продукты Kaspersky Lab защищали от реальных атак, а в каких просто детектировали автоматически созданные тем или иным червем уязвимые ярлыки. Однако большое число срабатываний на CVE-2010-2568 говорит о том, что в мире еще очень много систем, уязвимых для атак с помощью соответствующих эксплойтов.

«Очевидно, что подобная ситуация создает постоянный риск заражения вредоносным ПО в тех организациях, где до сих пор работают такие уязвимые серверы. Поэтому мы призываем IT-руководство компаний уделять больше внимания актуальности программного обеспечения в корпоративном парке и использовать адекватные средства защиты от киберугроз», – заявил В. Закоржевский, руководитель группы исследования уязвимостей Kaspersky Lab ***(Призрак Stuxnet: уязвимость в Windows все еще создает опасность //InternetUA (http://internetua.com/prizrak-Stuxnet--uyazvimost-v-Windows-vse-esxe-sozdaet-opasnost). – 2014. – 7.08).***

***

Группа российских хакеров предположительно похитила 1,2 млрд учетных записей пользователей Интернета по всему миру.

6 августа газета New York Times сообщила о беспрецедентной по своим масштабам краже, которую выявила американская фирма Hold Security, занимающаяся обеспечением сетевой безопасности, пишет Украинская правда.

По данным IT-специалистов фирмы, преступники завладели логинами и паролями более 500 млн адресов электронной почты. Hold Security удалось установить, что группа хакеров состоит примерно из 10 человек и базируется в небольшом российском городе неподалеку от границы с Казахстаном.

Американские эксперты утверждают, что в руках у злоумышленников оказались данные почти 420 тыс. сайтов, некоторые из которых представляют известные компании, передает Deutche Welle.

Hold Security отказалась назвать какие-либо конкретные имена пострадавших от кражи личных данных. Однако привлеченные к

расследованию независимые эксперты подтвердили достоверность базы данных обворованных пользователей.

По словам основателя Hold Security А. Холдена, теперь фирма намерена инициировать судебный процесс против российских хакеров. Кроме того, ее специалисты начали разрабатывать программное обеспечение, позволяющее пользователям узнать о краже личных данных ***(Российские хакеры похитили более миллиарда учетных записей пользователей интернета // Николаевские Вести (http://nikvesti.com/news/incidents/57160). – 2014. – 6.08).***

***

По данным FireEye, несколько провайдеров Интернет-услуг в США и Азии, медиакомпания из США, а также финансовое учреждение и государственная организация, расположенные в Азии, стали мишенью для мошенников в ходе операции под названием «Отравленный Ураган» (Poisoned Hurricane).

FireEye начала анализировать деятельность группы в марте 2014 г., когда эксперты заметили семейство PlugX (Kaba), подключенное к легальным доменам и IP-адресам. Один из образцов, отмеченный исследователями, был подписан законным цифровым сертификатом Ассоциации полиции по взаимопомощи (Police Mutual Aid Association), в то время как другой использовал цифровой сертификат с истекшим сроком действия от компании под названием MOCOMSYS.

Вредоносная программа была создана для подключения к доменам, таким как adobe.com, update.adobe.com и outlook.com. Поскольку маловероятно, что нападавшие имели доступ к этим доменам, исследователи решили, что они изменили маршрут трафика, предназначенного для этих доменов от конкретных пользователей.

PlugX был настроен для разрешения DNS-запросов через серверы имен в компании под названием Hurricane Electric. Любой желающий может зарегистрировать бесплатный аккаунт с помощью сервиса DNS компании, который позволяет пользователям регистрировать зону и создавать записи. Эти записи могут быть перенаправлены на любой IP-адрес.

В общей сложности, FireEye выявила 21 домен, взломанный в подобной манере. Тем не менее, по состоянию на 4 августа компания Hurricane Electric уже не передавала информацию на эти домены, сообщает компания.

Посетители взломанных доменов не пострадали, если их компьютеры не были заражены вредоносным PlugX, но эксперты отмечают, что эта тактика усложнит работу ИТ-специалистов по безопасности в будущем ***(Хакеры взломали популярные домены adobe.com, update.adobe.com и outlook.com // InternetUA (http://internetua.com/hakeri-vzlomali-populyarnie-domeni-adobe-com--update-adobe-com-i-outlook-com). – 2014. – 7.08).***

***

Компания «Доктор Веб» обнаружила новый троян-вымогатель для устройств под управлением ОС Android. Как сообщили CNews в «Доктор Веб», новый представитель данного класса угроз несколько выбивается из общей массы: получая от пользователя информацию о совершенном платеже, он не выполняет ее должной проверки и в большинстве случаев успешно снимает установленную блокировку.

Новый троян-блокировщик, внесенный в вирусную базу «Доктор Веб» под именем Android.Locker.27.origin, распространяется злоумышленниками под видом антивирусного приложения и после своего запуска имитирует сканирование мобильного устройства на предмет установленных на нем вредоносных программ, которые в конечном итоге якобы находит.

После этого троян запрашивает доступ к функциям администратора и, вне зависимости от предпринятого пользователем действия, блокирует устройство, демонстрируя на экране предупреждение о серьезном нарушении закона.

За разблокировку устройства, а также для снятия выдвинутых обвинений вымогатель требует заплатить выкуп в размере 500 дол., предоставив ему код предоплаченной карты GreenDot MoneyPak.

Основное отличие Android.Locker.27.origin от других аналогичных вредоносных программ заключается в процедуре проверки подлинности платежа, указали в «Доктор Веб». В частности, троян удостоверяется, что введенный пользователем код состоит из 14 цифр, а также не содержит наиболее предсказуемые комбинации вида «00000», «11111», «22222», «33333» и т. д. вплоть до «99999», а также «12345». Если эти требования соблюдаются, вредоносная программа загружает полученный код на принадлежащий злоумышленникам сервер, после чего снимает блокировку и запускает процесс своего удаления. Таким образом, пострадавшие пользователи могут легко и совершенно бесплатно избавиться от этой весьма неприятной угрозы, введя по требованию горе-вымогателя практически любую комбинацию из 14 цифр.

В отличие от этой вполне безобидной реализации трояна-блокировщика, многие аналогичные вредоносные приложения куда менее дружелюбны и могут доставить владельцам мобильных Android-устройств намного более серьезные неприятности ***(Новый Android-вымогатель бесплатно снимает ограничения с заблокированных устройств // InternetUA (http://internetua.com/novii-Android-vimogatel-besplatno-snimaet-ogranicseniya-s-zablokirovannih-ustroistv). – 2014. – 8.08).***

***

Сразу два американских федеральных агентства сообщили о временном прекращении сотрудничества с одним из крупнейших правительственных подрядчиков из-за хакерской атаки. Нападение, по предварительным данным, произошло в среду, 6 августа, и стало причиной утечки персональных

данных сотрудников Министерства внутренней безопасности США (Department of Homeland Security, DHS).

Интересно, что по мнению американского правительства, за хакерским нападением стоит правительство неназванной страны. К аналогичному выводу пришли эксперты пострадавшей компании US Investigations Services (USIS), которые активно расследуют инцидент.

Отметим, что USIS в настоящее время проводит так называемую проверку анкетных данных для более чем 90 государственных ведомств США. Для выяснения всех деталей и обстоятельств инцидента организация наняла стороннюю компанию, которая в ближайшее время выяснит «точный характер и масштабы компрометации компьютерной сети».

От услуг USIS, кроме DHS, временно отказалось Управление по управлению персоналом (of Personnel Management, OPM). Оба ведомства отметили, что надеются на скорое возобновление сотрудничества ***(Хакеры похитили личные данные чиновников США // InternetUA (http://internetua.com/hakeri-pohitili-licsnie-dannie-csinovnikov-ssha). – 2014. – 7.08).***