СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(8–21.09)

2014 № 17

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(8–21.09)
№ 17

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

Facebook является крупнейшей соцсетью и неудивительно, что ее кнопка «Поделиться» является самой популярной среди пользователей. По данным агентства Fractl и платформы BuzzSumo, 81,9 % «расшаренных» материалов в соцсетях приходится на детище М. Цукерберга, пишет sostav.ru.

На втором месте – Twitter с 8,6 %, далее следуют Google+ (4,3 %), Pinterest (3 %) и LinkedIn (2,2 %). Исследование охватывает 1 млн статей, которыми поделились 2,6 млрд раз.

В зависимости от площадки результаты будут меняться в ту или иную сторону. Например, на Upworthy 99,6 % «расшариваний» происходит через Facebook. Данная соцсеть очень популярна у аудитории Huffington Post (95,5 %), DailyMail.co.uk (92,1 %), Yahoo (91,5 %). Наибольшее разнообразие наблюдается у читателей Mashable: 41,3 % делится материалами на Facebook, 26,1 % – в Twitter, 23,4 % – в LinkedIn. У издания BuzzFeed заметную долю занимает Pinterest (10 %) ***(Пользователи предпочитают делиться через Facebook // Media бізнес (http://www.mediabusiness.com.ua/content/view/40637/126/lang,ru/). – 2014. – 11.09).***

***

Facebook начинает показывать своим пользователям количество просмотров, которые получают видео в социальной сети. Данные будут демонстрироваться для публичных видео пользователей и владельцев бизнес-страниц. Ранее сведения были доступны только владельцам публичных страниц.

Ф. Симо, директор по управлению продуктами (видео) Facebook, помимо анонса новой опции предоставил некоторые статистические данные и рассказал об изменениях, которые коснулись видео в социальной сети.

Так, количество просмотров видео в Facebook увеличилось на 50 % за период с мая 2013 по июль 2014 г. С июня 2014 г. среднее количество ежедневных просмотров составляет более 1 млрд. При этом более 65 % просмотров происходит с мобильных устройств.

За прошедший год компания внесла ряд улучшений, призванных облегчить поиск видеороликов и возможность поделиться ими в Facebook.

В сентябре прошлого года соцсеть начала тестирование автоматического воспроизведения видео в лентах новостей пользователей iOS- и Android-устройств. Позже началось тестирование десктопной версии функционала. В настоящее время англоязычные пользователи могут легко изменить настройки автопроигрывания как для мобильных устройств, так и для стационарных ПК. Русскоязычным пользователям пока доступны только настройки для мобильных устройств.

В июле текущего года был улучшен алгоритм ранжирования видео, чтобы показывать пользователям более релевантные и интересные им ролики. Другая опция, которая проходит тестирование на мобильных устройствах, призвана помочь найти новые видео. Теперь, когда пользователь заканчивает просмотр записи, ему будут показаны дополнительные релевантные видео, которые могут его заинтересовать.

В мае 2014 г. владельцы публичных страниц получили расширенные метрики для видео. Нововведение позволило им осуществлять детальный анализ взаимодействия пользователей с содержимым ролика.

Целевая кнопка Call-to-action – это один из инструментов, позволяющих владельцам публичных страниц после окончания видеоролика пригласить пользователей посетить веб-сайт компании и получить больше информации, посмотреть больше видео или сделать покупку.

«Цель новостной ленты Facebook – предоставить подходящие истории подходящим людям в подходящее время. И всё больше пользователей чем когда-либо смотрят, делятся и выражают себя через видео в социальной сети. Мы стремимся сделать Facebook лучшим местом для того, что находить, делиться и смотреть видео», – отметил Ф. Симо ***(Facebook показывает количество просмотров видео пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_pokazyvaet_kolichestvo_prosmotrov_video_polzovateley). – 2014. – 12.09).***

***

Мелкое нововведение было на днях реализовано в Facebook Messenger. Теперь перед отправкой изображения у пользователей программы появилась возможность сделать графические пометки, нарисовать которые можно с помощью пальца. Если заниматься рисованием нет никакого желания, то можно оставить текстовый комментарий.

Удивительно, но в настоящее время новая функция доступна только владельцам устройств на базе Android. Всем, кто захочет её опробовать, придётся скачать последнюю версию программы.

Напомним, что Facebook Messenger работает по принципу sms-сообщений и других мобильных приложений для отправки сообщений и создан для того, чтобы пользователи моментально получали сообщения на телефон. С недавних пор Facebook принудительно вынуждает пользователей воспользоваться новой программой – в обычном мобильном приложении соцсети возможность обмена сообщениями была отключена ***(В Facebook Messenger появилась возможность отправлять фотографии с комментариями // InternetUA (http://internetua.com/v-Facebook-Messenger-poyavilas-vozmojnost-otpravlyat-fotografii-s-kommentariyami). – 2014. – 8.09).***

***

Украинские разработчики выпустили приложение Staremap, которое в режиме реального времени показывает фотографии, которые публикуют

пользователи «ВКонтакте» и Instagram. Сервис представляет собой карту мира, где можно выбрать любую точку и посмотреть, какими фотоснимками поделились люди из выбранного региона. Например, можно посмотреть, что сейчас публикуют жители Донецка, Луганска, ваши соседи или даже депутаты Верховной Рады. Можно также настраивать фильтры – указать за какой период показывать снимки и в каком радиусе от центральной точки, пишет AIN.UA (http://ain.ua/2014/09/08/539699).

В будущем к источникам фотографий добавится Google+ и Facebook. Правда, с последней социальной сетью есть нюанс – из-за настроек безопасности там можно будет посмотреть только фотографии ваших друзей. В ближайшее время также появятся мобильные версии приложения под Android и iOS ***(Украинцы запустили сервис, который показывает, какие фотографии публикуют в сети ваши соседи // AIN.UA (http://ain.ua/2014/09/08/539699). – 2014. – 8.09).***

***

Мобильное приложение социальной сети «Одноклассники» для платформы iOS вернулось в интернет-магазин приложений AppStore. Об этом сообщили «Ленте.ру» в компании.

Приложение было удалено из AppStore более четырех месяцев назад в начале мая текущего года. Причины удаления мобильного приложения в компании не раскрывают.

Приложение перед возвращением в интернет-магазин было обновлено. В частности, теперь пользователь «Одноклассников» через iOS-приложение может отмечать свое местоположение при публикации поста как в своем профиле, так и в группах, в которых он состоит. К посту будет прикладываться карта с обозначением места (выбрать можно из списка или указать самостоятельно).

Кроме того, стала возможна отправка изображений внутри сообщений (как и в браузерной версии сайта). Изображение можно выбрать из галереи своего iOS-устройства или сделать фотографию с помощью камеры.

Однако в обновленном приложении социальной сети отсутствует сервис для прослушивания музыки. В компании «Ленте.ру» сообщили, что его планируется вернуть в ближайшее время, хотя отказались сообщить причины удаления сервиса ***(Приложение «Одноклассников» для iOS вернулось в AppStore // InternetUA (http://internetua.com/prilojenie--odnoklassnikov--dlya-iOS-vernulos-v-AppStore). – 2014. – 13.09).***

***

Социальная сеть Facebook подготовила к релизу собственный сервис обмена исчезающими сообщениями. Компания проводит тестирование новой возможности, сообщает cybersecurity.ru

Представители социальной сети утверждают, что возможность устанавливать время от одного часа до семи дней, после которого контент

автоматически будет исчезать, – это «небольшой пилот» для приложения iOS.

Сообщение, для которых будет избран срок действия, по его окончании не смогут использовать другие пользователи.

Такая опция в настоящее время доступна пользователям в Новой Зеландии, где и ранее Facebook и другие технологические компании проверили свои продукты и услуги.

Быстрые темпы роста Snapchat – популярного приложения обмена эфемерными сообщениями – с момента его основания заставили задуматься конкурентов. Эфемерные сообщения, которые со временем исчезают, становятся все популярнее среди подростков – целевой аудитории, о внимании которой мечтают большинство крупных технологических компаний ***(Facebook тестирует исчезающие сообщения // Media бізнес (http://www.mediabusiness.com.ua/content/view/40643/126/lang,ru/). – 2014. – 12.09).***

***

Facebook анонсировал запуск нового потока, который должен упростить интеграцию приложений с социальной сетью. Через несколько недель этот поток будет использоваться по умолчанию для интеграции нового приложения с социальной сетью или во время её расширения на новую платформу.

«В первоначальном потоке создания приложения пользователи должны были найти и скачать последнюю версию комплекта средств разработки SDK Facebook, создать идентификатор приложения в социальной сети, включить платформу, для которой они разрабатывают, и затем скопировать и вставить конкретную информацию между документами Facebook и средой разработки – и всё это одновременно с попыткой прочитать нашу документацию», – объясняет представитель социальной сети Д. Сошников.

«Мы всегда стараемся улучшить пользовательский опыт для разработчиков и интеграция с Facebook – один из примеров. В потоке регистрации нового приложения мы упростили процесс и добавили интерактивные руководства, чтобы направлять разработчиков в процессе интеграции приложения с Facebook. Теперь мы будем отображать только шаги, относящиеся к конкретным приложениям. Кроме того, загрузка SDK встроена наряду с кодом, который теперь можно скопировать и вставить в приложение», – добавил он.

Facebook также облегчил доступ к остальным частям документации и установил руководства для iOS, Android, Canvas и веб-сайтов. В будущем компания также планирует установить руководства для дополнительных платформ.

Разработчики, пользующиеся платформами, которые не поддерживаются новым потоком (например, Windows Phone), смогут использовать старую версию ***(Facebook упростил интеграцию сторонних***

приложений с социальной сетью // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_uprostil_integratsiyu_storonnih_prilozheniy_s_sotsialnoy_setyu). – 2014. – 12.09).

***

На просторах Интернета появилась новая социальная сеть – «Facebook для богатых» или, как она официально называется, Netropolitan. Специальный сервис презентует себя как «интернет-клуб для людей, у которых больше свободных денег, чем времени».

В социальной сети для людей со «свободными деньгами» не будет рекламы. Сам сайт не будет индексироваться поисковыми системами. А модераторы круглосуточно будут готовы решить любые возникшие проблемы или пресечь неподобающее поведение пользователей: например, если кто-то будет активно публиковать спам или рекламу в своих личных интересах.

Для того, чтобы зарегистрироваться «в социальной сети для избранных» необходимо заплатить 9 тыс. дол. в качестве членского взноса. А чтобы оставаться частью сообщества и впредь, ежегодно придется вносить по 3 тыс. дол. Разработчики социальной сети полагают, что довольно высокий вступительный взнос позволит Netropolitan остаться по-настоящему эксклюзивной и частной площадкой. Кроме того, стать членом клуба можно только с 21 года, а при регистрации обязательно нужно указывать свое настоящее имя и фамилию.

Несмотря на дороговизну пользования соцсетью, ее разработчики уверены – их детище будет пользоваться популярностью. Основатель Netropolitan Д. Тоучи-Петерс считает: «Я уверен на 100 процентов, что подобная социальная сеть необходима и будет востребована». Он говорит, что всегда существует потребность у людей общаться «со своей средой» и разговаривать «о своем». К тому же, надо полагать, аккаунт в Netropolitan в скором времени станет одним из атрибутов престижа.

Основатели соцсети говорят: «Мы рассматриваем Netropolitan, как любой другой закрытый клуб. Любой частный клуб имеет свои членские взносы и правила. Так вот Netropolitan и есть такой обычный клуб, только онлайн, цель которого объединить людей определенного круга по всему миру» ***(В интернете появился «Facebook для богатых» // Индустриалка (http://iz.com.ua/mir/53146-v-internete-poyavilsya-facebook-dlya-bogatyh.html). – 2014. – 18.09).***

***

Компания Facebook готовит к презентации приложение под кодовым названием Moments, которое позволит приватно делиться контентом.

Настройки приватности в Facebook неоднократно подвергались нападкам критиков, считающих, что в соцсети слишком сложно разобраться

с защитой своего личного контента от чужих глаз. Одной из «жертв» неправильного выставления настроек стала даже сестра М. Цукерберга, опубликовавшая в общем доступе фотографии, предназначенные для друзей и семьи.

Эту проблему потенциально сумеет решить новое приложение от Facebook под кодовым названием Moments, утверждают источники TechCrunch, видевшие рабочую версию сервиса.

Все контакты пользователя в нём визуально поделены по группам, и пользователю достаточно выбрать одну из этих групп, чтобы взаимодействовать только с теми людьми, которые входят в её состав. Таким образом, как предполагается, избирательный обмен контентом станет интуитивным и более удобным.

Представители Facebook от каких-либо комментариев отказались.

Информаторы TechCrunch сравнили новое приложение с мобильным сервисом Cluster, также позволяющим обмен контентом с отдельными группами людей, например, с друзьями, семьёй, коллегами по работе ***(Facebook создаст приложение для приватного общения Moments // IT Expert (http://itexpert.org.ua/rubrikator/item/38273-facebook-sozdast-prilozhenie-dlya-privatnogo-obshcheniya-moments.html). – 2014. – 18.09).***

***

Facebook, Google, Twitter, Square и ряд других компаний планируют совместно разработать открытое программное обеспечение.

Об этом сообщила социальная сеть Facebook.

Предполагается, что программное обеспечение, создаваемое в рамках инициативы TODO, будет бесплатным и его исходники будут находиться в свободном доступе.

Проект TODO вписывается в более широкую стратегию Facebook по предложению ее технологий другим компаниям и обмену с ними инновациями для снижения издержек на создание нового программного обеспечения и подключения большего количества людей к Интернету.

Кроме того, в Facebook заявили, что намерены заняться программным обеспечением для оганизации крупномасштабного компьютинга и программной среды.

Напомним, что в 2011 г. компания Google реализовала похожий подход Kubemetes, в котором предполагалось создать программное обеспечение для работы в сети ***(Facebook, Google и Twitter совместно разработают программное обеспечение // InternetUA (http://internetua.com/Facebook--Google-i-Twitter-sovmestno-razrabotauat-programmnoe-obespecsenie). – 2014. – 17.09).***

***

Польза от социальной сети Facebook – вопрос спорный, но компания всё-таки делает нечто полезное и даже вносит вклад в движение Open Source.

Она уже выпустила несколько программ с открытым исходным кодом, а 16 сентября к ним добавилась ещё одна – Mcrouter, инструмент маршрутизации запросов к сервису кэширования Memcached.

Программа пригодится для сайтов с очень большой нагрузкой. Например, в дата-центре Facebook программный маршрутизатор в пиковые часы обрабатывает почти 5 млрд запросов в секунду. Как известно, недавно Facebook купил социальную сеть Instagram, так что нагрузка ещё больше возросла. Кроме Facebook и Instagram, такая же система установлена на Reddit.

Программа написана на C и C++ группой разработчиков при участии А. Лихтарова и А. Гриненко. Они говорят, что Mcrouter помогает оптимизировать работу Memcached при большом количестве серверов, распределяя запросы по разным пулам.

Установка Mcrouter требует минимальных изменений, а со стороны серверов ничего не меняется, маршрутизатор работает совершенно прозрачно и незаметно. Mcrouter поддерживает все обычные команды Memcached, такие как get, set, delete, а ещё несколько собственных команд для получения статистики, просмотра номера версии и т.д.

Интересно, что для технического обсуждения Mcrouter создана группа в Facebook. Правда, там пока нет ни одного содержательного комментария. Но зато и от социальной сети, оказывается, может быть польза ***(Исходный код Facebook Mcrouter // InternetUA (http://internetua.com/ishodnii-kod-Facebook-Mcrouter). – 2014. – 17.09).***

***

Генеральным директором ООО «ВКонтакте» назначен Б. Добродеев, должность операционного директора социальной сети занял А. Рогозов, ранее руководивший в компании отделом разработки. Об этом сообщила пресс-служба «ВКонтакте».

Согласно сообщению, в результате данных назначений в компании завершен длившийся более года акционерный конфликт.

«Генеральным директором ООО “ВКонтакте” назначен Б. Добродеев, фактически исполнявший полномочия генерального директора с апреля этого года. Б. Добродеев будет руководить выработкой стратегии компании, финансовой и коммерческой деятельностью “ВКонтакте”», – говорится в сообщении.

А. Рогозов, назначенный на должность операционного директора, пришел в компанию в 2007 г. и стоял у истоков создания сети, а в последние годы управлял процессами разработки сервисов «ВКонтакте», добавляют в пресс-службе. В новой должности А. Рогозов будет руководить развитием продукта и возглавит все продуктовые и технологические направления деятельности компании.

«Позиция исполнительного директора, которую с января 2014 г. занимал Д. Сергеев, будет упразднена, а сам он станет директором

холдинговой компании VK.COM», – добавляется в релизе ***(«ВКонтакте» получила нового руководителя // InternetUA (http://internetua.com/vkontakte--polucsila-novogo-rukovoditelya). – 2014. – 18.09).***

***

Зачем Mail.ru поглотила «ВКонтакте»

Сделку по приобретению 48,01 % акций «ВКонтакте» компанией Mail.ru за 1,47 млрд дол. и получение таким образом полного контроля над социальной сетью (всего за период с 2007 г. на приобретение долей в ней было потрачено 2,07 млрд дол.) можно вполне обосновать с экономической стороны. Российский холдинг, общая месячная аудитория проектов которого пробила 100-миллионный рубеж еще год назад, получит весомую прибавку после поглощения популярного сервиса П. Дурова. Неплохо он будет смотреться и в одном портфеле с русскоязычными социальными сетями второго эшелона «Мой Мир» и «Одноклассники», почтовым сервисом и порталом Mail.ru и известным сайтом поиска работы HeadHunter.

Управляющий партнер AVentures Capital А. Колодюк назвал сделку давно ожидаемой. По его мнению, она должна привести к большей коммерциализации «ВКонтакте». «Надеюсь, теперь Mail.ru будет вынуждена решать вопрос пиратства, так как является публичной компанией, и это отразится на курсе ее акций». Феноменальный успех «ВКонтакте» на просторах рунета принято связывать с размещением в этой социальной сети большого количества нелегального аудио- и видеоконтента. Сообщения в СМИ о приобретении нового актива положительно сказались на стоимости ценных бумаг Mail.ru.

«Для меня лично это хорошая новость, – продолжает основатель и генеральный директор Clickky и управляющий партнер стартап-инкубатора WannaBiz В. Роговский. – Это однозначно говорит о том, что будет больше уделяться внимания монетизации пользователей сети, и, соответственно, откроется больше возможностей для рекламных сетей и агентств». По его словам, основатели «ВКонтакте» фокусировались на росте аудитории, но теперь пришло время научиться эффективно трансформировать ее в доходы. В первом полугодии 2014 г. выручка сервиса составила около 50 млн дол., чистая прибыль –7 млн дол.

… «Новость неожиданная, и любопытно, какими ресурсами и рычагами воспользовалась Mail.ru Group для совершения этой сделки», – признает соучредитель инвестиционного фонда Fison Д. Вишнев. Возможно, все дело в умении А. Усманова работать на благо государства и добиваться лояльного отношения властей. На вопрос корреспондента газеты Guardian, как он мог бы охарактеризовать свои отношения с российским президентом В. Путиным, несколько лет назад миллиардер ответил буквально следующее: «Как гражданина, который поддерживает своего президента и гордится тем, что у нашей страны такой лидер». Нет оснований полагать, что в настоящее время мнение изменилось.

В итоге Mail.ru Group получила еще один инструмент для заработка, став монополистом. Если учесть, что по популярности «ВКонтакте» легко может конкурировать с федеральными телеканалами первой величины, очевидно, для власти очень важно держать в «поле зрения» столь эффективный канал коммуникаций.

«Хорошо ли это для пользователя, когда все социальные сети принадлежат одной группе, покажет только время, – говорит Д. Вишнев. – Не думаю, что все будет объединено в одну, – аудитории слишком разные. Возможно, создадут привязку к одному аккаунту или отправку сообщений между сетями». Логичным шагом эксперт считает проведение анализа сетей для увеличения средней выручки с одного пользователя. С учетом рекламной практики «Моего Мира» и «Одноклассников» в сочетании с сомнительной «политикой конфиденциальности» Mail.ru Group укрепит свои возможности в таргетинге, и на страницах «ВКонтакте» появится больше рекламы.

Теперь более полная аналитика о пользователях рунета, чем у Mail.ru Group, будет разве только у «Яндекса». Большой Брат следит за тобой? ***(Зачем Mail.ru поглотила «ВКонтакте» // InternetUA (http://internetua.com/zacsem-Mail-ru-poglotila--vkontakte). – 2014. – 19.09).***

***

Бум на украинские патриотические соцсети, начавшийся весной 2014 г., дошел до абсурда – в сети возникло два проекта с практически одинаковым названием. Весной запустилась WEUA.info, а в сентябре появилась WE.UA, которую создатели называют «первой патриотической социальной сетью». По словам основателя WEUA.info Б. Олиярчука, конкурирующую сеть создали россияне. Поначалу два проекта пытались договориться между собой о совместной работе, но теперь находятся в состоянии конфликта, пишет AIN.UA (http://ain.ua/2014/09/19/541335).

Ранее на AIN.UA выходил подробный материал о сети WEUA.info, которую Б. Олиярчук с командой запустил в апреле. Основной идеей создания проекта был бойкот российских соцсетей «ВКонтакте» и «Одноклассники». Тогда Б. Олиярчук пояснил, что регистрация сайта в доменной зоне .info (а не .ua или .com, что было бы более логично) – вынужденная, поскольку на момент регистрации адрес weua.com уже был занят. Оказалось, что домен weua.com зарегистрировали россияне, причем заявку Б. Олиярчука они опередили всего на час. По словам Б. Олиярчука, позже те же люди заняли и домен we.ua. «Они мне сами звонили еще в апреле, а сейчас трубку уже не берут. Не думаю, что они хотели заработать на продаже домена – торговая марка WE стоит минимум 50–100 тыс. дол.», – рассказал Б. Олиярчук.

О российских корнях WE.UA свидетельствует ряд косвенных признаков. Если полистать страницы ресурса, можно обнаружить, что у контент-менеджеров есть проблемы с украинским языком. Других языковых версий, кроме украинской, у WE.UA не предусмотрено, однако буква «Ы» и

российские междометия периодически мелькают в сообщениях администрации.

То, что сайт сделан россиянами, констатируют и сами пользователи.

Однако у представителей WE.UA своя версия событий. Они утверждают, что создатели и организаторы проекта – украинцы, просто они проживают на территории другой страны. Что это за страна, администраторы не уточняют. «А если говорить о сотрудниках, то это люди, проживающие в разных частях Украины, – мы действительно национальный проект», – заявили они AIN.UA.

UPD: Позже представители WE.UA уточнили, в каких странах проживают основатели: «Сейчас двое основных проживают в стране (Украине. – Ред.), и один в Европе и США».

У создателей WE.UA, которые пока не раскрывают своих имен, тоже есть претензии к Б. Олиярчуку и его команде. Администраторы сети утверждают, что как только они узнали о запуске WEUA.info, то сразу выразили готовность передать им свой основной актив (домен weua.com), и предложили менеджмент для развития проекта. «Несмотря на первоначальный интерес со стороны команды WEUA.info и предварительные переговоры, ребята пропали и не дали никакого ответа, а также проигнорировали наше предложение встретиться в рамках презентации по запуску фонда Brain Basket в Киеве в апреле 2014», – рассказали в WE.UA. Представители компании говорят, что позже Б. Олиярчук снова возник на горизонте, но уже с угрозами и требованием встречи во Львове. «К тому моменту мы уже понимали, что нам не интересен вектор развития, выбранный ими, мы преследуем более возвышенные цели», – пояснили в WE.UA.

Кроме регистрационных зон .ua и .com, создатели WE.UA также заняли домены WEUA в социальных сетях в Facebook, Twitter и YouTube, однако с момента регистрации 9 мая 2014 г. никакой активности в пабликах не наблюдается.

Счетчика зарегистрированных пользователей на WE.UA нет, но если полистать страницу «Пользователи», методом простой арифметики можно вычислить, что на сегодня их насчитывается менее тысячи. Преимущественно это мертвые или рекламные страницы – живые люди пока недоумевают, в чем соль WE.UA и почему здесь такая тишина. Впрочем, администраторы утверждают, что на их сайте зарегистрировано уже 11 тыс. пользователей, активность которых составляет 40 %.

По словам представителей WE.UA, у проекта пока нет инвестора и он развивается на деньги создателей. Сколько им пришлось выложить за торговую марку WE, предпочитают держать в секрете: «Скажем так, на данный момент это самая большая инвестиция по проекту. Но согласитесь, оно того стоит. Конкретную цифру предпочитаем не раскрывать, давайте остановимся на том, что она просто большая».

А еще у новоиспеченной компании грандиозные планы – в будущем они хотят построить икубатор или бизнесс-акселератор, чтобы помогать развитию молодых украинских проектов, в идеале не только в сфере IT.

Б. Олиярчук констатирует, что WEUA.info давно «встала кому-то поперек горла». Так, еще до запуска соцсети в течение недели на нее осуществлялись мощные DDoS-атаки, из-за которых сайт работал с перебоями. Когда администраторам, наконец, удалось нейтрализовать нападения хакеров-недоброжелателей, WEUA.info запустилась в ограниченном режиме – только по приглашениям. Б. Олиярчук объяснил, что таким образом соцсеть борется с бот-аккаунтами, наплыв которых администраторы зафиксировали в первые часы работы сайта. По словам Б. Олиярчука, в ближайшие дни WEUA.info планирует выступить с официальным заявлением по поводу конкурентов из WE.UA ***(WEUA.info против WE.UA: как поссорились украинские патриотические соцсети // AIN.UA (http://ain.ua/2014/09/19/541335). – 2014. – 19.09).***

***

В Украине появилась платформа, которая позволяет найти лидеров мнений и определить рейтинг их влияния на своих друзей и подписчиков, сообщает портал «ДЕЛО» (http://delo.ua/tech/ukrainskij-startap-vyjavil-shest-kategorij-polzovatelej-facebook-278120/?supdated_new=1411316501).

Украинский стартап Publicfast проанализировал пользователей Facebook и выявил, что их можно разделить всего на шесть категорий: знаменитость, эксперт, блогер, спамер, человек, который просто проверяет ленту, и неидентифицированный.

Активных пользователей, которые среди посетителей соцсети являются достаточно популярными и знаменитыми, как оказалось, не так уж и много – всего 8 %. Пишут они не много, но имеют большое количество друзей, которое обусловлено широким кругом знакомых в реальном мире и постоянным налаживанием новых связей.

Лидеров мнений на порядок больше – около 17 %. Публикуют они тоже не много, но на определенные, иногда узкие, темы. Поэтому у них нет десятков тысяч друзей, но есть высокая вовлеченность.

Еще больше в Facebook СМИ и блогеров – 20 %. В эту категорию можно отнести новостные агентства, официальные каналы. Они много и регулярно пишут, могут иметь много подписчиков. Но так как новости у всех одинаковые, вовлеченности они не имеют.

Обычных пользователей приблизительно 50 %. Они просто что-то читают, пишут мало, у них небольшое количество друзей и низкая вовлеченность.

Спамеров, как ожидалось, всего около 2 %. Они очень похожи на СМИ, но в отличие от них имеют еще меньше вовлеченности и на порядок больше публикаций. И около 3 % пользователей не подходят ни под одну классификацию.

При определении рейтинга учитываются все лайки, репосты и комментарии, а также количество друзей и подписчиков. К другим показателям относятся охват публикаций, прогноз по количеству взаимодействий с постами на следующий месяц, а также роль пользователя в соцсети. Всего было проанализировано 100 тыс. зарегистрированных пользователей, из которых 95 % – это украинцы.

В настоящее время все пользователи в бесплатном режиме могут проверить свой рейтинг и измерить степень своего влияния в социальных сетях.

В процессе разработки алгоритма анализа пользователей в Facebook стартап выявил и ключевые различия между «ВКонтакте» и Facebook .

Например, что касается алгоритма выдачи новостей, то «ВКонтакте» по дефолту показывает все новости в хронологическом порядке, хотя пользователям доступен фильтр «популярные» – они редко им пользуются. Facebook делает наоборот, специально фильтруя новости и показывая только те, которые тебе должны понравиться, исходя из твоих предпочтений.

Другая отличительная особенность – пользователи используют Facebook в основном для публикации новостей и чтения ленты, в то время как «ВКонтакте» используется как мессенджер и музыкальный плеер.

В среднем, у пользователя «ВКонтакте» меньший показатель вовлечения, чем у пользователя Facebook.

Также в Publicfast будет добавлена и третья соцсеть – Twitter. В скором времени Twitter перейдет на алгоритм выдачи новостей, схожий с алгоритмом Facebook, что повысит вероятность заметить интересный вам твит. Также стоит отметить, что за последнее время аудитория Twitter в Украине увеличилась почти вдвое ***(Украинский стартап выявил шесть категорий пользователей Facebook // «ДЕЛО» (http://delo.ua/tech/ukrainskij-startap-vyjavil-shest-kategorij-polzovatelej-facebook-278120/?supdated_new=1411316501). – 2014. – 15.09).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

У соціальних мережах стартував флешмоб, який має на меті спонукати Президента підтримувати діалог з українцями.

Хештег #PoroshenkoPohovoryZNarodom активно пішов гуляти Інтернетом, повідомляє Еспресо.TV.

«У найскладніші для країни моменти реальні лідери нації звертаються до народу, пояснюючи причини зроблених кроків. Президент про щось домовився в Мінську. Про що – ми дізнаємося через коментарі політиків, західні ЗМІ, а також – що найгірше – через ЗМІ нашого ворога. Але не через Президента країни», – пише на своїй сторінці у Facebook ініціатор акції М. Саваневський.

«Вчора Рада проголосувала закони по Донбасу. Президент не пояснив, що це за закони і навіщо вони. І, як наслідок, знову вал здогадок та спекуляцій. Одні кричать, що П. Порошенко здав країну, інші – що він її рятує. Одні кажуть, що треба припинити платити податки, бо з держбюджету тепер будуть фінансувати сепаратистську владу на Сході, а Ю. Луценко каже – читайте уважно закони, а не заголовки ЗМІ. Закони вніс Президент. Хай виступить і пояснить свою позицію. Чи ми не гідні його уваги?» – наголошує М. Саваневський.

У соціальних мережах уже можна знайти кілька фотографій із проханням до Президента України П. Порошенка поговорити з народом.

З'явились в Інтернеті і кілька фотожаб на флешмоб ***(В Україні стартував флешмоб «Порошенко, поговори з народом» // Espreso.tv (http://espreso.tv/news/2014/09/17/v_ukrayini_startuvav_fleshmob_quotporoshenko__pohovory_z_narodomquot). – 2014. – 17.09).***

***

Вінницька обласна Рада оновила свою сторінку для користувачів соціальних мереж. На сторінці веб-сайту Вінницької обласної Ради відтепер відображаються віджети з інформацією про офіційні сторінки спільнот органу місцевого самоврядування в соціальних мережах Facebook, «ВКонтакте», YouTube та Twitter, які сьогодні здобувають дедалі більшу прихильність активних громадян української держави, повідомляє прес-служба Облради.

Зокрема, користувачі мережі Інтернет зможуть приєднатися до спільнот обласної Ради в соціальних мережах: www.facebook.com, vk.com, twitter.com,www.youtube.com. У спільнотах міститься інформація про діяльність обласної Ради, фото та відеоматеріали. Це полегшить взаємний обмін інформацією та комунікацію із читачами на зазначених веб-майданчиках, дасть можливість користувачам соціальних мереж ставити запитання і надавати свої пропозиції керівництву обласної Ради.

Щоб підписатися на новини обласної Ради або долучитися до її спільнот, варто зайти на сайт і знайти у правому нижньому куті віджети з назвами сторінок у соціальних мережах ***(Вінницька обласна Рада оновила свою сторінку для користувачів соціальних мереж // Перші новини Вінниці (http://ilikenews.com./article/vinnicka-oblasna-rada-onovila-svoyu-storinku-dlya-koristuvachiv-socialnih-merezh). – 2014. – 10.09).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Сеть микроблоггинга Twitter начинает тестирование встроенной системы покупок. С 9 сентября у пользователей в некоторых твитах появились кнопки Buy, которые позволяют посетителям покупать товары

прямо через твит. В настоящее время система работает только в США, да и то для ограниченного круга пользователей, но в конечном итоге Twitter надеется запустить эту систему в глобальном масштабе.

«Пользователи получат доступ к продуктовым предложениям и сделкам, которые являются уникальными и больше нигде не встречаются. Пользователи могут ими воспользоваться в версии приложений Twitter для Android и iOS», – говорится в сообщении компании.

Отметим, что Facebook также тестирует систему покупок на ее сайте. Она также позволяет покупать продукты, рекламируемые на Facebook.

В Twitter говорят, что вся покупка через новую систему работает буквально в пару кликов и доступна в том числе через смартфоны. Нажав на кнопку Buy, встроенную в твит, пользователь должен будет ввести адрес доставки и платежную информацию, которая напрямую передается продавцу для доставки товара ***(Twitter начинает тестирование системы покупок // IT Expert (http://itexpert.org.ua/rubrikator/item/38071-twitter-nachinaet-testirovanie-sistemy-pokupok.html). – 2014. – 9.09).***

***

На страницах соцсети «ВКонтакте» может появиться реклама, продаваемая через систему «Яндекс.Директ», рассказал газете «Ведомости» источник в одной из интернет-компаний. По его словам, контракт еще не заключен.

Исполнительный директор «ВКонтакте» Д. Сергеев и руководитель «Рекламной сети “Яндекса”» Д. Попов сообщили газете, что пока речь идет лишь об эксперименте. Д. Попов уверяет, что он уже стартовал. «4 сентября некоторые пользователи «ВКонтакте» увидели на своих страницах контекстную рекламу “Яндекс.Директ”. Это совместный тест», – сказал он.

Подробности проекта стороны не раскрывают. Близкий к одной из компаний источник говорит, что рекламу от «Яндекса» увидит только часть аудитории соцсети. А сам тест продлится около месяца. Собеседник издания отмечает, что «ВКонтакте» уже продает таргетированную рекламу, основанную на социально-демографических данных пользователей. При продаже контекста от «Яндекса» эти данные, возможно, будут использованы.

Если «Яндекс» и «ВКонтакте» договорятся, это будет гигантское событие для рекламного рынка, считает член совета директоров IMHO VI А. Ревазов. Но спрогнозировать, как вырастет выручка обеих компаний, сложно: такой крупный контракт может повлиять на весь рынок и даже спровоцировать падение цен на интернет-рекламу. А это сделает ее более конкурентоспособной по сравнению с другими видами рекламы, считает он.

Директор по цифровым продажам Dentsu Aegis Network Russia А. Чернышов считает, что речь может идти о десятках и сотнях миллионов руб. ***(Контекстная реклама «Яндекса» появится во «ВКонтакте» // ProstoWeb***

(http://www.prostoweb.com.ua/internet_marketing/internet_reklama/novosti/kontekstnaya_reklama_yandeksa_poyavitsya_vo_vkontakte). – 2014. – 8.09).

***

Генеральный директор HootSuite Р. Холмс в своем блоге на Harvard Business Review рассказывает о преимуществах нативной рекламы в социальных сетях и о том, как использовать эти преимущества с умом, пишет Marketing Media Review (http://mmr.ua/news/id/zachem-platit-za-posty-v-socialnyh-setjah-i-kak-pravilno-ispolzovat-nativnuju-reklamu-41236/).

Если вы бываете в социальных сетях, вы наверняка видели их: рекламные объявления, которые выглядят почти абсолютно так же, как обычные твиты, посты в Facebook и LinkedIn. Такие посты называются нативной социальной рекламой, и хотя мнения пользователей по их поводу варьируются от безразличия до раздраженности, результаты говорят сами за себя.

По данным AdRoll, на нативную рекламу в Facebook кликают в 49 раз чаще, чем на традиционные баннеры справа от новостной ленты. А рекламные твиты достигают уровня вовлеченности от 1 до 3 % по сравнению с 0,2 % у обычных баннеров.

Рекламодатели, разумеется, довольны: по данным аналитиков BIA/Kelsey, общие затраты на нативную рекламу в социальных сетях скоро практически утроятся – с 1,6 млрд в 2012 г. до 4,6 млрд дол. в 2017-м. Конечно, это крошечная сумма по сравнению со 121 млрд дол, которые были потрачены на интернет-рекламу в целом в этом году, но для компаний, которые в своих маркетинговых стратегиях ориентируются на социальные медиа, в реальном времени и с детальной отчетностью, нативная реклама – уникальное и многообещающее поле деятельности.

Моя компания была одной из первых адептов, нашу первую кампанию в соцсетях мы запустили в 2012 г. Сегодня мы тратим значительную часть нашего маркетингового бюджета на платную рекламу в социальных сетях, создавая и публикуя сотни постов каждый месяц на разных языках.

Отдача продолжает превышать все ожидания: реклама в соцсетях приводит к нам основную долю клиентов, причем за меньшие затраты, чем реклама, распространяемая через любые другие платные каналы. Вот мой опыт, как эффективно использовать коммерческие посты в социальных сетях.

1. Прежде, чем заплатить за размещение поста, испытайте его на читателях бесплатно.

Если у вашей компании есть аккаунты в социальных сетях, вы, скорее всего, и так ежедневно публикуете по несколько постов в Twitter, Facebook и LinkedIn. Некоторые из этих постов вызывают отклик у подписчиков, некоторые нет. Используя бесплатные аналитические сервисы, можно легко отслеживать, какие посты комментировали, на какие кликали, какие лайкали и шерили.

Именно эти, успешные, посты лучше всего подходят для рекламы. Вы уже знаете, что они работают, так что вам не придется тратить лишние деньги, чтобы понять, какие посты привлекают больше внимания. Вы просто берете старые популярные тексты и платите за то, чтобы их увидела новая, большая аудитория.

2. Используйте преимущества таргетирования.

Один из главных камней преткновения традиционной рекламы – неэффективность. Каждый раз, когда убежденный «зеленый» владелец Prius видит рекламу какого-нибудь неэкономичного джипа, который в его глазах буквально разбрызгивает бензин направо и налево, вы попросту тратите ресурсы. Реклама в социальных сетях минимизирует подобные неоправданные расходы.

В LinkedIn оплаченные материалы могут быть таргетированы на определенные регионы (страны, города и т. д.) и сферы деятельности вплоть до конкретных профессий и даже компаний. Twitter позволяет рекламодателям углубиться в области региона, пола аудитории, используемого девайса и в буквальном смысле сотни других интересных категорий. Сообщение может быть даже направлено на определенные бренды и их фоловеров, так что кампании получают доступ к подписчикам конкурентов.

Спонсорские посты на Facebook могут быть направлены на бесконечное количество групп по интересам. Если вам нужна, например, аудитория фанатов «Игр престолов» – пожалуйста. Facebook даже учитывает схожие аудитории, то есть пользователей, которые уже показали интерес к продуктам, аналогичным вашим. И во всех этих сетях вы не ограничены вашими подписчиками и фоловерами, и можете добраться до любой группы, подходящей вашему запросу.

3. Меняйте рекламу чаще.

В случае с рекламой на ТВ и другими традиционными ее видами, которые отрывают вас от чего-либо, повторение – залог успеха. Но промоутированные твиты и спонсорские посты появляются прямо в новостной ленте клиентов. Если вы будете атаковать пользователей повторяющимися сообщениями, вы не только потеряете потенциальную вовлеченность, но и вообще можете в итоге испортить свою репутацию вместо того, чтобы привлечь новых клиентов. Ключ к успеху – это свежий, постоянно меняющийся контент. Твиты и посты в основном короткие и необременительные, так что вряд ли для вас это станет проблемой.

В то же время реклама в социальных сетях может быть использована заново, если обратить ее на другую аудиторию. Показывать одно и то же сообщение разным группам – это на самом деле один из самых легких способов эффективно использовать рекламные посты.

4. Используйте A/B тестирование.

Одно их самых больших преимуществ нативной социальной рекламы – это постоянный фидбек. Уже через пару минут после публикации

промоутированного поста можно оценить его эффективность. Детальные аналитические отчеты и диаграммы показывают, кто кликает на посты и как часто.

За небольшую плату можно размещать небольшие посты, рассчитанные на ограниченную аудиторию, и получать точную, подтвержденную информацию, о том, какие сообщения работают лучше. Затем лучшие из них уже можно публиковать для широкой аудитории.

5. Изучите модели рекламных объявлений.

Разные сети продают рекламу по-разному. В Twitter компании платят по факту: каждый раз, когда юзер совершает действие (кликает, ретвитит, добавляет в избранное) – снимается плата. Facebook и LinkedIn предлагают оплату за показ – то есть деньги снимаются за показ рекламы в ленте пользователей (независимо от того, кликают на нее или нет).

Разница может показаться чисто теоретической, но важно держать эти две модели оплаты в голове, чтобы в соответствии с ними создавать твиты и посты. Например, раз мы платим Twitter каждый раз, когда пользователь кликает на нашу рекламу, важно, чтобы люди искренне интересовались тем контентом, который ждет их по вашей ссылке. Следовательно, нужно писать простые и ясные посты, а не твиты-приманки. Задача – создать подлинный интерес к сайту, а не привлечь как можно больше просмотров.

6. При создании рекламных постов не забывайте о пользователях смартфонов.

Социальные медиа потребляются преимущественно через мобильные платформы. 86 % трафика Twitter приходит из мобильных устройств, у Facebook это 68 %. Следовательно, посты должны быть адаптированы для устройств с маленьким экраном. Для твитов с их лимитом в 140 символов – это явно не проблема, а в Facebook не стоит забывать писать короткие и простые посты и сопровождать их картинками.

Тот факт, что нативные рекламные объявления просматриваются на устройствах, которые люди постоянно носят с собой, открывает уникальные маркетинговые возможности. Недавно Twitter создал функцию таргетирования платных твитов по почтовому индексу. Пользователи приезжают в какой-либо район, и в этот момент в ленте появляются посты о находящихся неподалеку пабах, химчистках или кафе. Такая технология, которая у Facebook появилась еще в 2011 г., позволяет компаниям наилучшим образом взаимодействовать с покупателями, и привлекать их внимание к специальным предложениям и акциям.

Электронная реклама считается непостоянным рынком. В 90-х кликабельность баннеров увеличилась на 5 % – до того, как пользователи научились их отключать. Но есть много причин верить, что нативная реклама в социальных сетях прослужит нам долгую службу. Нативные посты легче создавать, чем традиционную рекламу, и они достигают целевой аудитории с впечатляющей эффективностью. Кроме того, подобные посты креативны, интересны и даже полезны – новый концепт в рекламе, чье время, наконец,

пришло ***(Зачем платить за посты в социальных сетях и как правильно использовать нативную рекламу // Marketing Media Review (http://mmr.ua/news/id/zachem-platit-za-posty-v-socialnyh-setjah-i-kak-pravilno-ispolzovat-nativnuju-reklamu-41236/). – 2014. – 15.09).***

***

Социальные сети – это довольно густонаселенное место, где ежедневно расшариваются миллионы различных материалов, пишет Marketing Media Review. Пришло время узнать, чем же там любят делиться, и какие материалы гарантированно вызывают ответную реакцию? (http://mmr.ua/news/id/kakoj-kontent-rassharivajut-v-socsetjah-41196/).

Аналитики из BuzzSumo изучили 120 млн статей, и разобрались, какой тип контента предпочтительнее в Facebook, LinkedIn, Twitter и Pinterest.

1. Как создать контент, интересный пользователям Facebook

Наиболее популярный тип материалов в Facebook – тесты

Проанализировав миллион самых популярных статей в соцсети за прошедшие полгода, специалисты из BuzzSumo поделили их на категории, такие как:

Тесты

Текстовые посты

Посты с практическими рекомендациями

Видео

Викторины

Инфографики

Самым популярным типом контента оказались тесты, с количеством репостов 51 968. Для сравнения, текстовыми постами поделились всего 15 527 раз.

И у такой безоговорочной победы тестов есть объяснение. Они тешат наше самолюбие и еще раз заостряют внимание на нашей уникальности. Когда мы делимся результатами теста с друзьями, то, как бы, напоминаем им о своем присутствии, о том, что нам интересно и что для нас важно.

Длина текстовых постов в Facebook не должна превышать 2500 слов

С появлением мобильных устройств значительно ослабла наша способность на чем-то концентрировать внимание подолгу. Казалось бы, это вполне объясняет потребность в компактных постах. Однако это не совсем так.

Когда специалисты сопоставили количество расшариваний с количеством слов в посте, они обнаружили, что текст, содержащий 2000–2500 слов, лучше всего расходился в Facebook – 7 846,8 раз. Это на 15 % лучше, чем статьи с количеством слов до 500, и на 24 % больше, чем посты, содержащие от 500 до 1000 слов.

Тем не менее, если пост перешагивал порог в 2,5 тыс. слов, количество поделившихся им пользователей начинало неуклонно снижаться. Так что,

несмотря на то что ваши статьи должны быть понятными и информативными, им также не помешает быть емкими.

Оптимальная длина видеоролика в Facebook – 4 мин. 20 сек.

Видео – очень популярный контент в соцсетях. Какой же длины должен быть ролик, чтобы стать популярным?

Проанализировав 500 тыс. самых расшариваемых видео в YouTube длиной от 240 до 260 сек., специалисты обнаружили, что те же ролики в Facebook расшарили 79 859 раз. Среди всех изучаемых роликов этот результат был лучшим.

Десять лучших авторов в Facebook получают 60 % всех расшариваний соцсети

Этими авторами являются популярнейшие сайты. Из них 57 % расшариваний приходится на контент, публикуемый соцсетью YouTube.

Также пользователи Facebook очень любят вдумчивые материалы от New York Times в добавление к развлекательным статьям от BuzzFeed и Upworthy.

2. Как создать контент, интересный пользователям LinkedIn

Длина самых популярных текстовых постов в LinkedIn не превышает 3500–4000 слов

Как и обитатели Facebook, пользователи LinkedIn любят большой по объему контент. Статьи, содержащие 3500–4000 слов, расшаривались в среднем 251,9 раз, в то время как результаты статей с количеством слов 500 и менее показывали самые плохие результаты – 139,12 раз.

Причин этому может быть много, но в одном сомневаться не приходится – пользователи LinkedIn позиционируют себя как эксперты в своих профессиональных областях. Длинные, подробные посты обычно дополняются различными комментариями и результатами исследований. Расшаривая такие статьи, пользователи пытаются повысить свой статус в глазах коллег.

Тем не менее, вышесказанное не значит, что вы должны загромождать свои тексты огромным количеством ненужных цифр и фактов. Большинство опубликованных в LinkedIn аналитических статей действительно содержали в себе много профессиональной информации, но она была преподнесена таким образом, что текст было легко и понятно читать.

Подписчики LinkedIn любят статьи о самосовершенствовании

Проанализировав ключевые слова в заголовках популярных статей соцсети, аналитики из BuzzSumo обнаружили следующее:

Лидер: 433 расшаривания

Привычки: 322 расшаривания

Ошибки: 216 расшариваний

Карьера: 337 расшариваний

Менеджеры: 275 расшариваний

Уроки: 272 расшаривания

Резюме: 264 расшаривания

Сотрудники: 250 расшариваний

Интервью: 229 расшариваний

Советы: 223 расшаривания

Тренды: 219 расшариваний

Неудивительно, что такие темы, как лидерство, карьера и интервью занимают лидирующие позиции, ведь LinkedIn как раз предназначена для рабочих целей. Но, тем не менее, такие слова как «привычки», «уроки» и «советы» ясно дают понять, что пользователи соцсети заинтересованы в самосовершенствовании. А тот факт, что среди главных тем фигурирует слово «тренды» говорит о том, что юзеры озабочены вопросами будущего своих профессиональных отраслей.

3. Как создать контент, интересный пользователям Twitter

Популярные темы в Twitter варьируются от спорта до климатических изменений

При анализе наиболее интересных пользователям Twitter тем, специалисты из BuzzSumo обнаружили, что у подписчиков Twitter есть много общего с аудиторией LinkedIn. Пользователи Twitter тоже озабочены успехом и продуктивной рабочей деятельностью. Но, в отличие от аудитории LinkedIn, у пользователей Twitter есть и другие интересы помимо самосовершенствования.

Десять наиболее популярных в Twitter тем:

Спорт (1239 расшариваний)

Вегетарианство (971 расшаривание)

Успех (935 расшариваний)

Производительность (922 расшаривания)

Предпринимательство (844 расшаривания)

Психология (833 расшаривания)

Наука (831 расшаривание)

Викторины (775 расшариваний)

Климатические изменения (755 расшариваний)

Счастье (738 расшариваний)

Другие популярные в Twitter темы включают в себя: технологии, путешествия, рекламу, контент-маркетинг и здоровье.

Длина заголовков статей в Twitter должна составлять 40–50 знаков

Важно помнить о длине заголовков, особенно в Twitter, где на них стоит ограничение. Поскольку расшаривают в данной соцсети именно заголовки, то 50 знаков – это оптимальный вариант для того, чтобы осталось место для комментариев.

Если никак не получается сократить заголовок до 50 знаков, то «опасный» предел, за который не нужно выходить – это 80 знаков. Из 1 млн самых расшариваемых статей только у 12 % длина заголовка составляла 80 знаков.

4. Как создавать контент, интересный пользователям Pinterest

В Pinterest правят рецепты

Если вы пишете книги на кулинарную тематику и еще не зарегистрировались в Pinterest, то вы очень много упускаете. Здесь все, что связано с приготовлением пищи, стоит на первом месте. Конечно, пользователям интересны и другие темы:

Еда
Сделай сам
Свадьбы
Искусство
Дети
Мода и стиль
Декор интерьера
Красота
Садоводство
Вдохновляющий контент

В Pinterest очень популярны инфографики, даже касающиеся бизнеса

Если ваша компания работает по принципу «бизнес для бизнеса», то вы, вероятно, думаете, что вам не место в Pinterest. Однако и для таких случаев есть свое решение – инфографики. К примеру, инфографика, рассказывающая, в какие дни лучше публиковать контент в Facebook, собрала 674 пина.

Срок годности пинов гораздо дольше, чем у постов в Facebook или Twitter

Как часто, вбив в поиск Google какой-либо термин, в первых десяти позициях выдачи вы получали пост из Facebook или Twitter? Редко. А пин из Pinterest? Тоже редко, но все же чаще, чем посты из других соцсетей.

Чем этот факт может быть полезен для маркетологов? Если аудитория поровну разделена между тремя соцсетями – Facebook, Twitter и Pinterst, предпочтение нужно отдать Pinterest. Чем больше пинов, тем больше вероятность появления контента в чьем-то пинборде, а затем и в чьих-то результатах поисковой выдачи ***(Какой контент расшаривают в соцсетях // Marketing Media Review (http://mmr.ua/news/id/kakoj-kontent-rassharivajut-v-socsetjah-41196/). – 2014. – 11.09).***

***

С октября 2014 г. все владельцы платежных карт французского банка Banque Populaire Caisse d'Epargne, которые зарегистрированы в микроблоге Twitter, получат возможность переводить средства с одного банковского счета на другой посредством сообщений в социальной сети.

Услуга доступна благодаря мобильному приложению для перевода средств S-money, которое было разработано службами банка.

Данные о том, как будет работать система, пока засекречены, однако стало известно, что мобильный кошелек S-money будет интегрирован в социальную сеть Twitter, что позволит быстро совершать транзакции между владельцами аккаунтов.

Ж. Форель, главный исполнительный директор Groupe BPCE, ответственный за коммерческий банкинг и страхование, отметил, что эта инициатива является примером инновационной стратегии банка в отношении платежей.

BPCE стал первым банком, который предложит физическим лицам платежное решение, существенно упрощающее процесс перевода средств. Сервис S-money открывает много возможностей для осуществления платежей в социальных сетях ***(Французы смогут переводить деньги через Twitter // InternetUA (http://internetua.com/francuzi-smogut-perevodit-dengi-cserez-Twitter). – 2014. – 17.09).***

***

Социальная сеть Facebook изменила политику отображения рекламы.

Теперь пользователи могут указать причину неприязни к конкретному объявлению. Это позволит улучшить релевантность рекламных объявлений в новостной ленте для всех пользователей соцсети. В то же время компания отмечает, что изменение не скажется на количестве рекламных показов.

Новая политика призвана отсеять неуместную рекламу и грамотно распределить потоки объявлений среди всех пользователей социальной сети.

Алгоритм фильтрации не уточняется, однако кое-какие нестыковки в нем уже выявлены – случайная или злоумышленная блокировка объявления может привести к искажению всей рекламной статистики в целом. Также предполагается, что после указания причины блокировки пользователь может ощутить на себе эффект плацебо ***(Facebook разрешил указывать причину блокировки рекламы // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_razreshil_ukazyvat_prichinu_blokirovki_reklamy). – 2014. – 18.09).***

***

Популярный фотосервис для мобильных телефонов и планшетов Instagram объявил о начале размещения рекламы в лентах пользователей, пишет bbc.co.uk

Соцсеть обещает вводить рекламу постепенно и ненавязчиво, однако отмечает, что не может обойтись без этого непопулярного шага – в следующем году Instagram планирует выйти на самоокупаемость, а значит, должен начать зарабатывать деньги.

В 2014 г. компания опробовала систему размещения рекламы на некоторых пользователях в США.

Instagram обещает, что рекламные публикации будут максимально похожи на обычные пользовательские фотографии, и сначала реклама будет приниматься от тех компаний, которые уже самостоятельно ведут свои корпоративные ленты ***(В соцсети Instagram появится реклама // Media бізнес (http://www.mediabusiness.com.ua/content/view/40692/126/lang,ru/). – 2014. – 18.09).***

***

Крупнейшая социальная сеть Facebook запустила Facebook Media – новый ресурс, который поможет организациям средств массовой информации и общественным деятелям более эффективно взаимодействовать с Facebook. Новая платформа смоделирована по образцу Facebook for Business, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-predstavil-facebook-media-novyj-resurs-dlja-medijnyh-organizacij-i-obschestvennyh-dejatelej-41318/).

Н. Грудин, директор социальной сети по вопросам партнерства со средствами массовой информации, объяснил цель создания ресурса в блоге:

«Ежедневно создатели контента во всем мире, начиная от интернет-издателей и заканчивая общественными деятелями и продюсерами видео, используют Facebook, чтобы связаться со своей аудиторией инновационными способами.

В Facebook мы обязуемся построить платформу, которая расширит эти связи, обогатит и сделает их более динамичными. По этой причине мы сегодня представляем пользователям Facebook Media – чтобы выделить отличные примеры и новые тренды, иллюстрирующие то, как общественные деятели, организации и средства массовой информации используют Facebook для связи со своей аудиторией».

Новая платформа содержит множество практических советов, полезных для тех, кто использует социальную сеть в качестве маркетингового инструмента. Например, список советов по привлечению реферального трафика на публичные страницы.

Для достижения этой цели Facebook Media предлагает владельцам публичных страниц чаще постить информацию; делиться ссылками, фото и разнообразным контентом; загружать видео, к которому добавлена целевая кнопка call-to-action, побуждающая пользователей посетить веб-сайт; создавать контент с социальным контекстом, который вызовет у пользователей желание поделиться им с другими людьми; указывать в тегах поста другие публичные страницы в Facebook, привлекая их поклонников к своему ресурсу ***(Facebook представил Facebook Media – новый ресурс для медийных организаций и общественных деятелей // Marketing Media Review (http://mmr.ua/news/id/facebook-predstavil-facebook-media-novyj-resurs-dlja-medijnyh-organizacij-i-obschestvennyh-dejatelej-41318/). – 2014. – 19.09).***

СОЦІАЛЬНІ МЕРЕЖІ
І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив
мережевого спілкування на особистість

Сотрудники лондонского Имперского колледжа поделились интересными исследованиями на одном из саммитов, посвященных здоровому образу жизни. Как оказалось, популярнейшие сейчас во всем мире социальные сети, в которых общаются люди самых разных стран и разных возрастов, активно способствуют процессу похудения. Причем, избавиться от лишнего веса в большей степени удается тем людям, которые имеют аккаунты в Facebook и Twitter. Эти соцсети пользуются огромной популярностью, а сообществ и тематических групп, в которые объединяются люди, желающие похудеть, в них великое множество. Согласно статистике Министерства здравоохранения страны, от ожирения страдает каждый пятый ребенок Великобритании. Ежегодно страна вкладывает свыше 4 млрд фунтов стерлингов, чтобы приобщить людей к здоровому образу жизни. Тем не менее, заметных результатов до сих пор не было.

Британские ученые Имперского колледжа нашли легкий и не затратный способ похудеть. Они сравнили результаты 12 исследований, которые анализировали влияние на интернет-пользователей социальных сетей разного рода тематических приложений. Оказалось, что последние заметно отражаются на индексе массы тела человека. 1884 добровольца, принявших участие в эксперименте, продемонстрировали снижение индекса на 0,64. Это немного, но именно с социальными сетями открылось новое направление работы в области снижения лишнего веса. И над ним нужно упорно работать, учитывая его перспективу.

«Интернет – прекрасный способ сбросить лишний вес. К примеру, в социальных сетях можно получить консультацию специалиста, просто сидя дома в кресле. Врачи способны обслуживать одновременно нескольких клиентов. Да и давно доказано, что худеть большой компанией – гораздо проще с психологической точки зрения. А здесь таких желающих предостаточно», – отмечают медики ***(Социальные сети помогут похудеть // Узнай Всё (http://www.uznayvse.ru/zdorove/sotsialnyie-seti-pomogut-pohudet-69977.html). – 2014. – 12.09).***

Маніпулятивні технології

В останні дні почастішали випадки ворожої пропаганди вже в Чернігівській області. Особливо «капають на мізки» тим родинам, чиї чоловіки перебувають у зоні АТО. Недостатньо проінформоване і населення північних районів області, особливо у селах, куди не доходять сигнали українського радіо і телебачення, а тому може назрівати паніка. Сьогодні (8.09.2014. – Ред.) представники регіонального медіа-центру Міноборони України та журналісти говорили про шляхи протидії інформаційним атакам з боку Росії.

Інформаційний простір Чернігівської області вже почали атакувати російські пропагандисти. Наші ж люди, за браком об'єктивної інформації, починають панікувати. За словами начальника регіонального медіа-центру Міноборони України В. Мисника, усі факти витоку неправдивої інформації перевіряють.

Особливо активно російські пропагандисти працюють у соцмережах. Хакери атакують патріотичні українські групи і пишуть там неправдиву інформацію. Сіють паніку і серед родин, чиї чоловіки перебувають у зоні АТО, особливо коли батальйони вступають в активну фазу боїв.

Від імені офіційних українських джерел пропагандисти виходять і на ЗМІ та поширюють інформацію, яка не відповідає дійсності. На прес-конференції В. Мисник закликав журналістів об'єднатися і починати протидіяти атакам з боку Росії. Особливо там, куди об'єктивні дані не завжди доходять. Для нас це дуже важливо, бо Чернігівщина – прикордонна область. А тому вже наступного тижня журналісти обговорюватимуть питання створення єдиного інформаційного пункту, де військові, силовики та прикордонники об'єктивно інформуватимуть українські ЗМІ, а ті у свою чергу – населення всієї області ***(Чернігівщина готується до інформаційної війни з Росією // Чернігівщина: події і коментарі (http://pik.cn.ua/11636/chernigivshchina-gotuetsya-do-informatsiynoyi-viyni-z-rosieyu/). – 2014. – 8.09).***

***

Російська пропаганда продовжує тішити своєю недолугістю. 7 вересня в російських ЗМІ було поширено інформацію про нібито проведений у Венеції мітинг проти дій української влади.

За даними російських ЗМІ, у ньому взяли участь від 60 до 200 учасників. Правда, на єдиному фото, яке наразі є доступним, видно, що в заході взяли участь 4–5 осіб. Але хіба це проблема для російської пропаганди?

Для посилення ефекту про захід у Twitter через ботів було розміщено близько 3 тис. однотипних твітів з одним єдиним повідомленням «В Венеции прошел митинг против действий властей Украины».

Велику кількість повідомлень було зроблено чомусь ботами з напівоголеними жінками на аватарках ***(Напівоголені боти намагаються переконати в Твітері, що у Венеції відбувся мітинг проти України // UkrainianWatcher (http://watcher.com.ua/2014/09/08/napivoholeni-boty-namahayutsya-perekonaty-v-tviteri-scho-u-venetsiyi-vidbuvsya-mitynh-proty-ukrayiny/). – 2014. – 8.09).***

***

Министр обороны Финляндии К. Хаглунд заявил, что Москва ведет против Хельсинки информационную войну, а сам он стал жертвой интернет-троллинга. Об этом сообщает Цензор.НЕТ со ссылкой на Эхо Москвы.

Речь идет о большом количестве схожих по содержанию комментариев на его страницах в Facebook и в Twitter. По словам К. Хаглунда, трудно оценить, являются ли записи в Интернете активными действиями российских властей, но он допускает, что такая возможность существует. Министр и глава Шведской народной партии добавил, что Россия пытается с помощью новостей и Интернета влиять на общественное мнение, как внутри страны, так и за рубежом. По его словам, искажения информации связаны с украинским кризисом.

Эту точку зрения разделяет и специалист в области кибербезопасности, профессор университета А. Лимнелл. В интервью немецкому изданию «Вельт» он заявил, что Запад пока не знает, как можно реагировать на такой тип пропаганды, которая скрыто манипулирует общественным мнением.

Согласно данным последнего соцопроса, почти половина жителей Финляндии – 43 % – считают Россию угрозой. В марте, после присоединения Крыма, так считала четверть опрошенных ***(Министр обороны Финляндии обвинил Россию в гибридной кибервойне // Цензор.НЕТ (http://censor.net.ua/news/302655/ministr_oborony_finlyandii_obvinil_rossiyu_v_gibridnoyi_kibervoyine). – 2014. – 15.09).***

***

Добровольчий батальйон територіальної оборони Донецької області «Донбас» заявляє, що в соціальних мережах створюють їхні фальшиві акаунти та групи. Про це повідомляється на сторінці батальйону у Facebook.

Невідомі особи створили у Twitter фальшивий акаунт батальйону – @Donbass_Forces. Як зазначають у батальйоні «Донбас», небезпека цього акаунту в тому, що він пропонує надсилати інформацію про терорситів на невідомий e-mail russobit2007@ukr.net. Водночас користувач Twitter @Donbass_Forces заявляє, що в його діях немає нічого незаконного.

Існує також фейковий акаунт бійця батальйону @ru_988.

Крім цього, батальйон «Донбас» закликав інтернет-користувачів перевірити свою присутність у несправжніх групах «ВКонтакте» та скаржитися на них. Ідеться про http://vk.com/bn_dr (із 14300 підписників) та http://vk.com/batdonbass (2588).

Справжня група батальйону «Донбас» у соцмережі «ВКонтакте» знаходиться за адресою: http://vk.com/teroboronadonbass, а справжній (хоч і порожній) аккаунт у Twitter – http://twitter.com/bnDonbass ***(У соцмережах з'явилися фейкові аккаунти батальйону «Донбас» // «Телекритика» (http://osvita.mediasapiens.ua/material/34494). – 2014. – 11.09).***

***

Государственная служба по чрезвычайным ситуациям Украины опровергает информацию о выбросе ртути в Днепровском районе Киева. Об этом сообщили в пресс-службе ГосЧС.

«Это фейковое сообщение. У нас взломали электронную почту и отправляют от нашего имени информацию», – сообщили в пресс-службе ведомства.

Ранее отдельные СМИ со ссылкой на пресс-службу ГосЧС сообщили об эвакуации жителей Днепровского района Киева в связи с превышением допустимого содержания ртути на территории завода Радикал.

«11 сентября в 9:42 на территории, прилегающей к ОАО Завод Радикал по адресу г. Киев, ул. Краснoткацкая, б. 61, было установлено опасное для жизни и здоровья жителей Днепровского района превышение предельно допустимых концентраций ртути в почве (в 1,7·104 раз), воде близлежащего озера Лесное (в 4·103 раз) и воздухе (в 3·103 раз). Причины происшествия устанавливаются», – говорилось в сообщении, разосланном с адреса пресс-службы ГосЧС ***(От имени ГосЧС хакеры распространяли фейковые сообщения // InternetUA (http://internetua.com/ot-imeni-goscs-hakeri-rasprostranyali-feikovie-soobsxeniya). – 2014. – 11.09).***

***

26 октября волеизъявление мариупольцев может не ограничиться голосованием на досрочных выборах в Верховную Раду. Именно в этот день в городе предлагают провести еще и плебисцит об отделении Мариуполя от Донецкой области, пишет i24.com.ua. Призыв пока распространяется в соцсетях, а на специально созданной странице в Facebook он звучит так:

«Друзья! Мариупольцы! Если вы ПРИНЦИПИАЛЬНО согласны прийти и высказаться за отделение МАРИУПОЛЯ от Донецкой области, присоединяйтесь к этому мероприятию. Детали (Приазовский край, Запорожская область, город республиканского подчинения) не важны. Главное ЭТО ВАШЕ МНЕНИЕ!» ***(В соцсетях разворачивается кампания по отделению Мариуполя от Донецкой области // КИД (http://zadonbass.org/news/society/message_84369). – 2014. – 13.09).***

***

Адміністрація сервісу YouTube видалила на своєму відеохостингу акаунт російського телеканалу Lifenews. Відповідне повідомлення оприлюднено на головній сторінці акаунту, пише Корреспондент.net

(http://ua.korrespondent.net/world/3419105-YouTube-vydalyv-akaunt-rosiiskoho-telekanalu-Lifenews).

«Акаунт користувача lifenewsru був видалений внаслідок подання третіми сторонами численних скарг у зв'язку з тим, що розміщення користувачем матеріали порушували авторські права», – сказано в повідомленні адміністрації YouTube.

Як повідомляв Кореспондент.net, раніше в Україні затримали журналістів Lifenews, у яких в багажнику автомобіля виявили переносний зенітно-ракетний комплекс і відеодокази їхньої співпраці з терористами ***(YouTube видалив акаунт російського телеканалу Lifenews // Корреспондент.net (http://ua.korrespondent.net/world/3419105-YouTube-vydalyv-akaunt-rosiiskoho-telekanalu-Lifenews). – 2014. – 15.09).***

Зарубіжні спецслужби і технології «соціального контролю»

Представители Нацсовета по телерадиовещанию написали письмо основателю Facebook М. Цукербергу с просьбой обратить внимание на угрозу влияния российских пользователей на Украину. Как объяснила пресс-секретарь Нацсовета И. Докучаева, это обращение не Нацсовета, а его представителей – председателя Ю. Артеменко и первого зама О. Герасимюк, пишут «Вести» (http://vesti.ua/nauka-i-tehnologii/69905-kiev-poprosil-zawity-u-cukerberga).

В письме написано, что угроза исходит от администратора украинского сегмента Facebook, который является гражданином России. По мнению авторов, он блокирует аккаунты пользователей из Украины. «В ФБ нет места российскому ФСБ! Российский администратор украинского сегмента ФБ не может проводить свою политику!» – прокомментировала в соцсети О. Герасимюк.

В письме отмечается, что были заблокированы известные украинские блогеры, группа матерей украинских солдат: «Наша просьба – назначить руководить украинским ФБ, хотя бы на время кризиса, человека, который не имеет отношения к сторонам противостояния». Кстати, планируется, что обращение М. Цукербергу передаст посол США в Украине ***(Киев попросил защиты у Цукерберга // Вести (http://vesti.ua/nauka-i-tehnologii/69905-kiev-poprosil-zawity-u-cukerberga). – 2014. – 17.09).***

***

Российские депутаты считают, что Роскомнадзор должен проверить украинский «Яндекс», которые выдает в поиске по новостям статьи с «антироссийской пропагандой». По данным «Известий», этим вопросом озаботился зампред комитета российского парламента по IT В. Деньгин из фракции ЛДПР (что вполне ожидаемо – лидер этой фракции В. Жириновский

хорошо известен своей антиукраинской позицией), пишет AIN.UA (http://ain.ua/2014/09/08/539617).

Депутат считает, что для сайтов, принадлежащих российской компании, недопустимо показывать такие новости. Его возмутили заметки украинских СМИ, где содержатся «прямые выпады против России», данные о российской агрессии, о действиях российской армии в восточной Украине. Несложно предположить, что В. Деньгин, скорее всего, не очень разбирается в том, как работают онлайн-агрегаторы новостей, либо же подразумевает, что «Яндекс» как российская компания, должен фильтровать выдачу.

Инициативу проверить «Яндекс» на «неправильную» пропаганду поддержал и член комитета Госдумы по обороне И. Зотов. По его мнению, любая российская компания должна отвечать за свое дочернее предприятие, особенно «в вопросах, связанных с Интернетом как одним из главных на сегодня информационных каналов, формирующим общественные настроения».

В самой компании отмечают, что считают себя не российской, а международной компанией, а «Яндекс.Новости» в каждой стране показывает именно ту картину дня, которую формируют местные СМИ. «У “Яндекс.Новости” нет редакции и, соответственно, редакционной политики и своей точки зрения, сервис не создает собственные материалы, всю информацию поставляют партнеры», – заявили в компании. На yandex.ua новостные сюжеты формируются на основе сообщений украинских СМИ. Критерии, по которым новости попадают на главную «Яндекса»: цитируемость источника в других сообщениях этого сюжета, время публикации, общая цитируемость и оперативность источника ***(Роскомнадзор просят проверить «Яндекс Украина» на предмет «антироссийской пропаганды» // AIN.UA (http://ain.ua/2014/09/08/539617). – 2014. – 8.09).***

***

Облачное хранилище «Яндекс.Диск», сеть профессиональных контактов «Мой круг» и почтовый сервис «Яндекс.Почта» будут внесены в реестр организаторов распространения информации. Об этом со ссылкой на материалы ведомства сообщило агентство РБК. Роскомнадзор ведет этот реестр в соответствии с вступившими в силу 1 августа 2014 г. поправками в закон «Об информации…» (так называемый закон о блогерах), уточняется в сообщении.

С требованием внести в реестр именно эти сервисы «Яндекса» к Роскомнадзору обратилась ФСБ, пояснил РБК замруководителя Роскомнадзора М. Ксензов. Он не исключил, что в реестр попадут и другие проекты «Яндекса», но соответствующего запроса от ФСБ ведомство пока не получало. В самой компании уточнили, что Роскомнадзор по просьбе правоохранительных органов запросил у компании контактные данные для связи по вопросам работы коммуникационных сервисов. В ответ «Яндекс» направил данные для регистрации в реестре.

Согласно закону, организатор распространения информации обязан хранить на территории России в течение шести месяцев обезличенную информацию о действиях своих пользователей (например, об обмене электронными сообщениями) и делиться этой информацией со спецслужбами в случаях, оговоренных в других законах. Организатор распространения информации также должен установить специальное оборудование, которое позволяет проводить оперативно-розыскные мероприятия ***(Под действие «закона о блогерах» попали три сервиса «Яндекса» // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/09/15/yandex-swerices.html). – 2014. – 15.09).***

***

Как анонимно пользоваться Интернетом

Информация – это наиболее ценный ресурс в мире. Однако с развитием интернет-технологий получить доступ к персональным данным и конфиденциальной информации становится гораздо проще.

Кто за нами следит?

Правительство в первую очередь. «Правительство всегда следило, следит и будет следить за своими гражданами», – говорит С. Ложкин, ведущий антивирусный эксперт «Лаборатории Касперского». Ещё не забыта история экс-агента ЦРУ Э. Сноудена, который рассекретил программу Агентства национальной безопасности (АНБ) США по отслеживанию интернет-активности пользователей.

Крупные корпорации, в том числе и интернет-корпорации, следят за своими пользователями, преследуя сугубо коммерческие цели. «Они пытаются смотреть, что вы делаете в сети, и даже этого не скрывают», – говорит эксперт. Например, при регистрации почты Gmail вас предупредят, что определенные машинные алгоритмы обрабатывают содержимое вашей корреспонденции, и на анализе этого предоставляют рекламную информацию. Не удивляйтесь тому, что после того как вы сообщите своим родным о рождении ребенка, Google упорно будет рекламировать подгузники.

Телекоммуникационные компании и интернет-провайдеры. Компании, которые предоставляют доступ в Интернет, на самом деле не заинтересованы в слежке за своими клиентами, но к ним могут прийти люди из правительства с «предложением, от которого нельзя отказаться», говорит С. Ложкин. В России с 1 июля 2014 г. все интернет-провайдеры должны хранить трафик не менее чем 12 часов, причем спецслужбы получают прямой доступ к этим записям. В США три из четырех ведущих североамериканских мультисервисных операторов связи, согласно соглашению с правительством, должны предоставлять федеральным властям облегченный доступ к сетям, а также оснащать оборудованием для законной проверки и отслеживания информации.

Киберпреступники следят по заказу конкурентов и правительства в том числе. В «Лаборатории Касперского» отмечают, что среди киберпреступников очень много наемников, работающих на правительства разных стран.

Как избежать опасности?

Чтобы обезопасить свою интернет-жизнь от скрытых глаз шпиона и стать анонимным для правительства, крупных корпораций и злоумышленников, нет надобности удаляться из сети. Достаточно использовать существующие инструменты для безопасного пользования Интернетом.

1. Шифрование трафика

Сеть The Onion Router (Tor) устанавливает анонимное сетевое соединение, защищенное от прослушивания. К сожалению, TOR в большей степени заслужил славу прибежища киберпреступников, но это не уменьшает его значимость как блестящего инструмента для защиты от наблюдений. С помощью Tor можно сохранять анонимность при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями.

Сегодня сетью Tor пользуются журналисты, социальные работники, корпорации, общественные организации и даже правоохранительные органы.

«Tor немножко замедляет ваше интернет-соединение. Для браузинга и личной переписки – это вполне отличное решение, но скачивать большие объемы данных через Tor проблематично», – отмечает антивирусный эксперт С. Ложкин.

Помимо бесплатного Tor существуют и другие решения для защиты вашей анонимности – например, VPN (Virtual Private Network). С его помощью можно создать надежную и защищенную сеть. Примером защищенных VPN является OpenVPN, пользование которым стоит 5–10 дол. в месяц.

«Этот шифровой канал связи шифрует ваш трафик и полностью защищает от внешнего прослушивания. Его преимущество в том, что он работает гораздо быстрее – на той же скорости, что и ваш интернет-канал», – говорит С. Ложкин.

2. Безопасные сервисы электронной почты

Уже упоминалось, для чего и как Google «читает» почту, а спецслужбы в любой момент могут получить доступ к ней. Чтобы обезопасить переписку от чужого прослушивания, используйте безопасные почтовые сервисы, такие как ProtonMail или SAFe-mail.

ProtonMail является ответом сотрудников Европейской лаборатории по ядерным исследованиям (CERN) на скандал с АНБ. Принцип работы сервиса заключается в том, что все сообщения шифруются в веб-браузере пользователя, прежде чем они достигнут серверов ProtonMail. Ключ шифрования находится на компьютере пользователя. Это означает, что

ProtonMail не хранит пароли и не может расшифровать сообщения пользователей.

Письма между пользователями защищенной почты шифруются всегда и автоматически. Как правило, такие сервисы предоставляют возможность отправить зашифрованное послание получателю любого другого почтового клиента. В этом случае необходимо заранее договариваться о пароле с получателем. В письме приходит сообщение со ссылкой, перейдя по которой необходимо ввести пароль для доступа к содержимому письма.

3. OTR-шифрование

Для защиты личной переписки в сервисах мгновенной передачи сообщений используйте криптографический протокол Off the Record Messaging (OTR). Он позволяет шифровать передаваемые послания на клиенте отправителя и дешифровать их на клиенте получателя.

OTR позволяет зашифровать переписку в таких популярных клиентах, как Google Talk, Jabber и ICQ. К сожалению, Skype не поддерживает плагин шифрования переписки, при том он допускают одновременный логин с нескольких устройств, включая мобильные. Помимо этого, чтобы переписка случайно не попалась на глаза посторонним, не забывайте разлогиниваться.

4. Защищенная операционная система

Tails (The Amnesic Incognito Live System) – это абсолютно бесплатная операционная система, ориентированная на сохранение конфиденциальности и анонимности в сети. Tails загружается с диска или флешки, поэтому можно безопасно пользоваться практически любым компьютером. Система не устанавливается на жесткий диск ПК и не оставляет никаких следов. Tails включает в себя Tor, GPG для шифрования почты, OTR-чат, парольный менеджер KeePassX и другие программы, многие из которых модифицированы для безопасности. Графический интерфейс может подделываться под Windows XP, чтобы вызывать меньше подозрений у окружающих.

Именно этой системой пользовался Э. Сноуден, её рекомендуют такие организации, как «Фонд свободной прессы» и само АНБ для своих агентов.

«Вы получаете полностью защищенную среду с полным набором всех необходимых приложений, начиная почтой и заканчивая мессенджерами и браузерами. И вся ваша работа будет зашифрована», – говорит С. Ложкин.

Вышеперечисленные инструменты разработаны для того, чтобы защитить сохранность данных и обеспечить полную анонимность в сети. Но эти технологии ни в коем случае не защищают от вредоносного ПО. Ведь зловреды могут попасть на ваш компьютер и по защищенным каналам связи, они могут находиться там и до того момента, как вы решили стать анонимным ***(Как анонимно пользоваться Интернетом // InternetUA (http://internetua.com/kak-anonimno-polzovatsya-internetom). – 2014. – 10.09).***

***

Американские власти вынудили интернет-поисковик Yahoo! открыть доступ к конфиденциальным данным пользователей, угрожая ежедневно штрафовать компанию на 250 тыс. дол. Об этом говорится в сообщении, размещенном 11 сентября в официальном блоге поисковика, пишет «Лента.ру».

Компания опубликовала 1,5 тыс. страниц документов, связанных с судебной тяжбой с Агентством национальной безопасности (АНБ) США. Представитель Yahoo! Р. Белл в комментариях к документам пояснил, что претензии у властей к поисковику появились в 2007 г. после того, как в законодательство США были внесены изменения, позволившие требовать от интернет-компании информацию о пользователях.

Yahoo!, как отметил Р. Белл, отказалась выполнять требования АНБ, посчитав, что они нарушают конституцию, и подала на власти в суд по надзору за деятельностью иностранных разведок, где после 1,5 лет тяжб потерпела поражение. «На одном этапе правительство США грозило предъявлением штрафа в 250 тыс. дол. в день, если мы не подчинимся», – сообщил Р. Белл.

АНБ в рамках программы PRISM требовало от Yahoo! предоставить метаданные о пользователях ее электронной почты, позволяющие отследить, между кем происходит обмен сообщениями и когда. При этом доступа к самим письмам у спецслужб, как заверяют в компании, не было.

Летом 2013 г. Microsoft, Google, Yahoo!, Facebook и LinkedIn обратились в суд по контролю за внешней разведкой США после того, как благодаря деятельности Э. Сноудена стало известно об их сотрудничестве с АНБ в рамках программы PRISM по слежке за пользователями Интернета. Компании потребовали разрешить им публикацию подробной статистики запросов со стороны спецслужб о данных своих пользователей.

В феврале 2014 г. благодаря договоренностям с министерством юстиции США IT-компании опубликовали статистику запросов спецслужб за первое полугодие 2013 г.

10 сентября стало известно, что десятки крупнейших американских интернет-компаний подготовили обращение в адрес конгрессменов с призывом принять закон, защищающий конфиденциальность частной переписки ***(Вашингтон требовал от Yahoo выдачи персональных даннях // Media бізнес (http://www.mediabusiness.com.ua/content/view/40640/126/lang,ru/). – 2014. – 11.09).***

***

Специалист по безопасности Д. Здзиарски заявил, что приложение Facebook Messenger для iOS активно следит за пользователями, используя код «шпионского типа». Представители социальной сети утверждают, что подобный код нужен для аналитики приложения.

Д. Здзиарски написал в своём Twitter-аккаунте, что внутри Messenger находится «столько похожего на шпионский код, сколько он не видел даже в программах, предназначенных для промышленного шпионажа». Специалист рассказал изданию Motherboard, что приложение отслеживает практически всё, что пользователь делает внутри него – где производились касания экрана, как часто устройство переводят в ландшафтный или портретный режим, сколько времени приложение открыто на смартфоне.

Как отмечает Motherboard, многое из этого является стандартным в современной разработке, однако кое-что должно вызывать подозрения:

Facebook использует некоторые приватные API, при помощи которых может вытащить ваш Wi-FI SSID и, к примеру, отследить, к каким сетям вы подключаетесь.

Независимый специалист по безопасности А. Солтани подтвердил Motherboard, что особые отношения Facebook и Apple могли дать социальной сети привилегированный доступ к приватным функциям.

Д. Здзиарски при помощи реверс-инжинигринга приложения обнаружил, что некоторые строки оканчиваются на [“DO_NOT_USE_OR_YOU_WILL_BE_FIRED”] («не использовать под страхом увольнения»). Известный хакер Chpwn (настоящее имя – Г. Пол), работающий на Facebook, рассказал, что он сам является автором этих строк, и всё это – ничего больше, чем внутренняя шутка. Тем не менее, отмечает Д. Здзиарски, не ясно, что именно делают функции globalProviderMapData и isHeadPublisher, и почему ими нельзя было бы пользоваться под страхом увольнения.

В своём письме Motherboard Д. Здзиарски отметил, что внутри приложения много кода, который указывает на то, что Facebook пытается анализировать почти всё, чем занимается пользователь в приложении. Представители Facebook от комментариев воздержались, но указали на твиты одного из разработчиков Messenger Л. Жан, которая отметила, что компания использует подобную аналитику, чтобы глубже понимать поведение пользователей, подстраиваться под них и делать приложение «удобнее и быстрее».

Она привела в пример стикеры с огромным символом Like, которые люди использовали гораздо чаще прочих, в связи с чем разработчики приняли решение переместить их, чтобы уменьшить количество нажатий.

В середине июля 2014 г. Д. Здзиарски опубликовал доклад, в котором упомянул о фоновых процессах, запущенных на всех смартфонах Apple. По его предположению, они использовались для того, чтобы следить за пользователями. Apple в ответ опубликовала подробное описание каждого процесса – к примеру, многие из них нужны для получения диагностической информации ***(Эксперт по безопасности: «Facebook Messenger слишком активно следит за пользователями» // InternetUA (http://internetua.com/ekspert-po-bezopasnosti---Facebook-Messenger-slishkom-aktivno-sledit-za-polzovatelyami). – 2014. – 14.09).***

***

Как прослушивается Skype

Глобальные интересы стран, как показывает новейшая история, могут совпадать с интересами обычных компаний. Поэтому руководство и тех, и других заинтересовано в возможности мониторинга общения по Skype. Причины, которые побуждают к этому, очень разные, а вот цель всегда одна. Если государство собирается запретить Skype, то в бизнесе таких опрометчивых решений никто принимать не собирается. Это удобный инструмент, запрет которого может привести к огромным издержкам. Многие руководители нашли выход из положения. Если блокировать нельзя, значит, можно начать контролировать.

Вне конкурса

Первый способ, как узнать содержание чьей-то переписки, является настолько простым и очевидным, что причислять его к реальным техникам мониторинга просто не поднимается рука.

У Skype есть функция получения доступа к аккаунту сразу с нескольких устройств. Эта функция, с одной стороны, очень удобная, но с другой – она оборачивается настоящей проблемой для безопасности. Если кто-то знает ник и пароль в скайпе, то присутствие другого человека в сети можно даже не заметить. При этом такой человек сможет получать пересылаемые файлы, слышать звонки и следить за перепиской. Вся переписка окажется полностью скомпрометированной. Для такого рода деятельности, конечно, надо узнать ник и пароль. Но все логины доступны в обычном поиске по сети, а вторые можно добыть, взломав почтовый ящик и попросив Skype выслать на него «забытый» пароль.

«Минус» такого подхода заключается в том, что следить одновременно за несколькими людьми просто не получится. Про скрытность тоже не приходится говорить. Поэтому придется переходить к более сложным и специфическим методам слежения.

Вначале было слово

О расшифровках протоколов Skype говорят много, но найти конкретные решения, которые бы работали для широкой публики, пока все еще невозможно. Поэтому основные правила перехвата сводятся к тому, что нужно перехватить информацию еще до того, как программа ее зашифрует. Получается, что шпионский софт должен быть установлен на компьютере того, за кем организуется слежка. Проще всего, если рассматривать техническую сторону вопроса, перехватить звонки. Есть разные средства, которые работают «из коробки» (к примеру, Power Intercept или AnyMessageRecorder, другие подобные программы). Но такой способ перехвата информации требует предварительного физического доступа к компьютеру. Даже если добраться к нему получится, скрыть следы такой деятельности будет проблематично.

Другой способ перехвата информации можно реализовать через штатные средства Windows. Задействовать стандартный WinAPI+.NETFramework, чтобы записывать звук с микрофона. Но недостатков у такого способа будет гораздо больше, чем полезного функционала. Потому что при такой прослушке будут записаны не только разговоры, но и прослушиваемая музыка с другими посторонними шумами. Если же функция стереомикшера на компьютере отключена, то перехватывать вообще будет нечего.

Но это не единственные подходы, которые могут помочь в перехвате звонков в Skype. Более сложная схема требует использования официального набора инструментов разработчика (SDK), который предоставляется самими разработчиками. Если немного доработать SDK, то на одном из шаблонов метода получения информации о текущем звонке будет реализована запись звука с микрофона, ответы собеседника в ходе беседы.

Прямая насыщения

Как и в математике при доказательстве теорем, при перехвате Skype есть условия необходимые, а есть достаточные. В этом ключе перехват звонков – необходим, но не достаточен. Если рассматривать реальную компанию, то вряд ли потенциальный «крот», или, говоря на языке специалистов по информационной безопасности, инсайдер, будет вслух надиктовывать сообщникам бизнес-планы или номера кредитных карт. Скорее всего, он либо перешлет информацию в файле, либо отправит сообщением. Это приводит к логическому выводу о том, что для качественного мониторинга Skype необходим не только перехват звонков, но и чатов, смс, а также пересылаемых файлов. Реализовать подобный функционал также можно с помощью SDK, черпая полезные знания из открытых документов и описаний библиотеки Skype4COMLib.

Но и здесь, как обычно, присутствуют минусы. Они, конечно, не такие серьезные, как в подходах, описанных ранее, но все же. При старте приложения, написанного с использованием SDK, Skype автоматически спросит «разрешить ли доступ?». Не нужно быть экстрасенсом, чтобы предугадать ответ пользователя. Поэтому необходимо предусмотреть автоматическое «одобрение» без участия человека. Эта проблема может быть решена, к примеру, через штатные функции WindowsFindWindow, GetWindowText и ряд других. Принципы подробно расписывались во времена расцвета «угонов» электронных кошельков WebMoney несколько лет назад.

По сути, перехват информации из Skype в нынешних условиях представляет собой не что иное, как работу логгера. Но организовать перехват – это лишь половина успеха. Информацию еще нужно где-то хранить, а затем пересылать. В случае перехвата звука также необходимо заботиться об объеме файлов, т. к. писать и пересылать WAV-файлы не столько роскошь, сколько глупость (в плане сокрытия действий программы

от пользователя). Все это приводит руководителей компаний к проблеме выбора.

На распутье

Поэтому первым вариантом будет заказать у хакера написание утилиты для перехвата Skype. Вариант этот упоминается, скорее, в ознакомительных целях, потому что он сопряжен с большой долей риска.

Сама по себе такая сделка не может быть проведена официально – это первый недостаток. Второй недостаток – если деньги уплачены, а работа не сделана (или сделана плохо), то вернуть их уже вряд ли получится (потому что сделка-то неофициальная). Если подделка будет работать хорошо, все равно нет гарантий, что исполнитель не оставит для себя определенной лазейки. Он сможет получить доступ к переписке компании, а дальше все зависит от совести такого хакера: может начаться шантаж начальства и сотрудников, информация может быть передана для публикации в открытые источники. Любое развитие событий не пойдет на пользу фирме, поэтому грамотные руководители на такой шаг просто не идут.

DLP-система

Наиболее безопасным способом мониторинга Skype-активности сотрудников является использование DPL-системы. Ее название имеет полный английский эквивалент: DataLeakPrevention. Данная система специально разработана для защиты от утечки информации. Мониторинг Skype в некоторых из подобных систем уже успешно реализован. Но только единицы способны на полный перехват и анализ информации.

Кроме того, понимая важность доверия со стороны заказчиков, производители DLP-систем проходят сертификацию. Наличие сертификата означает отсутствие недекларированных возможностей, бэкдоров и т. п., и является гарантией того, что обрабатываемая системой информация не передается третьим лицам.

К минусам DLP-систем следует отнести их стоимость. Помимо этого, далеко не все системы этого класса являются модульными. То есть заказчик не может купить себе только средство контроля мессенджеров, веба или принтеров. Системы, продающиеся «целиком и сразу», вынуждают компании переплачивать за те возможности и решения, которые они не планируют использовать.

И чтобы не заканчивать на негативной ноте, взглянем на проблему перехвата Skype чуть шире. Даже если информация была успешно перехвачена и передана, ее необходимо анализировать. Читать все и всех «по старинке» нерационально. При таком подходе один офицер безопасности хорошо если способен охватить 20–50 человек. А если сотрудников несколько сотен или тысяч? Поэтому главным козырем современных DLP-систем является их способность к автоматическому анализу информации с помощью различных поисковых алгоритмов и отработка заданных политик безопасности.

Послесловие

Не так давно стало известно о том, что с 1 декабря 2013 г. Microsoft собиралась закрыть APISkype под предлогом того, что «оно морально устарело». Другими словами, все сторонние приложения (в частности, модули перехвата ряда DLP-систем), работающие в виде плагинов через API, перестанут работать. Однако на улице год 2014 г., а API по-прежнему работает. Забыли ли его закрыть, или Microsoft прислушалась к возмущенным письмам сторонних разработчиков – неизвестно. Главное, что угроза закрытия API подтолкнула разработчиков DLP-систем к пересмотру подхода перехвата Skype в лучшую сторону. Сегодня этот мессенджер перехватывается на более «универсальном» уровне. К сожалению, подробности на сегодняшний день рассказывать запрещено.

Зато любопытно другое: пару лет назад Microsoft подала заявку на патент, описывающий технологию, которая позволит перехватывать разговоры в системах интернет-телефонии. В тексте патента Skype упоминался в качестве одного из сервисов, в которых новая технология может найти применение. Если принять во внимание те факты, что в мае 2011 г. IT-гигант приобрел Skype за 8,5 млрд дол., а спустя несколько месяцев опубликовал документ с описанием технологии Legal Intercept (легального перехвата), позволяющей незаметно для пользователя считывать информацию, передаваемую по каналам интернет-телефонии, становится понятно, что ставить точку в вопросе контроля Skype еще рано ***(Как прослушивается Skype // InternetUA (http://internetua.com/kak-proslushivaetsya-Skype). – 2014. – 12.09).***

***

Администрация облачного хранилища Dropbox выпустила 11 сентября отчет по прозрачности работы компании. В дальнейшем каждые шесть месяцев Dropbox будет отчитываться перед пользователям о своем взаимодействии с властями.

Адвокат Dropbox Б. Фолькмер в блоге компании сообщил, что за первые шесть месяцев 2014 г. в Dropbox было направлено 268 запросов о разглашении информации пользователей правоохранительным органам. Вдобавок было получено от «0 до 249» запросов, касающихся национальной безопасности.

В отчете также указывается, что в Dropbox также направили 120 ордеров на обыск. Компания удовлетворила 103 запроса, предоставив следователям необходимые данные. Отметим, что 37 запросов поступили от иностранных правоохранительных органов и спецслужб.

По словам Б. Фолькмера, компания вынуждена предоставлять следователям необходимые данные в случае, если запрос корректно оформлен и все законодательные требования были выполнены. Если следователи просят выдать больше данных, чем им нужно для проведения расследования, в Dropbox пытаются в судебном порядке оспорить этот запрос.

Как следует из отчета, количество запросов о выдаче данных остается на прежнем уровне. Стоит отметить, что спецслужбы теперь просят компанию не уведомлять своих пользователей о том, что в их отношении проводятся действия следственного характера.

Б. Фолькнер заявил, что в Dropbox будут и далее придерживаться политики большей прозрачности и лучшей защиты данных пользователей. По словам адвоката, в настоящее время в Конгрессе США зарегистрирован законопроект, реформирующий систему слежения и позволяющий компаниям поддерживать более открытую беседу с пользователями ***(В первом полугодии 2014 года Dropbox получила до 249 запросов национальной безопасности // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/09/15/Dropbox-requests.html). – 2014. – 15.09).***

***

Веб-обозреватель Sogou, предназначенный для китайскоязычных пользователей, собирает о них информацию. Об этом свидетельствуют данные исследования, проведенного Д. Хьюстоном, Д. Майклсоном и Б. Эллакотом из Азиатско-Тихоокеанского сетевого информационного центра (Asia-Pacific Network Information Centre, APNIC).

В ходе конференции центра ученые отметили, что в рамках исследования использовались рекламы Google в виде встроенных GIF-файлов. Пользователь может просмотреть рекламу только при наличии подключения v6. Каждая реклама получает уникальный URL-адрес, который потом отражается в APNIC.

По словам Д. Хьюстона, этот уникальный URL-адрес должен возвращаться исключительно к APNIC, и никто другой не должен получать к нему доступ. Однако, как оказалось, в каждом одном из 400 случаев URL «утекал», что свидетельствует о ведении слежки за пользователем.

Создатели Sogou Explorer пока отказываются комментировать произошедшее ***(Китайский браузер следит за своими пользователями // InternetUA (http://internetua.com/kitaiskii-brauzer-sledit-za-svoimi-polzovatelyami). – 2014. – 17.09).***

***

За период с января по июнь 2014 г. в компанию Google поступили два запроса от украинских властей, которые касались 18 аккаунтов пользователей. Данные девяти из них были раскрыты, свидетельствуют данные отчета компании.

Масштабы правительственных запросов за последние пять лет выросли на 150 %, говорится в отчете Google Transparency Report. Правительственные запросы на пользовательскую информацию, такую как регистрационные данные, электронная почта, IP-адреса, увеличились на 15 % только за первые

полгода 2014 г. и на 150 % с момента публикации первого отчета в 2009 г., пишет CyberSecurity.

Р. Сальгадо, юридический директор по информационной безопасности Google, говорит что в США объемы запросов за первые шесть месяцев 2014 г. возросли на 19 %, а с начала ведения статистики – на 250 %. В общей сложности Google получила 31 698 запросов за первое полугодие 2014 г, из которых полностью или частично были удовлетворены 65 %. Причем, в это число не входят секретные запросы по так называемым National Security Letters или запросы по постановлению суда Foreign Intelligence Surveillance.

Р. Сальгадо говорит, что Google видела, как «некоторые страны намеренно расширяли масштабы разведовательных структур, чтобы усилить контроль за интернет-провайдерами».

В Google говорят, что призывали ранее и призывают теперь к реформе американского законопроекта об электронных коммуникациях ECPA (Electronic Communications Privacy Act) и принятия закона, известного как USA Freedom Act, запрещающего доступ к данным без судебного решения и письменного уведомления. В Google и ряде других технологических компаний утверждают, что это пойдет на пользу всему ИТ-сектору ***(Google раскрыла украинским властям данные о 9 пользователях // InternetUA (http://internetua.com/Google-raskrila-ukrainskim-vlastyam-dannie-o-9-polzovatelyah). – 2014. – 17.09).***

***

Пять основных спецслужб мира, включая американское АНБ и британскую GCHQ, совместно работают над созданием визуализации Интернета в реальном времени, в рамках программы разведки NSA Treasure Map.

Помимо сотрудников из США и их британских коллег из GCHQ в проекте участвуют спецслужбы Австралии, Канады и Новой Зеландии.

«Карта Сокровищ» предполагает создание общей карты всего Интернета, на которой можно будет отслеживать «любое устройство, в любом месте и в любое время».

Для реализации этого проекта спецслужбы собирают данные с каналов с большим трафиком, вроде телекоммуникационных кабелей.

Кроме того, обработке подвергаются перехваченные по всему миру данные с каждого подключённого устройства, включая смартфоны, планшеты и ПК.

Представители АНБ отмечают, что программа не предназначена для наблюдения, а в качестве инструмента визуализации работы всего Интернета для нужд оборонных ведомств.

Ранее в сети обнаружили «легальный» вирус, при помощи которого спецслужбы всего мира могут получать доступ к содержимому мобильных и стационарных пользовательских устройств ***(Спецслужбы пяти стран создали систему слежения за всем Интернетом // Блог***

Imena.UA(http://www.imena.ua/blog/treasure-map-five-eyes-surveillance/). – 2014. – 18.09).

***

Основатель портала WikiLeaks Д. Ассанж назвал работу Google шпионажем и сравнил компанию со спецслужбами США. Об этом он заявил в интервью BBC News, пишет «Лента.ру».

«Бизнес-модель Google – по сути, шпионаж. Компания зарабатывает около 80 процентов выручки, собирая информацию о людях, сводя ее воедино, храня и индексируя ее, создавая профили пользователей, чтобы предсказывать их интересы и поведение. Потом она продает эти профили – в основном, рекламодателям, но и другим заинтересованным сторонам тоже. В результате смысл работы Google практически идентичен Агентству национальной безопасности США», – заявил Д. Ассанж.

В ближайшее время в продажу в США выходит книга Д. Ассанжа под названием When Google Met Wikileaks («Когда Google встретилась с Wikileaks»). Наиболее громкими разоблачениями его проекта – WikiLeaks – стала публикация архивов Вооруженных сил США о войнах в Ираке и Афганистане, а также дипломатической переписки Госдепартамента США.

Корреспондент BBC News поинтересовался, почему Д. Ассанж выделяет именно Google из числа других крупных американских корпораций, которым тоже приходится считаться с правительством и сотрудничать с ним. По словам Д. Ассанжа, за счет маркетинга Google не воспринимается людьми как «большая злая корпорация». «С этим можно спорить, но я считаю, что Google сейчас является наиболее влиятельной среди корпораций и коммерческих организаций мира», – отметил он ***(Ассанж обвинил Google в шпионаже // Media бізнес (http://www.mediabusiness.com.ua/content/view/40705/126/lang,ru/). – 2014. – 19.09).***

***

Египет начал беспрецедентную слежку за пользователями всех популярных соцсетей. За онлайн-коммуникациями египтян теперь ведет зоркое наблюдение компания See Egypt, которая является «дочкой» американской фирмы Blue Coat, специализирующейся на кибербезопасности. Она предоставляет властям Египта беспрецедентную возможность проводить тщательный анализ данных из Skype, Facebook, Twitter, YouTube и других ресурсов, пишет BuzzFeed.

See Egypt летом выиграла контракт египетского правительства на оказание услуг по проверке сетевых пакетов с помощью технологии Deep Packet Inspection, которая делает возможными геолокацию, отслеживание и расширенный мониторинг интернет-трафика.

«Мы принимаем во внимание любые сообщения, любой обмен информацией, которые мы находим вызывающими обеспокоенность или к

которым мы хотели бы пристальнее присмотреться, – заявил BuzzFeed египетский чиновник, пожелавший сохранить анонимность. – Мы следим за перепиской между исламистами или теми, кто обсуждает исламизм. Мы наблюдаем за сообществами, которые мы считаем опасными».

Когда его попросили привести примеры, чиновник заявил, что участвующие в «оргиях» или «гомосексуальных актах» будут находиться под наблюдением «в целях защиты Египта».

По данным BuzzFeed, в последние недели ЛГБТ-сообщество Египта призывает геев не использовать популярное приложение для знакомств Grindr, после того как распространились слухи о том, что египетские чиновники используют этот ресурс, чтобы отследить и арестовывать египетских мужчин-гомосексуалов.

Авторы статьи приводят опубликованное пояснение МВД Египта о содержании интернет-коммуникаций, которые оно собирается отслеживать: богохульство и религиозный скептицизм; региональные, религиозные, расовые и классовые противоречия; распространение слухов и намеренная подтасовка фактов; клевета; сарказм; использование непристойных слов; призыв к подрыву опор общества; поощрение экстремизма, насилия и инакомыслия; призыв к демонстрациям, сидячим и незаконным забастовкам; порнография, распущенность и аморальность; методы обучения изготовлению взрывчатых веществ и тактикам нападения, создания хаотичной обстановки и бунта; призывы к нормализации отношений с противниками; распространение лжи и сообщений о чудесах и пр.

«Вызывает обеспокоенность то, что люди, которые не обязательно являются участниками протеста, могут внезапно оказаться под наблюдением египетских властей, потому что они поставили лайк под чьим-то статусом на Facebook или чем-то поделились в Twitter», – отметила правозащитник в британском НКО Privacy International Е. Блюм-Дюмонте ***(Египет начал беспрецедентную слежку за пользователями всех популярных соцсетей // InternetUA (http://internetua.com/egipet-nacsal-besprecedentnuua-slejku-za-polzovatelyami-vseh-populyarnih-socsetei). – 2014. – 19.09).***

***

Генеральная прокуратура Ирана потребовала от Министерства информационно-коммуникационных технологий страны заблокировать доступ к приложениям Viber, Tango и WhatsApp. Об этом сообщает Press TV.

По словам генерального прокурора Ирана, в этих приложениях распространялись «непристойные материалы», которые носили «оскорбительный характер в отношении исламских и нравственных ценностей».

Также генпрокурор отметил, что к распространению ряда указанных «непристойных материалов» имеют отношение иностранные правительства, враждебные к Ирану ***(Генпрокуратура Ирана требует заблокировать доступ к WhatsApp и Viber // InternetUA***

(http://internetua.com/genprokuratura-irana-trebuet-zablokirovat-dostup-k-WhatsApp-i-Viber). – 2014. – 21.09).

Проблема захисту даних. DDOS та вірусні атаки

Социальная сеть Facebook предложила пользователям проверку конфиденциальности, которая поможет им анализировать и контролировать, с кем они делятся своей информацией.

В ближайшие дни соцсеть будет показывать своим пользователям новое окно с предложением проверить конфиденциальность. Опция Проверка конфиденциальности активируется кликом на кнопке Let's Do It!, сама процедура займет не более двух минут.

Первый шаг помогает убедиться, что пользователь делится с нужными людьми.

Второй шаг показывает, в каких приложениях человек использовал свой аккаунт в Facebook. Можно редактировать видимость каждого приложения и сообщения от него, а также удалить приложения, которые больше не используются.

Заключительный шаг поможет просмотреть и отредактировать конфиденциальность ключевых элементов информации профиля.

Проверка доступна в любое время по клику на иконку конфиденциальности ***(Facebook обновил проверку конфиденциальности // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_obnovil_proverku_konfidentsialnosti). – 2014. – 10.09).***

***

«Яндекс» провел исследование базы паролей от ее почтового сервиса и выяснил, что инфраструктура сервиса не была скомпроментирована. Об этом говорится в сообщении пресс-службы компании, полученном «Лентой.ру».

Владельцев 150 тыс. аккаунтов «Яндекс» отправил на принудительную смену пароля. В компании отмечают, что смена пароля всеми пользователями «Яндекс.Почты» не требуется, сервис адресно направил предложение о смене пароля для тех, кого мог затронуть опубликованный список. «Лента.ру» убедилась, проверив произвольный адрес из списка, что его владельца предупреждают о возможном взломе и предлагают поменять пароль.

Об остальных скомпроментированных аккаунтах почтового сервиса известно уже несколько лет. Владельцы этих аккаунтов были предупреждены компанией и им предложили сменить пароль, но этого сделано не было. Специалисты «Яндекса» считают, что аккаунты либо заброшены, либо

создавались роботами, в том числе с целью дальнейшей продажи базы паролей.

«Речь не идет о взломе инфраструктуры Яндекса, данные стали известны злоумышленникам в результате вирусной активности на зараженных компьютерах некоторых пользователей или фишинга. Это не целенаправленная атака, а результат сбора скомпрометированных аккаунтов в течение длительного периода времени», – говорится в сообщении компании.

Компания опровергла мнение, высказанное в соцсетях, о том, что данные пользователей «Яндекса» хранятся в открытом виде – в таком виде их представили злоумышленники ***(«Яндекс» назвал причины появления в сети паролей от его почты // InternetUA (http://internetua.com/yandeks--nazval-pricsini-poyavleniya-v-seti-parolei-ot-ego-pocsti). – 2014. – 8.09).***

***

У мережі з'явилася база з 4,7 млн паролів до поштового сервісу Mail.ru. Про це повідомляє російське видання «Лента.ру».

Видання заявляє, що при перевірці бази було знайдено пароль до поштової скриньки одного із співробітників. При спробі застосувати його поштовий сервіс видав попередження, що з цієї скриньки була спроба розсилки спаму, і запропонував змінити пароль.

Невдовзі компанія Mail.ru відреагувала на появу в мережі бази з приблизно 4,7 млн паролів від поштового сервісу. У повідомленні компанії говориться, що «досить великий відсоток» опублікованих паролів – неактуальні, на момент публікації їх вже замінили власникам.

Фахівці сервісу вважають, що база стара і зібрана зі шматочків, тобто з декількох баз паролів, які були вкрадені в різний час і, скоріше за все, різними способами, за допомогою фішингу та вірусів. «Досить великий відсоток паролів зі списку вже неактуальний, тобто власники акаунтів вже встигли їх змінити. Приблизно 95 % від актуальних акаунтів вже проходять у нас в системі як підозрілі, що означає, що вони обмежені у відправці пошти, а їх власникам ми вже давно рекомендуємо змінити пароль. Що стосується решти 5 %, які виявилися невідомі нашій системі, вони були додані в базу підозрілих сьогодні і або вже отримали таке повідомлення, або отримають його до кінця сьогоднішнього дня», – пояснили свою точку зору в прес-службі Mail.ru.

Mail.ru пояснює, що превентивно заблокувати 95 % актуальних акаунтів вдалося завдяки складній системі аналізу дій акаунта за цілою низкою критеріїв. Згідно з ними для кожного акаунта ведеться динамічний рейтинг, «карма». При його падінні нижче певного параметра до користувача починають застосовуватися різні санкції, у тому числі рекомендація змінити пароль.

Фахівці з безпеки Mail.ru зазначили, що в переважній більшості випадків причиною витоку паролів стає недосвідченість або легкодумство

користувача. Основні причини злому: фішинг, віруси, прості паролі, однакові паролі на різних сервісах – спочатку ламають слабозахищеним форум, потім заходять на пошту Mail.ru. Раніше загроза виходила також від публічних мереж Wi-Fi, але вона усунена після переходу на https в пошті, а також на головній сторінці.

Експерти сервісу радять уникати простих паролів: коротких, що складаються з одних цифр або йдуть підряд на клавіатурі символів, що представляють собою словникові слова або дані, які легко дізнатися, наприклад, дату народження, номер мобільного телефону тощо. Бажано міняти пароль не рідше ніж раз на три місяці і придумувати окремий для кожного сервісу. Оскільки на практиці це складно реалізувати, рекомендується придумати унікальний пароль хоча б для поштової скриньки, який найбільш критичний з точки зору захисту даних. На комп'ютері слід встановити антивірус і не забороняти йому оновлення, оскільки відвести пароль від електронної пошти здатна майже будь-яка троянська програма ***(Хакери оприлюднили кілька мільйонів паролів до поштових скриньок Mail.ru // «Телекритика» (http://www.telekritika.ua/kontekst/2014-09-08/97860). – 2014. – 8.09).***

***

Вторая по популярности соцсеть России «Одноклассники» заморозила страницы своих пользователей, чьи электронные адреса утекли в Интернет вместе с паролями. Об этом сообщил пресс-секретарь «Одноклассников» И. Грабовский.

«Заморозили аккаунты пользователей, зарегистрированных на скомпрометированные адреса "Яндекса" и Mail.Ru, до момента, пока их владельцы не поменяют свои пароли», – сообщил «Известиям» И. Грабовский ***(Испугавшись взлома, «Одноклассники» заморозили аккаунты пользователей // IT Expert (http://itexpert.org.ua/rubrikator/item/38070-ispugavshis-vzloma-odnoklassniki-zamorozili-akkaunty-polzovatelej.html). – 2014. – 9.09).***

***

В Интернет попали базы данных пользователей электронной почты Gmail, в открытом доступе оказалось более 4,9 млн адресов и паролей.

В базе данных имеются пароли и логины русско-, англо- и испаноязычных пользователей Google. Этими данными злоумышленники могут воспользоваться не только для доступа к почте Gmail, но и к остальным сервисам Google ***(5 миллионов паролей от Gmail попали в открытый доступ // «Бизнес» (ttp://www.business.ua/articles/it/_millionov_paroley_ot_Gmail_popali_v_otkrytyy_dostup-74663/). – 2014. – 11.09).***

***

Опубликованный в сети документ, якобы содержащий почти 5 млн учетных данных пользователей сервисов Google, на самом деле является собранием паролей с различных ресурсов. Как следует из заявления техногиганта, слитая база данных не была получена хакерами вследствие компрометации систем компании.

По утверждениям экспертов Google, в случае хакерской атаки и попытки взлома системы, направленные на противостояние похищениям данных, заблокировала бы большинство попыток авторизации. Они также добавили, что сумели защитить учетные записи, попавшие в базу данных, и попросили их владельцев сменить пароли.

В компании считают, что слитая база данных могла быть получена в результате целого ряда ресурсов и посредством фишинговых кампаний. Но стоит отметить, ранее заявлялось о том, что подлинности больше чем 60 % паролей именно от сервисов Google.

Для того чтобы обезопасить свои учетные данные, техногигант настоятельно рекомендует задавать сильные пароли ***(Google: Слитая база данных паролей от Gmail не была получена в результате компрометации сайта // InternetUA (http://internetua.com/Google--slitaya-baza-dannih-parolei-ot-Gmail-ne-bila-polucsena-v-rezultate-komprometacii-saita). – 2014. – 11.09).***

***

Администрация социальной сети «ВКонтакте» заморозила 226 тыс. аккаунтов пользователей из-за того, что их почтовые ящики на «Яндексе», Mail.ru и Gmail были взломаны. Об этом стало известно благодаря сообщению пресс-секретаря социальной сети «ВКонтакте» Г. Лобушкина.

Количество замороженных аккаунтов «ВКонтакте», привязанных к почтовому сервису Mail.ru, составило 185 тыс., «Яндекса» – 31 тыс., Gmail – 10 тыс. ***(В «ВКонтакте» заблокировано 226 тысяч аккаунтов // 05366.com.ua (http://www.05366.com.ua/news/619672). – 2014. – 15.09).***

***

Правительство Китая организовало атаку человек посередине (MITM-атака) на зашифрованный трафик, передаваемый между «Образовательной» и «Исследовательской» сетью Китая (China Education and Research Network, CERNET) и Google. При этом на территории Поднебесной доступ к сайту поисковика можно получить только через CERNET.

Многие ИБ-эксперты считают, что китайское правительство следит за пользователями, посещающими сайт Google через CERNET. Кроме того, в последнее время им стали приходить сообщения об использовании такими сайтами, как google.com и google.com.hk недействительных SSL-сертификатов. По утверждениям специалистов, подобное положение весьма понятное, учитывая тот факт, что с целью перехвата информации

правительство страны осуществляет атаку человек посередине, направленную на Google.

В GreatFire уверены, что власти Поднебесной использовали этот подход во избежание блокировки американского поисковика, способной вызвать волну недовольства со стороны студентов, исследователей и пр. Кроме того, MITM-атака позволит предоставлять доступ к ресурсам Google, контролируя при этом (и блокируя в случае необходимости) результаты поисковой выдачи.

Эксперты Netresec согласны с вышеупомянутым утверждением, основываясь на анализе двух пакетов, задействованных во время атаки. По их данным, именно правительство Китая несет ответственность за MITM-атаку на www.google.com и отслеживание зашифрованного при помощи SSL-сертификата трафика, передаваемого между CERNET и Google ***(Власти Китая осуществляют MITM-атаку на сайт Google // InternetUA (http://internetua.com/vlasti-kitaya-osusxestvlyauat-MITM-ataku-na-sait-Google). – 2014. – 8.09).***

***

Уже другу добу поспіль сайт організації «Мама Солдата» зазнає надзвичайно потужної DDoS-атаки, – про це йдеться в повідомленнях організації в соціальних мережах. В організації зазначили, що сайт атакують не якісь «вороги чи шпигуни» з-за кордону, а з Росії.

«Друзі, це страшно – нашу роботу хочуть заблокувати наші ж співвітчизники. Наша мета – щоб не помирали наші діти, наші чоловіки та брати на незрозумілій, чужій війні. Але, видно, в когось зовсім інші цілі», – ідеться в повідомленні.

Нагадаємо, що сайт MamaSoldata.org запустився минулого тижня. Його мета – допомогти матерям російських солдат не допустити їх потрапляння в Україну, де російські військові беруть участь у війні проти України ***(Антивоєнний сайт російських матерів mamasoldata.org ДДоСять з Росії // UkrainianWatcher (http://watcher.com.ua/2014/09/08/antyvoyennyy-sayt-rosiyskyh-materiv-mamasoldata-org-ddosyat-z-rosiyi/). – 2014. – 8.09).***

***

В ходе саммита НАТО в Уэльсе, Великобритания, лидеры Североатлантического альянса приняли новую доктрину, которая, помимо прочего, будет трактовать крупномасштабную кибератаку на любое из государств-членов Альянса, как акт войны, направленный сразу на весь блок.

Таким образом, НАТО оставляет за собой право нанести военный удар в ответ на полномасштабную атаку одной из стран Альянса.

Для выполнения этой доктрины участники Альянса договорились обмениваться информацией о хакерских атаках и делиться опытом усиления внутригосударственной интернет-безопасности страны.

Впрочем, пока что в новой доктрине отсутствует понимание того, насколько крупной должна быть хакерская атака, чтобы она считалась нападением на весь блок, поскольку дать такое определение довольно сложно.

Аналитики НАТО отмечают, что отсутствие ясности масштабов атаки, необходимой для начала военной операции членами Альянса, будет вызывать у хакеров больший страх, чем чёткие определения.

По предварительным данным, новая доктрина была принята после того, как аналитики установили, что инициатором одной из самых мощных DDoS-атак, которой в 2009 г. подвергли входящую в Альянс Эстонию, была Россия.

Тогда в результате атаки из строя на три недели были выведены серверы, обслуживающие государственные и финансовые организации страны ***(НАТО ответит военными ударами на хакерские атаки стран-участников альянса // Блог Imena.UA (http://www.imena.ua/blog/nato-defense-in-case-of-major-cyberattack/). – 2014. – 9.09).***

***

В первом полугодии 2014 г. специалисты компании F-Secure Labs зафиксировали значительное увеличение количества онлайн-атак с использованием программ-вымогателей. Вредоносные программы блокируют доступ к данным пользователя и вымогают выкуп за разблокирование информации.

Во II квартале 2014 г. эксперты обнаружили 295 новых угроз для мобильных устройств на базе Android (294) и iOS (1). При этом самыми распространенными угрозами для Android были трояны, которые рассылали SMS-сообщения на премиум-номера абонентов или похищали информацию с устройства пользователя, отправляя полученные данные на удаленный сервер злоумышленников.

Лидером по количеству случаев заражения ПК стал компьютерный червь Downadup/Conficker (32 %). По данным экспертов, вредоносная программа инфицировала миллионы компьютеров в 200 странах мира. Как отмечают специалисты, зараженными оказались, в основном, машины, которые используют устаревшее программное обеспечение.

Кроме того, сотрудники F-Secure Labs обнаружили 25 новых MAC-угроз, некоторые из которых использовались в ходе хакерских атак на различные организации. По словам советника по безопасности F-Secure Ш. Салливана, количество шпионских программ увеличивается с каждым днем, поскольку интерес для злоумышленников представляет практически любая информация, например конфиденциальные корпоративные данные, которые всегда можно выгодно продать ***(В первом полугодии 2014 года увеличилось число атак с использованием программ-вымогателей // InternetUA (http://internetua.com/v-pervom-polugodii-2014-goda-uvelicsilos-csislo-atak-s-ispolzovaniem-programm-vimogatelei). – 2014. – 9.09).***

***

Администрация компании Salesforce опубликовала уведомление, в котором предупреждает своих клиентов об опасности компрометации их систем. Так, по данным поставщика облачных CRM-систем, в начале текущего месяца стало известно, что неизвестные злоумышленники предпринимают активные попытки хищения учетных данных пользователей сервиса.

«3 сентября один из наших партнеров по информационной безопасности выяснил, что троян Dyre (также известный, как Dyreza), который изначально использовался для проведения атак на клиентов крупных финансовых организаций, в настоящий момент применяется против некоторых пользователей Salesforce», – следует из сообщения администрации.

В компании также подчеркивают, что в настоящее время у них отсутствуют доказательства того, что кто-либо из клиентов уже стал жертвой злоумышленников. «Если мы установим, что действие вируса затронуло наших пользователей, мы свяжемся с этими людьми, чтобы проинструктировать и дать им необходимые рекомендации», – заботливо заключили в Salesforce ***(Злоумышленники используют банковский троян для хищения учетных данных пользователей Salesforce // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-bankovskii-troyan-dlya-hisxeniya-ucsetnih-dannih-polzovatelei-Salesforce). – 2014. – 9.09).***

***

40 % используемых государством IP-адресов уязвимы к несанкционированному вторжению

«На сегодня уровень защиты государственных интересов в сфере информационных технологий (ИТ) мы оцениваем как низкий. Согласно статистике команды реагирования на компьютерные инциденты CERT-UA в государственном секторе скомпрометировано 40 % IP-адресов. Под компрометацией мы подразумеваем или факты несанкционированного доступа, или вирусную активность», – сообщил редакции «proIT» председатель Государственной службы специальной связи и защиты информации, В. Зверев.

Первая и основная причина – систематическое невыполнение большинством владельцев государственных информационно-телекоммуникационных систем требований информационной безопасности. Сейчас эти требования регламентируются почти 150 нормативными документами Госспецсвязи, каждый из которых призван повысить уровень защиты этих систем. Однако все требования могут привести к созданию дополнительных неудобств в работе администраторов и пользователей ИТС.

В условиях отсутствия контроля они стараются избегать выполнения этих требований.

Вторая причина – Госспецсвязи уполномочена проверять исполнение требований вышеупомянутых документов, но ни служба, ни учреждение, которое проверяется, обычно не имеют ресурсов для проверки фактического состояния дел – аудита информационной безопасности. За прошлый год было проведено лишь 11 таких аудитов, за текущий – 4. Это капля в море. Без выделения средств на аудиты может быть проверено только формальное выполнение требований по документам. Госспецсвязи неоднократно требовала обязательного аудита безопасности ИТС хотя бы центральных органов власти и объектов критической инфраструктуры, но в текущей экономической ситуации у государства и ее учреждений другие бюджетные приоритеты.

Третья причина – фактическое отсутствие ответственности за нарушение требований информационной безопасности. Если при проверке выявлены нарушения, Госспецсвязи имеет право потребовать их устранения и проверить этот факт по документам. Но если ИТС государственного органа была взломана или атакована, согласно действующему законодательству ответственного за это лицо найти трудно. Технические специалисты государственного органа, в котором произошел инцидент, в своих докладных записках фиксируют форс-мажорную ситуацию и отмечают, что их предыдущие докладные записки о необходимости модернизации ИТС не были удовлетворены по причине отсутствия бюджетных средств. Максимальная ответственность – выговор. Уголовную ответственность за несанкционированный доступ или препятствования деятельности ИТС должны нести хакеры. Однако, если их деятельность не привела к существенному материального ущербу, уголовные дела по таким статьям, как правило, не доходят до суда из-за недостатка доказательств.

«Отсутствие ответственности, возможность формального выполнения требований ИБ и отсутствие бюджетных средств приводят к систематическому повторению киберинцидентов в государственных органах. Мы надеемся, что принятие Верховной Радой закона “Об основных принципах обеспечения кибернетической безопасности Украины”, проект которого подготовлен при участии Госспецсвязи, сдвинет ситуацию для усиления ответственности за безопасность информационно-телекоммуникационных систем государственных органов», – говорит В. Зверев ***(40 % используемых государством IP-адресов уязвимы к несанкционированному вторжению // proIT (http://proit.com.ua/news/technology/2014/09/09/171331.html). – 2014. – 9.09).***

***

Эксперты Cisco обнаружили на сайтах YouTube, Amazon и Yahoo всплывающую вредоносную рекламу. Об этом в понедельник, 8 сентября,

сообщил журналист Д. Кирк из IDG News Service со ссылкой на исследователя Cisco А. Пелкманна.

По словам эксперта, вредоносная реклама перенаправляет пользователей Windows и Mac OS X на сторонние ресурсы, с которых в зависимости от операционной системы жертвы загружается контент, содержащий вредоносное ПО. Уникальное контрольное число вредоносного кода намного усложняет его обнаружение для антивирусных решений. Примечательно, что загружаемый контент может быть вполне легитимным, например, медиаплеером. Для того чтобы вредонос инфицировал систему, пользователь должен открыть файл.

Рекламная сеть получила название Kyle and Stan, поскольку именно эти имена часто встречаются в поддоменах более 700 сайтов, используемых злоумышленниками для распространения вредоноса.

А. Пелкманн пояснил, что большое количество доменов позволяет преступникам использовать один из них в течение короткого промежутка времени, а затем переходить на другой для осуществления следующей атаки. Благодаря этому им удается обходить решения безопасности и не попадать в «черные списки».

По словам эксперта, вредоносная реклама присутствует в 74 доменах, в том числе на сайтах youtube.com, amazon.com и ads.yahoo.com. Для заражения компьютеров злоумышленники используют исключительно методы социальной инженерии без применения каких-либо эксплоитов ***(На YouTube, Amazon и Yahoo обнаружена вредоносная реклама // InternetUA (http://internetua.com/na-YouTube--Amazon-i-Yahoo-obnarujena-vredonosnaya-reklama). – 2014. – 10.09).***

***

Бывший руководитель Агентства национальной безопасности США К. Александер основал компанию IronNet Cybersecurity. Она разработала технологию для пресечения кибератак, но репутация основателя не даёт продвигать продукт.

Разработанная специалистами компании технология отличается тем, что может пресечь атаку до её идентификации. Отметим, что современные подобные технологии пока пресекают только известные виды атак.

В настоящее время IronNet Cybersecurity оформляет патент на свою разработку. Виной бюрократических проволочек является бывшая должность К. Александера.

Его компания столкнулась с критикой, что Александер получает прибыль от разработок, которые изначально создавались в интересах государства. Сам бывший чиновник отмечает, что эта разработка кардинально отличается от тех, которые развивают в АНБ.

Ранее стало известно, что АНБ США разрабатывает интеллектуальную защитную систему нового типа, способную не только предотвратить хакерскую атаку, но и самостоятельно нанести ответный удар.

Программа MonsterMind с помощью специальных алгоритмов может просматривать большие объёмы метаданных и анализировать их, чтобы отличить нормальный сетевой трафик от аномального или вредоносного ***(Стартап бывшего директора АНБ борется с хакерскими атаками и критикой в свой адрес // Блог Imena.UA (http://www.imena.ua/blog/ex-spymaster-seeks-anti-hacker-patent/). – 2014. – 11.09).***

***

В используемый экспертом honeypot попало вредоносное ПО Lightaidra, которое представляет собой сканер/эксплуататор, использующий протокол IRC. Это довольно редкое явление, поскольку вредонос распространяется через сетевые устройства пользователей, а не через уязвимые ПК.

Обнаруженный исследователем бот был разработан в 2012 г. и распространяется через пользовательские кабели и DSL-модемы с именами пользователя и паролями, установленными по умолчанию. Жертвами Lightaidra становятся пользователи Linux, а его главным предназначением является осуществление DDoS-атак.

Варианты этого вредоносного ПО были обнаружены в инструментах для осуществления DDoS-атак, которые работают на Linux. К примеру, инструмент ELF DDoS создан на основе Lightaidra и предназначен для рабочих станций, маршрутизаторов и серверов на базе Linux.

Исходный код вредоноса был опубликован в сети в декабре 2012 г. и доступен до сих пор ***(Обнаружен бот для маршрутизаторов, меняющий конфигурацию межсетевых экранов // InternetUA (http://internetua.com/obnarujen-bot-dlya-marshrutizatorov--menyauasxii-konfiguraciua-mejsetevih-ekranov). – 2014. – 11.09).***

***

Согласно данным исследования, проведенного специалистами нескольких университетов США, по всей вероятности, об одной из самых серьезных уязвимостей, получившей название Heartbleed, стало известно только после ее обнаружения. Эксперты отметили, что масштабные атаки, использующие брешь Heartbleed, начались через сутки после того, как об этой уязвимости стало известно в сети.

Уязвимость Heartbleed была обнаружена в старых версиях криптографического пакета OpenSSL, используемого для шифрования трафика данных между сервером и клиентом. Брешь позволяла несанкционированно читать память на сервере или на клиенте, в том числе для извлечения закрытого ключа сервера.

Для того чтобы определить вероятность совершения атак с использованием уязвимости Heartbleed до того, как о ней стало известно, специалисты проанализировали данные сетевого трафика Национальной лаборатории им. Лоуренса в Беркли, центра NERSC (National Energy Research

Scientific Computing) и облачного веб-сервиса Amazon EC2. Анализ показал, что в период с ноября 2013 г. по апрель 2014 г, хакерских атак с использованием уязвимости Heartbleed зафиксировано не было.

Также специалисты выяснили, что первые хакерские атаки с использованием бреши Heartbleed начались через 21 час 29 мин после обнаружения уязвимости. Атаки производились с сервера, расположенного в сети Латвийского университета ***(Исследование: Об уязвимости Heartbleed стало известно только после ее обнаружения // InternetUA (http://internetua.com/issledovanie--ob-uyazvimosti-Heartbleed-stalo-izvestno-tolko-posle-ee-obnarujeniya). – 2014. – 11.09).***

***

Специалисты обнаружили первый случай внедрения алгоритма шифрования AES-256 на мошенническом веб-сайте, специально созданном для выманивания персональных данных пользователей.

Специалисты Symantec обнаружили мошеннический веб-сайт, использующий алгоритм шифрования AES-256 для маскировки контента поддельной страницы. По словам аналитика компании П. Вуда, такая тактика затрудняет проведение анализа веб-сайта для специалистов по безопасности.

Как пояснил П. Вуд, на поддельной странице злоумышленники реализовали алгоритм AES на JavaScript, который активизируется посредством внедренного пароля (используемого для генерации ключа) и зашифрованного текста. Далее незашифрованный фишинговый контент динамично вписывается в веб-страницу. Происходит этот процесс мгновенно и незаметно для пользователей.

Как только расшифровка данных закончена, мошеннический сайт становится неотличим от настоящего. Более того, определить наличие подозрительного контента с помощью обычного анализа страницы практически невозможно, поскольку он содержится в нечитабельном зашифрованном тексте.

Специалист по безопасности Symantec Н. Джонсон отметил, что киберпреступники изобретают новые тактики, призванные продлить дееспособность мошеннических веб-сайтов. Несмотря на то что на сегодняшний день подобные попытки далеки от совершенства, со временем фишинговые атаки могут стать более эффективными и изощренными ***(Злоумышленники используют алгоритм AES-256 для маскировки контента мошеннических сайтов // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-algoritm-AES-256-dlya-maskirovki-kontenta-moshennicseskih-saitov). – 2014. – 11.09).***

***

Террористы из группировок «Аль-Каида» и «Исламское государство Ирака и Леванта» объявили кибервойну Соединённым Штатам Америки.

На сегодняшний день лидеры организаций вербуют хакеров в социальных сетях. Кибервойна подразумевает создание структуры под названием «Киберхалифат», которая будет взламывать различные государственные и частные структуры США.

Согласно разведданным, экстремисты уже вложили огромные деньги в технологии шифрования и разработали собственное программное обеспечение для защиты коммуникаций.

Предполагается, что «онлайн-джихад» против США начнётся в самое ближайшее время. Главной целью террористов станут правительственные агентства, банки, энергетические и транспортные компании Северной Америки ***(Арабские экстремисты объявили кибервойну США // Блог Imena.UA (http://www.imena.ua/blog/islamic-state-attacks-west/). – 2014. – 12.09).***

***

Компания «Доктор Веб» обнаружила очередной троян-вымогатель, обладающий, по сравнению с другими вредоносными программами данного класса, более широким функционалом. Так, помимо блокировки зараженного устройства с типичным требованием выкупа, он также может самостоятельно установить пароль на разблокировку экрана, задействовав для этого стандартную системную функцию, сообщили CNews в «Доктор Веб».

Новый троян, добавленный в вирусную базу Dr.Web под именем Android.Locker.38.origin, является представителем растущего семейства вредоносных программ, блокирующих мобильные устройства пользователей и требующих выкуп за их разблокировку. Данный Android-вымогатель распространяется киберпреступниками под видом системного обновления и после своего запуска запрашивает доступ к функциям администратора устройства. Далее троян имитирует процесс установки обновления, удаляет свой значок с главного экрана, после чего передает на удаленный сервер информацию об успешном заражении и ждет дальнейших указаний.

Команда на блокировку целевого устройства может быть отдана злоумышленниками как при помощи JSON-запроса с веб-сервера, так и в виде SMS-сообщения, содержащего директиву set_lock. Как и многие трояны семейства Android.Locker, Android.Locker.38.origin блокирует устройство, демонстрируя сообщение с требованием выкупа, которое практически невозможно закрыть.

Однако если пострадавший пользователь все же попытается удалить вымогателя, отозвав у вредоносной программы права администратора, Android.Locker.38.origin задействует дополнительный уровень блокировки, отличающий его от прочих подобных Android-угроз, указали в «Доктор Веб». Вначале троян переводит зараженное устройство в ждущий режим, блокируя экран стандартной системной функцией. После его разблокировки он демонстрирует ложное предупреждение об удалении всей хранящейся в памяти устройства информации.

После подтверждения выбранного действия экран устройства снова блокируется, и троян активирует встроенную в операционную систему функцию защиты паролем при выходе из ждущего режима. Вне зависимости от того, была задействована эта функция ранее или нет, вредоносная программа устанавливает на разблокировку мобильного устройства собственный пароль, состоящий из числовой комбинации «12345». Таким образом, зараженный Android-смартфон или планшет окончательно блокируется до получения злоумышленниками оплаты (блокировка может быть снята ими при помощи управляющей команды set_unlock) или выполнения пользователем полного сброса параметров устройства.

Помимо блокировки мобильных устройств, Android.Locker.38.origin также может выступать и в роли SMS-бота, выполняя по команде киберпреступников отправку различных SMS-сообщений, что может привести к дополнительным финансовым потерям ***(Новый троян-вымогатель устанавливает пароль на Android-устройства // InternetUA (http://internetua.com/novii-troyan-vimogatel-ustanavlivaet-parol-na-Android-ustroistva). – 2014. – 13.09).***

***

Совершенные недавно кибератаки на четыре крупных американских банка, а также фондовые и деривативные биржи доказали: кибертерроризм может быть разрушительным, но на сей раз он решил пощадить экономику США.

В действительности новый уровень кибервойны угрожает экономической системе, побуждая правительство США дискретно предоставлять крупнейшим банкам гарантии за счет налогоплательщиков, сообщает информационное агентство Bloomberg.

М. Галлиган, участвовавшая в инициированном правительством расследовании хакерских атак на NASDAQ, утверждает: киберпреступники продемонстрировали, что они могут проникнуть в экономические институты, но атаки были не столь разрушительным, какими они могли бы быть. Это заставило М. Галлиган предположить, что хакеры всего лишь хотели отправить «послание», угрозу.

Реальная опасность в настоящее время исходит не от таких крупных государств, как Россия или Китай, но от «изгоев-кибертеррористов, которые приобретают инструменты и разрабатывают методы нападения на экономическую инфраструктуру США», – сказала М. Галлиган.

«Спонсируемый государством кибертерроризм – это кошмар для ФБР и разведывательного сообщества, – сказала она. – Но еще худшим кошмаром может стать кибер-атака, совершенная террористом-одиночкой».

Террористы, в частности религиозные фанатики, добиваются установления нового мирового порядка. Их главный мотив – разрушение существующего экономического порядка и культуры западного общества, подчеркнула М. Галлиган ***(Специалист по кибер-атакам: что станет***

кошмаром для ФБР // InternetUA (http://internetua.com/specialist-po-kiber-atakam--csto-stanet-koshmarom-dlya-fbr). – 2014. – 14.09).

***

Эксперты компании Akamai-Prolexic обнаружили ботнет, известный под названиями IptabLes и IptabLex. Он использовался для осуществления DDoS-атак на DNS-серверы и прочие объекты сетевой инфраструктуры. Жертвами ботнета становились неверно настроенные Linux-серверы.

По словам специалистов, во II квартале 2014 г. команда Prolexic обнаружила ботнет, проводящий DDoS-атаки с помощью DNS- и SYN-флуда. Атаки выполнялись через скомпрометированные серверы, использующие уязвимые версии Apache Struts, Apache Tomcat и Elasticsearch.

После заражения сервера ботнет получает корневые права и ожидает получения команд от C&C-сервера. Эксперты обнаружили, что вредоносное ПО использовало два неизменяемых IP-адреса.

Специалисты Akamai советуют администраторам Linux-серверов установить последние обновления и изменить настройки безопасности. Они отмечают, что ранее такие серверы не использовались в проведении DDoS-атак.

Антивирусы неспособны справиться с новой угрозой. В настоящее время ботнет детектируется лишь 23 из 52 антивирусов.

Для того чтобы очистить зараженную систему от вируса, администраторам требуется выполнить несколько bash-команд:

sudo find / -type f –name ‘.*ptabLe*’ – exec rm –f {} ‘;’

ps –axu | awk ‘/\.IptabLe/ {print $2}’ | sudo xargs kill -9

Затем необходимо перезагрузить систему и выполнить детальную проверку ***(Обнаружен Linux-ботнет, использующийся для совершения широкомасштабных DDoS-атак // InternetUA (http://internetua.com/obnarujen-Linux-botnet--ispolzuuasxiisya-dlya-soversheniya-shirokomasshtabnih-DDoS-atak). – 2014. – 14.09).***

***

9 сентября Apple представила свои новые продукты – смартфоны iPhone 6, iPhone 6+ и «умные» часы Apple Watch. Примечательно, что в ходе презентации ни разу не было упомянуто о безопасности iOS 8 и сервиса iCloud, а все внимание было сосредоточено на новых функциях мобильной платформы. Тем не менее, именно безопасность операционной системы и сервисов Apple более всего волнует пользователей, учитывая недавнюю утечку откровенных фотографий звезд шоу-бизнеса.

Эксперты новостного портала Ars Technica решили проверить, действительно ли так сложно скомпрометировать данные пользователей iCloud и других сервисов компании. С помощью инструментов от Elcomsoft, используемого правоохранительными органами для сбора информации, и

ряда хакерских приемов, они обнаружили несколько способов похищения хранящихся на iPhone данных.

Для того чтобы осуществить атаку, злоумышленнику необходимо получить физический доступ к устройству, однако эксперты нашли способ сделать это незаметно для жертвы. По их мнению, хакерам удалось похитить фотографии знаменитостей iCloud из-за слабой аутентификации сервиса для функции Find My iPhone. Возможно также, что злоумышленники подобрали пароли на основании контрольных вопросов, ответы на которые известны только жертве. Тем не менее, хакеры могли узнать нужную информацию о знаменитостях для ответов из общедоступных источников.

Теперь для того, чтобы пользователь знал о возможных попытках злоумышленников сменить его пароль или войти в учетную запись в iCloud, Apple отсылает по электронной почте соответствующие уведомления. Эта мера не предотвращает взлома как такового, однако позволяет жертве как можно скорее принять меры безопасности.

Что касается Elcomsoft, то инструменты компании разработаны без какого-либо участия Apple. То есть, разработчики создали их на основании реверс-инжиниринга протоколов компании ***(Эксперты обнаружили несколько способов похищения хранящихся на iPhone данных // InternetUA (http://internetua.com/eksperti-obnarujili-neskolko-sposobov-pohisxeniya-hranyasxihsya-na-iPhone-dannih). – 2014. – 13.09).***

***

Домашние роутеры читателей популярной бразильской газеты подверглись хакерским атакам, информирует компания Sucuri, специализирующая на защите информационных сетей. Злоумышленники внедрили «плавающие фреймы» в веб-сайт газеты Politica Estadao, осуществлявшие брут-форс атаки на компьютеры, с которых выполнялся вход на этот веб-сайт.

Злоумышленники пытались изменить настройки DNS атакованных роутеров: полезная нагрузка подбирала имена пользователей admin, root, gvt и другие, которые обычно используются с паролями по умолчанию. Скрипт задействуется для определения локального IP-адреса компьютера, а затем пытается установить IP-адрес маршутизатора.

В ходе атаки применялся код, направленный на пользователей Internet Explorer с рядом IP-адресов, в том числе 192.168.0.1 и 192.167.1.1. Загрузка контента происходила с потенциально опасного сайта laspeores.com.ar и двух других сайтов, задействовавших «плавающие фреймы» с вредоносным JavaScript кодом.

По словам Ф.Соуза, ИБ-эксперта фирмы, это один из нескольких векторов компьютерных атак. Несмотря на то, что веб-сайты долгое время являлись основным механизмом распространения вредоносного ПО, теперь тенденция несколько иная. Наиболее простой способ уберечься от атаки – задавать разные имена пользователей и пароли. Кроме того, следует

отключить JavaScript и игровые опции для объектов браузера, а также использовать блокировщики скриптов NoScript или Not Script, советуют в Sucuri ***(Хакеры взломали сайт популярной бразильской газеты, чтобы получить доступ к роутерам ее читателей // InternetUA (http://internetua.com/hakeri-vzlomali-sait-populyarnoi-brazilskoi-gazeti--cstobi-polucsit-dostup-k-routeram-ee-csitatelei). – 2014. – 15.09).***

***

Редко какому вирусу удаётся беспроблемно проработать несколько лет, однако вредоносный код под названием Harkonnen Operation «успешно» работал целых 12 лет и всё это время не был никому известен (кроме своих создателей), пока его наконец не обнаружила израильская компания CyberTinel.

Harkonnen Operation был не просто программой, а целой сетью киберпреступной деятельности, которая включала в себя 800 подставных компаний в Великобритании. Злоумышленники устанавливали вредоносный код на серверах и сетевом оборудовании различных организаций, в основном банков, крупных корпораций и госучреждений в Германии, Швейцарии и Австрии. Управляющий центр находился в Германии, жертвами стали около 300 разных организаций.

Harkonnen Operation не был самым технически совершенным вредоносным ПО, однако злоумышленникам удавалось получать подлинные сертификаты DNS, что усложняло его обнаружение. Кроме того, они каждый раз использовали другую программную оболочку. В CyberTinel о нём узнали почти случайно, после того как одна из немецких фирм обнаружила странное поведение трафика на своих серверах. В компании не раскрывают название фирмы, но говорят, что это «крупная фирма, о которой вы наверняка слышали».

«Они искали очень конкретные вещи, их метод был: зайти и выйти очень быстро, надеясь, что никто не заметит», – объясняет гендиректор компании К. Бен-Наим. Этот подход позволял им работать больше десяти лет, пока они не совершили роковую ошибку, по словам К. Бен-Наима: «[они] просидели на сервере нашего клиента немного дольше – ровно столько, сколько нужно было, чтобы обнаружить их активность».

В CyberTinel точно не знают личности киберпреступников, но говорят, что это «больше похоже на организованную преступную группу, чем на деятельность государства». Известно, что эта группа за всё время инвестировала в свою сеть больше 150 тыс. дол. «Сеть эксплуатировала относительно терпимые британские требования при покупке сертификатов безопасности SSL и создавала поддельные британские компании, которые имитировали законные веб-сервисы. Немецкие хакеры получали полный контроль над компьютерами жертв и могли много лет осуществлять шпионаж, оставаясь незамеченными».

«Было много сигналов о подозрительной активности, которые должны были заметить регуляторы. Думаю, имеет смысл задать ряд вопросов о произошедшем», – подытоживает К. Бен-Наим ***(Немецкий вирус Harkonnen Operation проработал необнаруженным 12 лет – новый рекорд? // InternetUA (http://internetua.com/nemeckii-virus-Harkonnen-Operation-prorabotal-neobnarujennim-12-let---novii-rekord). – 2014. – 16.09).***

***

Электронные книги, которые загружаются на «читалку» Kindle из сомнительных источников, могут стать причиной похищения пользовательской учётной записи на Amazon.

Специалисты отмечают, что уязвимость, при помощи которой можно «увести» учётную запись, содержится на странице Manage Your Kindle.

Через неё злоумышленники могут спрятать в метаданные книги вредоносный код, который будет выполнен автоматически при открытии библиотеки Kindle. Так хакеры получают доступ к cookie-файлам и, следовательно, к учётным данным жертвы.

«Дыра» в программе была обнаружена ещё в октябре 2013 г. Тогда Kindle исправила ошибку, но, по-видимому, она была допущена повторно, с выходном очередного обновления.

Из-за недавно обнаруженной уязвимости любое устройство, оснащённое портом USB и подключённое к компьютеру, может быть использовано хакерами для несанкционированного получения доступа к данным пользователей ***(Пиратские книги воруют учётные записи на Amazon // Блог Imena.UA (http://www.imena.ua/blog/amazon-stored-xss-book-metadata/). – 2014. – 17.09).***

***

Согласно данным компании Avast, банковский троян Tiny Banker, также известный как Tinba, атакует финансовые организации США.

Tinba является самым маленьким из известных на сегодняшний день банковских троянов (порядка 20 КБ). По словам аналитика Avast Я. Хорейси, вредоносная программа внедряла поля HTML в банковские веб-сайты, которые посещал пользователь и запрашивала разнообразную конфиденциальную информацию под видом системного апдейта. Запрашиваемая информация включала в себя номер кредитной карты, адрес, номер социального страхования, номер водительской лицензии и даже девичья фамилия матери.

Версия трояна, которую проанализировали специалисты Avast, была специально разработана для атак, нацеленных на целый ряд финансовых организации США, в том числе Wells Fargo, Bank of America и Chase ***(Троян Tiny Banker атакует финансовые организации США // InternetUA (http://internetua.com/troyan-Tiny-Banker-atakuet-finansovie-organizacii-ssha). – 2014. – 16.09).***

***

Исследовательская компания Palo Alto Networks обнаружила вредоносное приложение AppBuyer, нацеленное на пользователей iPhone и iPad. Троян крадет учетные записи Apple ID и пароли с мобильных устройств, подвергнутых процедуре джейлбрейка.

Имя разработчика AppBuyer, как и количество зараженных гаджетов, не называется. Как сообщили исследователи, вирус распространяется с расширением Cydia Substrate, после чего инициирует загрузку EXE-файла, генерирующего уникальный идентификатор UUID, скачивает специальный твик для кражи Apple ID и пароля, а также утилиту для входа в App Store и покупки приложений.

Изучив код и информацию отладки, которую оставляет вредоносное ПО, эксперты выяснили, что программа работает в фоновом режиме и обнаружить ее присутствие достаточно сложно. AppBuyer оставляет файлы в пяти местах:

-/System/Library/LaunchDaemons/com.archive.plist
-/bin/updatesrv
-/tmp/updatesrv.log
-/etc/uuid
-/Library/MobileSubstrate/DynamicLibraries/aid.dylib
-/usr/bin/gzip

Каким образом троян попадает на мобильные устройства пользователей в Palo Alto Networks пока не выяснили. Удаление файлов программы приводит к прекращению работы AppBuyer.

Всем пользователям джейлбрейкнутых iPhone и iPad эксперты безопасности рекомендуют пользоваться только проверенными источниками, так как велика вероятность, что заражение происходит при подключении в Cydia пиратских репозиториев.

AppBuyer – не первый вирус для iPhone и iPad, о котором стало известно в последнее время. Троян AdThief, обнаруженный в августе, заразил свыше 75 тыс. iOS-устройств с джейлбрейком. Этот вредонос распространяется с расширением Cydia Substrate, после чего изменяет рекламные объявления, появляющиеся в бесплатных приложениях. Деньги за показ объявлений, уплаченные разработчикам приложений, перенаправляются на счет хакеров ***(Троян для iPhone и iPad с джейлбрейком крадет Apple ID и пароли // InternetUA (http://internetua.com/troyan-dlya-iPhone-i-iPad-s-djeilbreikom-kradet-Apple-ID-i-paroli). – 2014. – 17.09).***

***

Лишь одно из каждых четырех мобильных приложений удовлетворяет требованиям корпоративной безопасности, указывают эксперты. По их словам, с учетом темпов распространения мобильных технологий

предприятиям следует в обязательном порядке внедрять механизмы тестирования приложений и страхования от рисков.

Более 75 % мобильных приложений не удовлетворяют базовым требованиям корпоративной безопасности, сообщила исследовательская компания Gartner. Аналитики предупредили, что такая ситуация сохранится как минимум до конца 2015 г.

В компании прогнозируют, что в 2014 г. пользователями во всем мире будет загружено на мобильные устройства почти 139 млрд приложений. К 2017 г. это значение возрастет почти до 269 млрд.

«Предприятия, пользующиеся мобильными устройствами или внедряющие стратегию “принеси свое собственное устройство” (Bring Your Own Device – BYOD), остаются уязвимы к нарушениям защиты, пока они не внедрят методы и технологии тестирования мобильных приложений на безопасность и не воспользуются страхованием от рисков», – заявил старший аналитик Gartner Д. Зумерли.

Сегодня свыше 90 % предприятий, внедряющих стратегию BYOD, пользуются сторонними мобильными приложениями. Поэтому так важно использовать механизмы проверки этих приложений, подчеркнул эксперт.

Аналитики поясняют, что сегодня разработчики в основном посвящают свое время функциональности мобильных приложений и не уделяют внимания их безопасности. Поэтому риски, связанные с использованием таких программ, обусловлены по большей части не действиями злоумышленников, а отсутствием в этих приложениях какого бы то ни было бережного отношения к данным.

Согласно Gartner, в период до 2017 г. включительно 75 % нарушений защиты мобильных приложений будут связаны с неправильной работой этих приложений, а не с атаками на мобильные устройства. В качестве примера аналитики приводят приложение для доступа к какому-либо бесплатному облачному сервису, в которое случайно могут попадать корпоративные данные, хранящиеся на смартфоне. Такая ситуация может привести к утечке коммерческих секретов.

Однако и хакерские атаки приобретут большее значение. Аналитики прогнозируют, что в ближайшие годы количество атак на мобильные устройства продолжит возрастать. Уже сегодня оно втрое превышает количество атак на рабочие станции.

Данные Gartner подтверждаются и другими исследованиями. В конце 2013 г. похожий отчет был выпущен исследовательским подразделением крупнейшего в мире производителя серверов и второго по величине поставщика персональных компьютеров Hewlett-Packard. Согласно HP Security Research, 86 % мобильных приложений не содержат адекватных механизмов защиты от атак и утечек информации ***(75 % приложений на гаджетах сотрудников опасны для работодателей // InternetUA (http://internetua.com/75--prilojenii-na-gadjetah-sotrudnikov-opasni-dlya-rabotodatelei). – 2014. – 18.09).***

***

По мнению экспертов, «Интернет вещей» может стать причиной неприятностей для владельцев компаний и конечных пользователей.

По словам технического директора компании-разработчика McAfee Р. Самани, в то время как «Интернет вещей» обладает огромным потенциалом и способна перевернуть образ жизни человечества, она может стать причиной увеличения активности киберпреступников. Самани подчеркнул, что из-за огромного объема данных такие системы становятся мишенью для злоумышленников, поэтому обеспечение безопасности должно являться наиважнейшей задачей для разработчиков подобных технологий.

Главный аналитик компании «Лаборатория Касперского» Д. Эмм согласен с мнением коллеги. По его словам, наибольшему риску в данной ситуации подвергаются промышленная и энергетическая сферы, поскольку злоумышленники могут похищать данные, манипулировать ими и отсылать неверную информацию. Например, существует возможность подделки данных электрических счетчиков или измены радиочастотной идентификации (RFID) потребительских товаров, что может доставить массу неприятностей производителям одежды.

Д. Эмм уверен, что «Интернет вещей» создаст больше возможностей не только для нелегального заработка, но и для кибершпионажа, кибер-саботажа, а также политических и социальных протестов ***(«Интернет вещей» подвергает риску промышленные предприятия и электросети // InternetUA (http://internetua.com/internet-vesxei--podvergaet-risku-promishlennie-predpriyatiya-i-elektroseti). – 2014. – 18.09).***

***

Хакеры, совершающие целенаправленные атаки, стали использовать усовершенствованную версию вредоноса Citadel для проведения кибератак на несколько ближневосточных нефтехимических компаний. Об этом сообщают исследователи компании Trusteer.

По словам руководителя отдела корпоративной безопасности Trusteer Д. Тамир, пострадавшие компании получили уведомления о том, что на них ведется направленная кибератака. Среди жертв числятся поставщик нефтехимических элементов и один из наибольших продавцов нефтехимической продукции в регионе. Личности киберпреступников остались неизвестными, пишет Д. Тамир в своем блоге.

Д. Тамир заявила, что модификация банковских троянов под инструменты для совершения целенаправленных атак не является чем-то новым. Тем не менее, это первая атака, в которой Citadel использовали для получения доступа к внутренним сетям компаний, хищения интеллектуальной собственности или перехвата внутренней почты.

Ранние версии Citadel использовались для совершения атак «человек посередине» и похищения финансовых данных, но модифицированная версия вредоноса способна нанести гораздо больше вреда. Новый вариант

Citadel способен перехватывать логины и пароли при входе на корпоративную почту, записывать нажатия клавиш, делать скриншоты, встраивать вредоносный код в веб-страницы и предоставлять хакерам полный контроль над ПК жертвы. Более того, вирус использует продвинутые технологии антидетекции и обфускации кода. Из-за этого его гораздо сложнее обнаружить и исследовать.

Д. Тамир сообщила, что благодаря массовому распространению вредоносного ПО киберпреступникам больше не требуется совершать целенаправленные фишинг-атаки. Вместо этого хакеры пытаются заразить как можно большее количество ПК ***(Вирус Citadel превратился в инструмент для совершения целенаправленных атак // InternetUA (http://internetua.com/virus-Citadel-prevratilsya-v-instrument-dlya-soversheniya-celenapravlennih-atak). – 2014. – 18.09).***

***

Редакция телеканала Russia Today сообщила о мощнейшей DDoS-атаке на свой сайт. Соответствующая информация опубликована на ресурсе, пишет «Лента.ру».

«Сайт RT.com сегодня подвергся самой мощной DDoS-атаке за все время существования телеканала. Мощность DDoS-атаки типа UDP-flood на сайт RT достигала 10 Гбит/сек. Благодаря надежной технической защите сайта, RT.com был недоступен лишь несколько минут, однако при этом DDoS-атака продолжалась», – говорится в сообщении.

Ответственности за хакерскую атаку пока никто не заявлял.

Сайт RT.com подвергался DDoS-атакам неоднократно. Одна из самых мощных хакерских атак произошла 18 февраля 2013 г. Работу сайта RT на английском языке удалось восстановить лишь спустя шесть часов после начала атаки. В августе 2012 г. сайты телеканалов RT на английском и на испанском также подверглись хакерской атаке. Тогда ответственность за нее взяла на себя хакерская группа AntiLeaks, выступающая против проекта WikiLeaks Д. Ассанжа ***(Russia Today заявил о мощнейшей DDoS-атаке на свой сайт // Media бізнес (http://www.mediabusiness.com.ua/content/view/40695/126/lang,ru/). – 2014. – 18.09).***

***

Специалисты «Лаборатории Касперского» проанализировали фишинговые письма, подделывающиеся под корреспонденцию компаний, занимающихся международными доставками. Как оказалось, чаще всего спамеры используют бренды DHL, FedEx, United Parcel Service и TNT. У всех этих компаний существуют миллионы клиентов по всеми миру, в связи с чем они стали приоритетной целью для злоумышленников.

При совершении фишинг-атаки киберпреступники чаще всего преследуют две цели. Они либо стремятся заполучить финансовые и

персональные данные жертвы с целью дальнейшей перепродажи, либо пытаются установить на их ПК вредоносное ПО. В дальнейшем такие компьютеры становятся невольными участниками ботнет-сетей по распространению спама или организации DDoS-атак.

Для того чтобы распознать фишинговое письмо, пользователю необходимо обратить внимание на ряд важных деталей. В первую очередь стоит проверить адрес отправителя. Если он не совпадает с официальным сайтом компании, письмо является фишинговым. Такую корреспонденцию следует немедленно удалять без открытия.

Злоумышленники порой допускают ошибки при написании фишингового письма. Нескольких грамматических, пунктуационных или орфографических ошибок будет достаточно для того, чтобы распознать, подлинное ли письмо пришло пользователю.

В фишинговых письмах также подделывается графический дизайн компании. Злоумышленники пытаются подобрать цветовую гамму, шрифты и изображения, максимально близкие к оригиналу. Тем не менее, обычно им не удается этого сделать, и обычное фишинговое письмо выглядит неаккуратно, а ряд его элементов выбивается из общего дизайна.

Стоит также прочитать содержимое письма. Если в нем пользователя просят немедленно предоставить персональные данные (такие, как логин и пароль), загрузить прикрепленный файл или перейти по определенной ссылке, такое письмо может быть фишинговым.

Пользователю также следует проверять адреса, по которым ведут ссылки. Для того чтобы это сделать, следует просто навести курсор мыши на ссылку. Если используется интернет-браузер, адрес ссылки будет отображаться в правом нижнем или левом нижнем углу экрана. При использовании почтового клиента адрес появится во всплывающем сообщении над ссылкой.

Не стоит открывать вложения. Если пользователь не запрашивал получения какого-либо документа через электронную почту, не следует открывать любые документы, которые пришли по электронной почте ***(Спамеры стали подделывать корреспонденцию компаний по доставке // InternetUA (http://internetua.com/spameri-stali-poddelivat-korrespondenciua-kompanii-po-dostavke). – 2014. – 18.09).***

***

Twitter исправила уязвимость, позволявшую неавторизованным пользователям удалять любую кредитную карту со всех аккаунтов, тем самым уменьшая прибыль компании от рекламы.

Атаки осуществлялись путем эксплуатации уязвимости «прямой ссылки на объект» (direct object reference vulnerability) и манипуляций с последовательностями чисел в URL-адресах. Уязвимость оказалась весьма критичной, поскольку для удаления кредитной карты необходим только

идентификатор, состоящий из шести цифр, например, «220152», сказал А. Абул-Эла, специалист по информационной безопасности.

Первая уязвимость касалась карт, хранившихся в «ads.twitter.com/accounts/[account id]/payment_methods». А. Абул-Эла показал, как, изменив всего два параметра в POST-запросе и переслав измененный запрос, можно удалить карту. Вторая уязвимость состояла в генерировании опции dismiss при использовании недействительной карты, что создавало эффект удаления карты. Расширяя идентификаторы, можно удалить огромное количество карт.

В начале сентября Twitter запустил программу выплаты вознаграждений за выявленные уязвимости и теперь платит всем, кто обнаружит уязвимости и сообщит об этом на специально созданный сайт HackerOne . В рамках программы А. Абул-Эла получил от Twitter 2800 дол. – по его словам, самое крупное вознаграждение на сегодняшний день ***(Уязвимость в Twitter позволяла удалить кредитные карты с любого аккаунта // InternetUA (http://internetua.com/uyazvimost-v-Twitter-pozvolyala-udalit-kreditnie-karti-s-luabogo-akkaunta). – 2014. – 18.09).***

***

Как сообщают разработчики SCADA Expert ClearSCADA (линейка популярных SCADA-систем) из Schneider Electric, сторонние исследователи безопасности обнаружили в продуктах компании три опасные бреши. При этом уязвимые программно-аппартаные комплексы используются в таких отраслях как энергетика, водоснабжение, контроль крупных коммерческих объектов и наиболее распространены в США и Европе.

Обнаружить уязвимости удалось специалистам из ICS-CERT, по словам которых эти бреши позволяют потенциальному удаленному злоумышленнику обойти механизм аутентификации и осуществить CSRF-нападение. Третья брешь заключается в наличии слабого алгоритма хеширования.

В сумме эти изъяны в системе безопасности позволяют полностью скомпрометировать атакуемую систему. Тем не менее, для этого атакующим необходимо вынудить пользователя с правами администратора перейти по специально сформированной ссылке.

Представители Schneider Electric заверяют, что соответствующие исправления безопасности будут выпущены в конце текущего месяца. При этом слабый алгоритм можно будет заменить специальной отдельной утилитой ***(В линейке SCADA-систем Schneider Electric обнаружены опасные бреши // InternetUA (http://internetua.com/v-lineike-SCADA-sistem-Schneider-Electric-obnarujeni-opasnie-breshi). – 2014. – 21.09).***

***

Специалисты компании-производителя антивирусных программ ESET обнаружили спам-рассылку, в которой содержался троян

Win32/Injector.BLWX, сообщает портал CNews. Наибольшее количество случаев инфицирования вредоносной программой было зафиксировано в Украине и Великобритании.

Вредоносная программа распространялась в приложениях электронных писем и маскировалась под финансовый документ. Что примечательно, троянец был обнаружен в архиве, упакованном довольно редким архиватором ARJ. Первично эта программа использовалась для операционной системы DOS и ранних модификаций Windows.

Как отмечают в ESET, троянцы семейства Win32/Injector обладают широким набором функций. Различные модификации этих вредоносов могут использоваться для инфицирования ПК, похищения конфиденциальной информации пользователей, а также для формирования сети ботнет, которая рассылает спам или принимает участие в DDoS-атаках.

По словам специалиста по безопасности Г. Клули, до появления широкополостного интернета IT-специалисты старались любыми способами уменьшить размер исходного файла. Примерно в то время появился архиватор ZIP, однако у него были свои конкуренты. Одной из альтернативных (и довольно удачных) программ была ARJ, которая через некоторое время была забыта ***(Новый троян использует раритетный архиватор ARJ // InternetUA (http://internetua.com/novii-troyan-ispolzuet-raritetnii-arhivator-ARJ). – 2014. – 21.09).***

***

Вышедшая недавно финальная версия iOS 8 оказалась традиционно богатой на мелкие баги и недоработки. Всё лето разработчики Apple ловили и убивали мелкие баги в системе, но этого оказалось недостаточно.

Спустя пять дней, в Купертино не рады тому, как пользователи отзываются о прошивке в социальных сетях. Разработчиков iOS 8 загнали в большую комнату, основали там круглосуточный штаб и, грубо говоря, заперли дверь – до тех пор, пока все жалобы в Twitter и Facebook не будут проверены, а корень каждой проблемы – найден и исправлен.

Естественно, напрямую об этом Apple не заявляла. Но пару дней назад с одним из владельцев устройства с iOS 8 случилась неожиданная история, о которой он и поведал в подробностях. Пользователь социалки Reddit под ником Kiggsworthy опубликовал твит, в котором заявил о проблеме с функцей Семейный доступ (Family Sharing). При попытке загрузить что-либо из списка покупок у его жены, устройства демонстрировали специфическую ошибку:

Элемент не может быть загружен.

[Имя песни] не может быть загружена, так как была приобретена с другого Apple ID.

Спустя несколько минут с ним связался сотрудник Apple, немедленно захотевший пообщаться через личные сообщения, прямо в Twitter. Как выяснилось, в Купертино уже знали об этой проблеме, но не могли

идентифицировать её источник. Получив максимально подробную информацию от пользователя, сотрудник обрадовался и заявил: теперь он и его коллеги знают, что случилось. Восемь лет назад какая-то доля контента была загружена в базу iTunes Store с ошибками файловой структуры. Изолировав причину, разрабочтики смогут наконец-то найти решение. В данном случае – переконвертировать все проблемные музыкальные треки на сервере Apple.

В ходе разговора сотрудник проговорился о том, что он и многие другие разработчики iOS 8 в реальном времени ищут твиты, публикации в сети и социальных сетях на предмет ошибок у пользователей, чтобы исправить как можно больше багов к выходу следующей версии прошивки. Специально для этого был создан штаб оперативного реагирования. Сейчас наибольшего внимания удостаиваются проблемы с Семейным доступом ***(Программисты Apple ищут баги iOS 8 по отзывам в соцсетях // InternetUA (http://internetua.com/programmisti-Apple-isxut-bagi-iOS-8-po-otzivam-v-socsetyah). – 2014. – 21.09).***

***

В прошлом году ICANN зарегистрировала новые доменные зоны, в том числе .guru, .fly, .pharmacy, .support, .pizza, .network, .auction и .market. В ICANN надеются добавить поддержку еще порядка 1300 доменных зон в ближайшие несколько лет.

Тем не менее, киберпреступники уже начали использовать новые доменные зоны в своих целях. Исследование, проведенное компанией Malwarebytes, показало, что за последние 60 дней значительно увеличилось количество вредоносных сайтов в доменных зонах .pictures, .consulting, .xyz, .club, .email, .solutions, .company, .domains, .photos, .directory, .enterprises и .guru.

Старший исследователь безопасности Malwarebytes Ж. Сегура сообщает, что специалисты компании обнаружили небольшое количество вредоносных сайтов. Тем не менее, поскольку новые доменные зоны появились в сети относительно недавно, исследователь ожидает значительного всплеска активности киберпреступников уже в ближайшем будущем.

Большинство вредоносных сайтов оказались взломанными либо с помощью брутфорс-атак, либо с помощью эксплуатации различных уязвимостей. Пока неизвестно, были ли атаки целенаправленными либо киберпреступники взламывали случайные веб-страницы.

На взломанные сайты устанавливался набор эксплоитов Angler, внедряющий вредоносное ПО напрямую на ПК посетивших сайт пользователей. Все зараженные веб-страницы использовали порт 37702.

Кроме того, исследователи обнаружили новые фишинговые схемы, в которых были задействованы новые доменные зоны. Исследователи SANS Institute Internet Storm Center успешно идентифицировали фишинг-атаку,

использующую сайт «url-bofa.support/bankofamerica.com». Домен был зарегистрирован киберпреступниками и даже не имел SSL-сертификата ***(Хакеры стали использовать новые доменные зоны для совершения киберпреступлений // InternetUA (http://internetua.com/hakeri-stali-ispolzovat-novie-domennie-zoni-dlya-sovershеniya-kiberprestuplenii). – 2014. – 20.09).***