СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(25.08–7.09)

2014 № 16

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(25.08–7.09)
№ 16

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

Социальные сети на Сумщине – статистические данные

К лету 2014 г. во «ВКонтакте», «Одноклассниках», Facebook и Twitter было зарегистрировано более 40 млн аккаунтов украинцев. Из них около 720 тыс. принадлежат жителям Сум и Сумской области.

Примерно 450 тыс. аккаунтов во «ВКонтакте» принадлежит жителям Сумщины. По этому показателю она занимает 19 место среди регионов страны. Проникновение соцсети «ВКонтакте» (то есть отношение аудитории сервиса к численности населения) составляет в Сумской области почти 40 %. Таким образом, количество аккаунтов во «ВКонтакте» приближается к половине численности населения области по данным Госкомстата Украины.

Больше половины сумчан, зарегистрированных во «ВКонтакте», – это люди до 25 лет.

Среди сумчан, указавших во «ВКонтакте» свой пол, больше мужчин, чем женщин – 54 и 46 % соответственно. Похожее распределение характерно и для Украины в целом. Примерно в седьмой части аккаунтов пол вообще не указан.

В «Одноклассниках» жители Сум и области зарегистрировали 219 тыс. аккаунтов. По этому показателю область занимает 16 место в стране. По проникновению «Одноклассников» она несколько выше, на 13 месте – 19 %.

Больше всего сумских пользователей «Одноклассников» – почти треть – приходится на возрастную группу 26–35 лет. Для сравнения, у «ВКонтакте» самая большая возрастная группа – 16–25 лет. В Сумской области аудитория «Одноклассников» в целом старше, чем аудитория «ВКонтакте». Если в первой соцсети пользователи старше 35 лет составляют 41 %, то во второй – всего 15 %.

В отличие от «ВКонтакте», «Одноклассниками» в Сумской области пользуется больше женщин, чем мужчин – 54 и 46 % соответственно. Зато среди самых юных посетителей «Одноклассников» (до 15 лет включительно) больше мальчиков, чем девочек.

По количеству пользователей Facebook Сумская область 11 в Украине – более 45 тыс. аккаунтов. Проникновение Facebook здесь невелико – 4 %, но это далеко не самый низкий показатель в стране.

Как и в «Одноклассниках», в сумском Facebook больше женщин, чем мужчин. На их долю приходится 51 % аккаунтов, а на долю мужчин – 49 %.

В настоящее время в Twitter насчитывается около 5 тыс. аккаунтов жителей Сум и области. По этому показателю область 15 в стране. В Twitter люди не указывают свой пол. Однако как минимум для 40 % аккаунтов сумчан пол можно с высокой степенью точности определить с помощью лингвистических алгоритмов – по имени и фамилии. Среди этих

пользователей больше мужчин – 57 %. Соответственно, женских аккаунтов – 43 %.

Использование Twitter сильно изменилось во время Евромайдана. Если до ноября 2013 г. каждый месяц в Украине появлялось 6–7 тыс. новых Twitter-аккаунтов, то в декабре 2013 г. было зарегистрировано 16 тыс. аккаунтов, а в январе 2014 г. – почти 55 тыс.

Два года назад украинцы оставляли в среднем около 90 тыс. твитов ежедневно. За период Евромайдана это число возросло до 130 тыс. твитов в день. Рекордным по количеству твитов стало 22 февраля 2014 г. – в ту субботу украинские пользователи оставили почти 240 тыс. твитов ***(Социальные сети на Сумщине – статистические данные // Данкор онлайн (http://dancor.sumy.ua/news/newsline/138500). – 2014. – 26.08).***

***

Сервис микроблоггинга Twitter официально заявил об изменении «Хроники» (Timeline).

Многие пользователи сервиса заметили, что в «Хронику» были добавлены твиты, которые им не принадлежат. И это не случайность. Компания обновила статью о Timeline в Справочном центре.

К изначальному определению «Хроники» «все твиты пользователей, на которых вы подписаны, плюс ретвиты и реклама» теперь добавлена новая секция: «Дополнительно, когда мы определяем твит, аккаунт для подписки или другой популярный или релевантный контент, мы можем добавить его в вашу “Хронику”. Это значит, что иногда вы увидите твиты пользователей, на которых вы не подписаны. Мы отбираем каждый твит, используя разнообразные сигналы, включая его популярность и то, как ваши друзья с ним взаимодействуют. Наша цель – сделать вашу “Хронику” еще более релевантной и интересной».

В большинстве случаев, это «избранные» твиты. Несколько дней назад «Избранное» в Twitter стало общедоступным. Теперь пользователи видят в своей ленте не только твиты и ретвиты друзей, но также и то, что друзья заносят в «Избранное». Нововведение уже обеспокоило некоторых пользователей: будет ли все, что они внесли в «Избранное», даже личные твиты, показано их подписчикам? Кажется, ответ отрицательный. Twitter обещает освещать только популярный или релевантный контент.

Лента новостей Facebook показывает только фрагменты постов друзей и располагает их в порядке релевантности для пользователя. Twitter традиционно показывал все твиты друзей в строгом хронологическом порядке. Новое определение «Хроники» проясняет тот факт, что пока этот порядок не меняется, но сервис добавит твиты, которые могут понравиться пользователю.

Напомним, что интерфейс «Хроника» (Timeline) был запущен Twitter по всему миру в конце 2011 г. Новый формат позволил пользователю выстраивать информацию, публикуемую в профиле, в хронологическом

порядке. Таким образом воссоздавая целостную картину жизни владельца аккаунта. По сути, Timeline – это непрерывный поток информации о пользователе, демонстрирующий друзьям профиля все загруженные фотографии, обновления статуса, загружаемые приложения, отметки на карте, заметки пользователя и т. п. ***(Twitter добавил популярные и релевантные твиты в Timeline // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_dobavil_populyarnye_i_relevantnye_tvity_v_timeline). – 2014. – 27.08).***

***

Представитель Twitter А. Чен в своем Twitter объявил о расширении органической аналитики и доступности ее панели мониторинга для всех пользователей. Инструменты аналитики были запущены еще в июне, но они были доступны только рекламодателям и владельцам подтверждённых (верифицированных) аккаунтов.

Справочный центр Twitter сообщает, что панель мониторинга доступна пользователям, которые размещают твиты на английском, французском, японском и испанском языках, а также зарегистрировали свои аккаунты не менее 14 дней назад. В ближайшее время функция будет расширена для остальных пользователей.

Русскоязычная версия аналитики уже введена в действие.

Панель позволяет увидеть, сколько раз пользователи просматривают твиты и как они действуют в режиме реального времени. Также можно сравнить впечатления, общую вовлеченность и ретвиты месяц за месяцем.

Пользователи также смогут использовать Twitter-карточки, чтобы увидеть, сколько ретвитов, ответов, избранного, подписок, кликов по ссылкам и кликов по встроенным медиа получил каждый твит ***(Twitter расширил Аналитику для всех пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_rasshiril_analitiku_dlya_vseh_polzovateley). – 2014. – 3.09).***

***

Руководство Twitter задумалось о введении в соцсети групповых чатов и существенном усовершенствовании внутреннего поиска по твитам. Об этом, ссылаясь на слова финансового директора сервиса Э. Ното, сообщает The Wall Street Journal, пишет sostav.ua.

О планах Twitter на 2014–2015 гг. Э. Ното рассказал во время своего выступления на конференции Citi Global Technology Conference, проходящей в начале сентября в Нью-Йорке.

По мнению топ-менеджера, в ближайшее время переписка в личных сообщениях между пользователями сервиса микроблогов может стать «более социальной». В частности, это означает появление возможности вести групповые беседы, содержание которых доступно только тем, кто приглашён в конкретный чат.

«Предположим, я твитнул что-то о футбольном матче, и пара моих коллег ответили на твит. Между нами завязалась беседа. Я не уверен, что хочу, чтобы её читал мой босс и ещё сотни пользователей по всему миру. Сейчас личные сообщения можно отправлять только одному пользователю, но в будущем, я думаю, наше развитие будет сконцентрировано также и на том, чтобы у сервиса появились настройки, позволяющие общаться приватно сразу с несколькими людьми», – рассказал Э. Ното.

Ещё одним приоритетным направлением развития интернет-компании Э. Ното назвал улучшение работы внутренней системы поиска в Twitter. Подробностей того, как может функционировать обновлённый алгоритм поиска по твитам, представитель соцсети не раскрыл, отметив лишь, что поиску должна быть отведена более заметная роль. «Twitter обладает огромным количеством ценной информации по твитам на ту или иную тему. Всё, что нам нужно теперь – это разработать новый алгоритм, который позволял бы глубоко и широко анализировать этот контент, выдавая релевантные данные с привязкой к теме и конкретным пользователям», – считает Э. Ното ***(Twitter задумался о внедрении групповых чатов и нового поисковика // Media-бізнес (http://www.mediabusiness.com.ua/content/view/40557/126/lang,ru). – 2014. – 4.09).***

***

Сервис микроблогов Twitter изменил процесс регистрации пользователей, чтобы быстрее вовлекать новых участников в активное взаимодействие с платформой. Эта мера должна снизить количество забросивших свои микроблоги людей

Теперь новые пользователи Twitter будут просматривать во время регистрации большое количество рекомендованных сервисом аккаунтов, чтобы сразу составить свой круг чтения. Рекомендации составляются на основе указанных при регистрации интересов. При этом Twitter автоматически устанавливает галочку на подписку для всех автоматически выбранных аккаунтов. Из-за этого пользователю придется собственноручно снимать галочки, чтобы не читать тех, кто ему не интересен.

Если раньше пользователи сервиса микроблогов видели только аватарки рекомендованных пользователей, то теперь Twitter выводит образец одного из популярных твитов блогера, чтобы помочь составить впечатление о человеке.

Это крупнейшее изменение в страничке регистрации Twitter за последние три года. В последнее время Twitter активно работает над модернизацией сервиса. Такая активность связана, прежде всего, с продолжающимися попытками сервиса достичь безубыточности. В 2014 г. сервис микроблогов столкнулся с замедлением прироста пользовательской базы и падением активности читателей.

Компания в данный момент отчаянно нуждается в большем количестве лояльных ресурсу потребителей, которые, зайдя раз, оставались бы надолго. Только так можно обеспечить стабильный поток рекламных средств ***(Twitter попробовал стать интереснее для новых пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_poproboval_stat_interesnee_dlya_novyh_polzovateley). – 2014. – 5.09).***

***

Американский разработчик создал социальную программу для трезвых людей

Социальная программа Sobbr представляет собой сервис, который постоянно фильтрует публикуемые материалы и при необходимости может автоматически удалить всё, что было выложено пользователем в сеть в течение последних 24 часов.

Предполагается, что программа будет помогать пользователю удалять любой «компромат», который мог быть выложен в социальные сети во время особо весёлых моментов жизни, когда градус алкоголя вступает в конфронтацию с инстинктом самосохранения. Проще говоря, программа позволит пользователю «сохранить лицо» и не показывать всему миру свои фотографии с алкогольных вечеринок.

Так, программа Sobbr автоматически удаляет всё, что было опубликовано в социальных сетях за последние 24 часа, включая фотографии, видеоролики и тестовые записи. Кроме того, программа удаляет всех друзей, которые были добавлены за это время, и полностью зачищает истории переписок.

В настоящее время аудитория сервиса, который свободно доступен пользователям всего мира, составляет более 10 тыс. пользователей, и этот показатель постоянно растет ***(Американский разработчик создал социальную программу для трезвых людей // Блог Imena.UA (http://www.imena.ua/blog/американский-разработчик-создал-соц). – 2014. – 26.08).***

***

Facebook анонсировала два новых улучшения, которые в ближайшее пару месяцев должны затронуть ленту новостей соцсети. Первое из них направлено на борьбу с так называемыми кричащими заголовками постов. Речь идет о публикациях, которые для привлечения внимания снабжают надписями вроде «Смотреть всем!», «Это невероятно!», «Это должен видеть каждый!», «Вы не поверите!» и т. п. Как правило, такая уловка почти всегда работает: пост получает больше кликов и поднимается в ленте выше.

При этом опрос показал, что пользователи (80 %) предпочитают видеть в своих лентах такие публикации, заголовки которых не давят на них, но позволяют им самим решать, хотят ли они прочитать всю статью целиком. А

в реальности такой по-настоящему ценный материал может быть погребен под кучей «нечестных» постов, часто недалеко ушедших от спама.

Чтобы изменить ситуацию, распознавать и искусственно «заминусовывать» такие посты, разработчики Facebook придумали два сценария. Во-первых, они будут замерять, сколько времени пользователь проводит на стороннем ресурсе после перехода туда со страницы соцсети. Если он кликнул на ссылку, а потом почти сразу закрыл ее и вернулся обратно в свою ленту, значит материал особой ценности для него не представлял. Во-вторых, они будут учитывать соотношение переходов по ссылке с количеством лайков, перепостов и комментариев к ней. Если переходов много, а всех видов «обратной связи» нет, это также укажет на низкое качество контента.

Второе улучшение связано с оформлением ссылок в ленте новостей. Сотрудники соцсети выяснили, что люди предпочитают кликать на ссылки, которые публикуются в естественном виде, то есть выглядят как веб-адрес. Это дает им дополнительную информацию о ресурсе, на который им предлагается перейти. Так вот такие посты будут в большем приоритете в сравнении с теми, которые содержат короткие «нечитаемые» ссылки в подписях к картинке или обновлениях статуса ***(Facebook будет бороться с кричащими заголовками // InternetUA (http://internetua.com/Facebook-budet-borotsya-s-kricsasximi-zagolovkami). – 2014. – 27.08).***

***

Соцсеть «ВКонтакте» обновила свое мобильное приложение для Android. Одним из главных новшеств, пожалуй, стала функция быстрого добавления в друзья находящихся поблизости пользователей.

Чтобы найти потенциального друга, нужно зайти в раздел «Друзья» и нажать кнопку «друзья поблизости». В результатах отобразятся пользователи, находящиеся в радиусе 2 км и при условии, что они в это же время также заняты поиском друга с помощью этого сервиса. Если нужного человека обнаружить не удается, можно использовать камеру для QR-кода.

Как сообщается на странице соцсети «LIVE Экспресс», в приложении также появились и другие «приятные мелочи». Как, например, выбор из недавно отправленных стикеров, настройка уведомлений от игр, возможность загружать аватарку сообщества, а также полноценная двухфакторная аутентификация и поддержка португальского языка. Последнее, по всей видимости, вызвано нарастающей аудиторией «ВКонтакте» в Бразилии ***(«ВКонтакте» запустил сервис «Друзья поблизости» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/vkontakte_zapustil_servis_druzya_poblizosti). – 2014. – 3.09).***

***

После того как Mail.ru Group выкупит «ВКонтакте», социальную сеть постепенно интегрируют в сервис интернет-компании. Такую точку зрения высказал в интервью Abnews интернет-эксперт А. Меркуров.

«Ничего хорошего, я думаю, “ВКонтакте” уже не ждет. UCP сделало свое “черное дело”. С точки зрения бизнеса, они заработали денег. С другой стороны, благодаря акционерным конфликтам, они все-таки подразвалили компанию. Я не думаю, что Mail.ru Group идеологически близок “ВКонтакте”, и им не будет интересно с этим сервисом возиться, так как он развивался при Дурове. <…> Если сделка произойдет, “ВКонтакте” постепенно будет интегрироваться в сервис Mail.ru Group. Тот “ВКонтакте”, который мы помним при Дурове, уже не тот, и мы про него можем забыть», – уверен А. Меркуров.

Также он отметил, что в политике социальной сети не будет резких изменений. По мнению А. Меркурова, изменения могут, в частности, коснуться увеличения количества рекламы.

Напомним, по данным газеты «Ведомости», переговоры Mail.ru Group и фонда UCP о покупке 48 % акций «ВКонтакте» в настоящее время находятся в завершающей стадии. Если сделка произойдет, то компании А. Усманова будет принадлежать 100 % акций социальной сети.

Человек, хорошо знакомый с совладельцами «ВКонтакте», рассказал, что, по его данным, летом А. Усманов провел переговоры с П. Дуровым о его возможном возвращении в компанию – не на операционные позиции, а на должность «главного архитектора» сети. Источник, близкий к «ВКонтакте», сомневается, что П. Дуров вернется – для него это «пройденный этап» ***(Можете забыть про тот «ВКонтакте», который был при Дурове // InternetUA (http://internetua.com/ekspert--mojete-zabit-pro-tot--vkontakte---kotorii-bil-pri-durove). – 2014. – 7.09).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Украинские пользователи вывели в безоговорочные лидеры сети микроблогов Twitter хэштег #RussiaInvadedUkraine.

Записи с соответствующим тэгом появляются ежесекундно сотнями. Всего за несколько часов пользователями со всего мира было создано более 195 тыс. записей, помеченных хештегом #RussiainvadedUkraine. Инициатива в сети микроблогов стартовала сразу после появления сообщений о прямом вторжении российской военной техники и солдат вблизи Новоазовска и Мариуполя.

Таким образом, пользователи социальной сети решили привлечь внимание мирового сообщества к новому этапу российского вторжения в Украине.

Помимо рядовых пользователей, акцию поддержал ряд европейских политиков, в частности весьма активно хештег #RussiainvadedUkraine использует министр иностранных дел Швеции К. Бильдт, признавший наличие регулярных российских войск на Донбассе ***(Хэштег #RussiaInvadedUkraine стал абсолютным лидером в Twitter // Блог Imena.UA (http://www.imena.ua/blog/russiainvadedukraine). – 2014. – 29.08).***

***

Рада національної безпеки і оборони склала список достовірних сторінок органів влади в соцмережі Facebook. Він оприлюднений на сайті РНБО.

«Для запобігання створенню так званих “фейкових”, фальшивих сторінок недоброзичливцями, які порочать роботу українського уряду та окремих посадових осіб, відтепер правильні сторінки мають відповідну відмітку: синю “галочку” і напис “Підтверджена сторінка”», – повідомив Я. Дух, керівник прес-служби РНБО.

При цьому уточнюється, що список поки що не остаточний ***(РНБО склав список достовірних сторінок органів влади у Facebook // LB.ua (http://ukr.lb.ua/news/2014/08/27/277420_snbo_sostavil_spisok_dostovernih.html). – 2014. – 27.08).***

***

В социальной сети Facebook россияне создали группу «Груз 200 из Украины в Россию», к которой за несколько дней добавилось несколько сотен участников.

Как отмечается в сообщении, люди в соцсети сгруппировались для того, чтобы возвратить тела российских военных, погибших в Донбассе. «На правах администратора сообщаю: сегодня в группу самостоятельно добавилось 1750 человек. Это много. Большинство людей не знали о том, что в Донбассе идет война и очень много груза 200. Украина за свой счет готова передать тела в Россию, однако российские власти умалчивают этот факт», – говорится в сообщении группы.

Администраторы страницы также в данной группе запрещают агрессию и оскорбления, а все споры рекомендуют отправлять личным письмом или высказывать свою позицию на собственных страницах. «Многие испытали шок от правды. Тем, кто не верит, советую проехать в ростовские морги для начала. Если вы ищете родных, не стесняйтесь оставлять запросы в этой группе, не пишите мне в личку. Никакой ложной скромности тут не должно быть. Если вам уже пригрозили, что не вернут тело, если вы будете спрашивать открыто, – значит, это блеф!!! Все, кто был с документами, известны и в ростовских моргах, и в СБУ Украины –

установленные тела вернут обязательно, причем с Украины за счет украинской стороны!» – говорится в сообщении группы в соцсети ***(Россияне без помощи власти работают над возвращением тел погибших в Украине // Донецкие вести (http://www.donetskie.com/news/rossiyane-bez-pomoshchi-vlasti-rabotayut-nad-vozvrashcheniem-tel-pogibshikh-v-ukraine). – 2014. – 28.08).***

***

Украинцы с помощью Twitter призывают Европу и НАТО вмешаться в военный конфликт и помочь Украине в противостоянии с Россией. На момент выхода этой новости хештег #NATOforUkraine занимал первую позицию в украинском рейтинге Twitter – им уже поделилось более 60 тыс. пользователей сервиса. Инициатива стартовала после очередного обострения ситуации на Востоке Украины и окружения сил АТО террористами и регулярными войсками РФ, пишет AIN.UA (http://ain.ua/2014/09/04/539285).

Помимо текстовых сообщений, многие пользователи публикуют тематические фотографии. Фотограф В. Содель предложил использовать демотиваторы о возможном вторжении России в Европу ***(Украинцы запустили Twitter-шторм, в котором предостерегают Европу от российского вторжения // AIN.UA (http://ain.ua/2014/09/04/539285). – 2014. – 4.09).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Социальная сеть «ВКонтакте» с 25 августа ввела премодерацию размещаемых через биржу «ВКонтакте» постов, что позволило размещать коммерческие постинги с помощью собственной биржи на страницах официальных сообществ, СМИ и брендов, рассказал Roem.ru евангелист социальной сети А. Усманов.

Изменения уже доступны и видны в интерфейсе биржи постов. Ранее верифицированные сообщества не могли размещать рекламу на своих страницах, так как это противоречило правилам социальной сети.

Страницам официальных сообществ установлен более жёсткий лимит на число рекламных постингов: их можно публиковать не чаще пяти раз в неделю. Продвижение собственных проектов организаторов сообществ при совпадении тематики не ограничивается.

Проверка предлагаемых к публикации сообщений модераторами «ВКонтакте», по словам А. Усманова, не изменит уже сложившуюся схему взаимодействия администраторов и рекламодателей: рекламодатели по-прежнему сами смогут выбирать желаемые площадки для размещения

рекламы, а руководство сообществ – определять, какую именно рекламу из предложенных публиковать.

Скорее всего, дополнительная проверка модераторам «ВКонтакте» вводится для приведения рекламных постов к единообразному виду, что позволит рекламодателям ожидать более предсказуемого эффекта от размещений, а администраторам получать более однородную и привычную пользователям рекламу.

Биржа постов «ВКонтакте» была запущена в конце 2013 г., в то время она решала несколько задач:

– помогала крупным рекламодателям закупать посты непосредственно через «ВКонтакте» при оплате их по безналичному расчёту;

– позволила упорядочить и исследовать «дикий» рынок размещения платных постов;

– дала возможность размещать рекламу, которую видят и мобильные пользователи «ВКонтакте» (на мобильной версии социальной сети тогда не было возможности размещения рекламы) ***(ВКонтакте начал проверять коммерческие посты // InternetUA (http://internetua.com/vkontakte-nacsal-proveryat-kommercseskie-posti). – 2014. – 26.08).***

***

Корпорація Twitter має наміри поширити свою рекламну мережу на ще 12 країн Центральної та Східної Європи, у тому числі Україну. Про це повідомляє Financial Times.

Ідеться про Австрію, Боснію та Герцеговину, Болгарію, Хорватію, Чехію, Македонію, Румунію, Сербію, Словенію, Швейцарію, Португалію та Україну.

«Ми бачимо попит від брендів [у цих країнах]», – сказав А. Джафарі, керівник Twitter із прямого продажу в Європі та Африці. За його словами, підприємці самі прагнули працювати із сервісом мікроблогів.

Відтепер бізнесмени в згаданих країнах отримають змогу публікувати в сервісі мікроблогів платні повідомлення, маркетингове відео, фото тощо ***(Twitter надаватиме рекламні послуги у ще 12 європейських країнах // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/34023). – 2014. – 26.08).***

***

Социальная сеть Facebook позволит рекламодателям показывать пользователям рекламу в зависимости от скорости их интернет-соединения, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-stargetiruet-reklamu-v-zavisimosti-ot-skorosti-soedinenija-40999).

Новая функция рекламного таргетинга позволит разделять аудиторию в зависимости от типа интернет-соединения: 2G, 3G или 4G. В пресс-релизе компания отмечает, что новый тип таргетинга будет особенно актуальным

для быстроразвивающихся стран, где интернет-инфраструктура ещё не стабильна.

Facebook начинает экспансию в новые страны, в том числе благодаря глобальной инициативе Internet.org – программе, позволяющей людям, не имеющим доступа в Интернет, получить его. Большое количество пользователей, в особенности новых, использует Facebook с мобильных устройств. В марте 2014 г. социальная сеть запустила видеорекламу, которая встраивается в ленты пользователей. В частности, именно её качество будет зависеть от скорости соединения.

Во II квартале 2014 г. рекламная выручка Facebook составила 2,7 млрд дол., из них 72 % пришлось на США, Канаду и Европу. Пользовательская база социальной сети в развивающихся странах растёт в четыре раза быстрее, чем в вышеупомянутых. В Индии каждый месяц Facebook используют 100 млн человек, из них 66 % не используют смартфоны.

Facebook регулярно подвергается нападкам пользователей – некоторые из них считают рекламные механизмы социальной сети не очень эффективными, некоторые не могут понять алгоритм сортировки записей в ленте пользователей, другие утверждают, что Facebook регулярно нарушает приватность. В пресс-релизе представители социальной сети подчеркнули, что рекламодатели не имеют доступа к личным данным ***(Facebook старгетирует рекламу в зависимости от скорости соединения // Marketing Media Review (http://mmr.ua/news/id/facebook-stargetiruet-reklamu-v-zavisimosti-ot-skorosti-soedinenija-40999). – 2014. – 28.08).***

***

Facebook в партнерстве с Parse и Mixpanel представил аналитику для кросс-платформенной системы глубоких ссылок App Links. Система призвана упростить разработчикам переход по ссылкам к конкретному контенту. Этот шаг должен убедить разработчиков использовать App Links для трафика между приложениями.

С момента запуска системы в апреле 2014 г. было создано более 3 млрд уникальных ссылок на сотни приложений, включая Spotify, Hulu, Vimeo, и Airbnb.

Разработчики, использующие новые аналитические инструменты Facebook, могут отследить:

– перенаправление пользователя в другое приложение;

– вход пользователя в их приложение из App Link;

– его возвращение из другого приложения.

Использование разработчиками App Links призвано способствовать развитию электронной коммерции и рекламы в мобильной ленте новостей Facebook. Таким образом, Facebook сначала вынуждает разработчиков приложений платить социальной сети за установку приложений на устройства пользователей, а потом еще раз платить – за возврат этих же

пользователей, которым будут транслироваться специальные напоминания в новостной ленте в виде нативной рекламы с прицельным таргетингом.

Facebook также объявил о нескольких незначительных обновлениях App Links. Система теперь поддерживает Windows 8 и универсальные Windows-приложения и ОС Android.

Кроме того, на сайте App Links также появится блог, который будет обновляться примерами проектов и тематических исследований, чтобы дать пользователям лучшее представление о технологии.

В начале июля 2014 г. Facebook сообщил, что отныне будет обеспечивать повторное вовлечение пользователей в работу с приложением с помощью AppLinks ***(Facebook представил аналитику для App Links // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_predstavil_analitiku_dlya_app_links). – 2014. – 27.08).***

***

WebMoney представила финальную версию Keeper для Facebook и обновления приложения для российских социальных сетей, сообщает lenta.ru

Доработка бета-версии Keeper для Facebook касалась технической части приложения, функциональность сервиса сохранилась такой же. Для российских соцсетей увеличилось число партнеров, для которых можно провести оплату, изменена система навигации по провайдерам услуг и упрощена процедура оплаты для сокращения времени операций пользователем.

Для всех трех соцсетей приложения позволяют вести расчеты с «френдами» из социальных сетей, оплачивать услуги и товары со страницы своего профиля пользователя. Компания отмечает возможность оплаты популярных онлайн-игр и пополнение счета аккаунтов в интернет-сервисах.

Особенность версий для соцсетей: пользователь видит, кто из «френдов» установил Keeper. Приложение позволяет перечислить средства, взять или дать в долг знакомому из социальной сети.

После установки WebMoney Keeper программа доступна на странице социальной сети в разделе «Приложения». На ней пользователь получает доступ к истории предыдущих операций по переводу денег. Если пользователь ранее не регистрировался в системе WebMoney, ему необходимо создать новый кошелек.

WebMoney Keeper для социальных сетей доступен на русском, английском, испанском, португальском, вьетнамском и турецком языках. Платежная система расчетов WebMoney Transfer имеет приложение Keeper для операционных систем Windows, MacOS, Linux, iOS, Android, Bada ***(Facebook получила финальную версию приложения для платежей через WebMoney // Media бізнес (http://www.mediabusiness.com.ua/content/view/40514/126/lang,ru). – 2014. – 1.09).***

***

П. Лэй из Facebook недавно опубликовала в одном из сообществ пост о готовящихся изменениях в рекламном функционале социальной сети. Это уже вторая волна нововведений, которые коснутся рекламодателей. Что это за изменения и что они несут, разбирается известный эксперт по Facebook Д. Лумер.

Очередные изменения в настройках рекламных объявлений начнутся в Facebook с сентября 2014 г. Прежде чем мы разберем их, стоит вспомнить, как обстояли дела с настройками рекламы ранее. В марте 2014 г. Facebook представил новый функционал менеджера рекламных кампаний:

1. Кампания: Цель РК.
2. Наборы объявлений: Расписание, Бюджет.
3. Объявление: Создание, Размещение, Таргетинг, Ставки.

Самым большим изменением было появление наборов рекламных объявлений. С учетом грядущих изменений интерфейс менеджера рекламных кампаний будет выглядеть следующим образом:

1. Кампания: Цель РК.
2. Наборы объявлений: Расписание, Бюджет, Ставки, Таргетинг, Размещение,
3. Объявление: Создание.

По задумке Facebook таргетинг, размещение объявления и торги перемещаются в наборы объявлений, что поможет рекламодателям облегчить процесс создания объявлений.

Что это означает?

Когда в марте этого года Facebook изменил менеджер рекламы, добавив в него «Наборы объявлений», для каждого набора рекомендовалось создавать отдельную аудиторию – таким образом, все рекламные объявления в наборе таргетировались на одну и ту же группу людей, что позволяло их легко оптимизировать.

Нынешнее же изменение официально означает, что рекламодатель больше не в состоянии будет изменить параметры таргетинга для объявлений группы. Поменять можно будет только содержание объявления.

Новый алгоритм настроек коснется только тех объявлений, которые созданы уже после очередного нововведения. На старые компании это повлиять не должно. Новая структура рекламной кампании Facebook станет для всех обязательной в январе следующего года. И ещё. Если ключевыми моментами в создании объявлений для вас являются такие критерии, как «ставки» (Bidding) и «размещение» (Placement), то в этом случае предстоит создавать больше наборов объявлений.

Когда этого ожидать?

Полноценное введение изменений начнется с 1 сентября для менеджера рекламы, для инструментов создания объявлений и сервиса Power Editor. Ожидается, что обновления окончательно завершатся к середине сентября,

чтобы все рекламодатели смогли использовать новые возможности с 1 октября 2014 г.

Участникам программы PMD (Preferred Marketing Developer) Facebook дает по меньшей мере пять месяцев, чтобы подготовиться к обновлению. Тем, кто использует API (интерфейс программирования приложений), придется перейти на обновленный интерфейс не ранее начала следующего года.

Чего ждать ещё?

В посте П. Лэй можно увидеть и прогноз на будущее. Наибольший интерес вызывает фраза о запуске передовых технологий контроля за частотой показов объявлений, управлением аудиторией и бюджетом рекламных кампаний, которые Facebook может внедрить в ближайшем будущем.

Многие рекламодатели уже давно мечтают о появлении функции управления всем, что относится к частоте показов объявлений. Однако пока не совсем ясно, что собой будет представлять такая функция, равно как и управление аудиторией. Введение потолка для бюджета на рекламную кампанию будет автоматически означать и лимит в дополнение к ежедневному бюджету, задаваемому на уровне набора объявлений.

Отметим, что Facebook также выпустил руководство, содержащее информацию об изменениях в структуре рекламной кампании и советы по созданию эффективных объявлений ***(Facebook снова обновляет структуру рекламной кампании // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_snova_obnovlyaet_strukturu_reklamnoy_kampanii). – 2014. – 1.09).***

***

Пользователи ежедневно публикуют в Интернете 1,8 млрд фотографий через сервисы вроде Facebook, Instagram, Flickr, Snapchat, WhatsApp. Это всё равно если бы каждый житель Земли выкладывал по одному фото чуть чаще, чем раз в неделю.

Аналитики указывают на то, что архив фотографий конкретного человека позволяет многое узнать о нём: увлекается ли спортом, что любит кушать, по каким странам путешествует, есть ли семья, дети и т. д.

Все эти сведения – весьма ценная информация для рекламодателей. Так, если на снимке человек держит в руках продукцию определённого бренда, ему можно начать показывать рекламу этого или конкурирующих производителей.

На другом снимке узнаваема марка косметики или обуви – соответственно, можно сделать вывод о лояльности клиента к данному товару.

Предполагается, что в самое ближайшее время фотохостинги начнут проводить такой анализ автоматически. Владельцы социальных сетей смогут

увеличить доходы от рекламы, предложив компаниям точное целевое таргетирование аудитории.

Кроме того, сегодня уже есть группы, которые специализируются на обработке фотографий в социальных сетях по заказу рекламодателей. Компания DittoLabs обслуживает такие известные корпорации, как KraftMacaroni&Cheese, Cadillac и Coca-Cola.

По их запросам специалисты, например, составляют отчёт о том, сколько людей фотографируются с продуктом конкретного производителя, по сравнению с продуктом конкурента ***(Личные фото превратились в источник данных для рекламных агентств // Блог Imena.UA (http://www.imena.ua/blog/18-billion-photos-to-social-media). – 2014. – 2.09).***

***

В конце августа 2014 г. в Facebook произошло несколько изменений, касающихся владельцев бизнес-страниц. Соцсеть запустила рекламу мероприятий прямо в новостной ленте как для десктопных, так и для мобильных посетителей, создала вкладку «Мероприятия» и обновила интерфейс страниц событий, пишет Marketing Media Review (http://mmr.ua/news/id/v-novostnoj-lente-facebook-pojavitsja-reklama-meroprijatij-41063).

Представители социальной сети отметили, что мероприятия на Facebook каждый месяц используют более 400 млн пользователей по всему миру. При этом почти 30 % всех событий, будь то концерт или вечеринка, создаются бизнес-страницами. Этот факт подтолкнул разработчиков Facebook к тому, чтобы предоставить владельцам таких страниц ещё один способ выйти к аудитории – объявления с рекламой предстоящих событий.

Объявления с рекламой мероприятий пользователи увидят в ленте новостей – как на обычном компьютере, так и на мобильном устройстве. Ранее информация о событиях отображалась в правой колонке интерфейса веб-версии Facebook.

Возможность создавать объявления появится в ближайшие несколько недель, и делать это можно будет при помощи Power Editor и инструмента создания рекламы.

Владельцы страниц смогут видеть в правой колонке следующие данные:

– число людей, видевших ссылку на событие;

– число людей, просмотревших событие;

– количество присоединившихся к мероприятию, число добавивших его в раздел «Сохраненное» и тех, кто примет участие в нем.

Вкладка «Мероприятия» (Events) также добавлена на панель инструментов бизнес-страниц, причем порядок вкладок можно поменять, поставив раздел «Мероприятия» первым. Если пользователь просматривает страницу с мобильного устройства, то он сможет ознакомиться ещё и с предстоящими событиями.

Изменен и интерфейс страницы события, что позволит сконцентрировать больше внимания на предстоящих мероприятиях. Пользователю будут рекомендоваться события на основе страниц, которые он лайкнул, а также согласно местоположению события и дню недели, в который оно состоится.

Нововведения помогут владельцам страниц понять, что работает при продвижении мероприятий. Напомним, что ранее в раздел «Мероприятия» был добавлен раздел аналитики ***(В новостной ленте Facebook появится реклама мероприятий // Marketing Media Review (http://mmr.ua/news/id/v-novostnoj-lente-facebook-pojavitsja-reklama-meroprijatij-41063). – 2014. – 2.09).***

***

Директор по маркетингу Buffer К. Сайтер рассказала в блоге компании об исследованиях в области социальной психологии, которые пригодятся маркетологам. По словам К. Сайтер, захватывающие исследования о соцмедиа публикуются едва ли не каждый день. Они позволяют узнать, как социальные сети влияют на взаимоотношения людей и обмен информацией и формируют личность человека. К. Сайтер выбрала несколько свежих исследований и объяснила, чем они могут быть полезны для маркетологов и SMM-специалистов, пишет Marketing Media Review (http://mmr.ua/news/id/kak-vazhno-byt-schastlivym-issledovanija-socsetej-o-kotoryh-polezno-znat-kazhdomu-marketologu-40980).

Эмоции заразительны

Эмоции передаются от человека к человеку в Интернете точно так же, как в оффлайне, пишет К. Сайтер, ссылаясь на масштабное исследование, проведенное учеными Калифорнийского университета. Они изучили эмоциональное содержание более миллиарда постов в Facebook, опубликованных за два года. Особое внимание ученые уделили постам, написанным в дождливые дни. Выяснилось, что мрачные эмоции, которыми делились люди в городах, где шел дождь, передавались их друзьям, живущим там, где дождя не было. Иначе говоря: то, что люди чувствуют и о чем говорят в одной точке мира, может в тот же день распространиться повсеместно.

Однако позитивные эмоции распространяются еще быстрее, чем негативные. Это показало другое исследование постов в Facebook. В среднем, одна мрачная запись вызывала 1,29 постов с тем же настроением, а одна позитивная – 1,75.

К. Сайтер советует маркетологам держаться «светлой стороны»: приносить радость покупателям, решать сложные проблемы в оффлайне, а на на негативные отзывы реагировать быстро, чтобы они не распространились на окружающих.

Как бороться с самоцензурой

К. Сайтер пишет, что люди чувствуют себя слегка неуютно, когда собираются сказать миру что-то новое. Иногда это чувство лишь обостряет творческие способности, а иногда оно делает людей нерешительными, и они просто отказываются от своего намерения.

Ученые провели исследование, посвященное самоцензуре – записям, которые были написаны, но так и не опубликованы. Они изучали данные 3,9 млн пользователей в течение 17 дней. Оказалось, что 71 % из них написал хотя бы один статус или комментарий, который не опубликовал. В среднем, одна набранная, но не опубликованная запись приходилась на 4,52 статусов и 3,2 комментариев.

Исследователи предположили, что люди передумывают публиковать свои записи тогда, когда им трудно определить свою аудиторию. Именно поэтому самоцензура в комментариях случается реже – там собирается более понятная аудитория.

К. Сайтер говорит, что маркетологу, который хочет успешнее взаимодействовать с аудиторией, нужно хорошо ее изучить. Для этого она советует использовать метод персон. При этом важно не забывать о «невидимой аудитории», которая ничего вам не говорит, но внимательно вас слушает.

По фото встречают

К. Сайтер пишет, что правильное фото в профиле соцсети ценится на вес золота. Недавно проведенное исследование показало, что люди делают вывод о тех, кто изображен на фото, меньше чем за секунду (точнее, за 40 миллисекунд).

Исследователи показали участникам эксперимента портреты, которые немного отличались выражением лица, и предложили оценить людей, изображенных на снимке, по различным характеристикам – таким как, например, надежность, интеллигентность, креативность. Выяснилось, что даже незначительное изменение выражения лица может вызвать совершенно противоположное впечатление о человеке.

К. Сайтер советует не пренебрегать A/B-тестированием своих фотографий в профиле.

«Щедрые» и «скупые» страны

Двадцать четыре процента пользователей соцсетей делятся всем или почти всем подряд. К такому выводу пришли специалисты компании Ipsos. 19 % не делятся вообще ничем. Кроме того, процент тех, кто делится и кто нет, зависит от страны. Если проникновение Интернета низкое (как в Азии, Латинской Америке и Африке), то люди делятся часто. И наоборот, в Европе, где все «сидят» в Интернете, люди делятся неохотно.

К. Сайтер рекомендует маркетологам привести свои ожидания о «шеринге» в соответствие с нормами, демографией и регионом проживания аудитории.

Соцсети объединяют

К. Сайтер пишет, что комьюнити в социальных сетях не пустое слово – оно действительно существует. Исследование, проведенное доктором С. Тобин из Школы психологии Квинслендского университета, подтвердило, что активное участие в соцмедиа приносит пользователям сильное чувство общности.

С. Тобин попросила одних участников эксперимента часто публиковать и общаться в выбранной группе Facebook, а других – лишь следить за активностью своих друзей. Через два дня последние пожаловались, что эксперимент ухудшил их самочувствие.

Другое исследование продемонстрировало схожие результаты: в нем участвовали люди, которые оставляли записи в Facebook, но не получали лайков и комментариев. Это также негативно повлияло на их самооценку и самочувствие.

К. Сайтер пишет, что пользователи соцсетей жаждут ответной реакции и маркетологам следует организовать свое время так, чтобы не только продвигать свой контент, но и включаться в обсуждения продуктов.

Страх и ненависть в соцсетях

Известно, что люди чаще всего делятся контентом, который пробуждает сильные чувства (как гнев и трепет). Исследователь Й. Бергер предлагает теорию того, почему это происходит: эмоциональное возбуждение резко активизирует нашу нервную систему. «Шеринг» гасит напряжение и помогает выйти из этого неприятного состояния. Как беда не ходит одна, так и сильные чувства нуждаются в сопереживании.

К. Сайтер рассказывает о двух связанных между собой исследованиях. В первой группе одни участники смотрели видео, возбуждающие сильные эмоции, а в другой – клипы с нейтральным содержанием. Во второй группе одни участники сидели на месте, а вторые бегали. После этого всех участников спросили, собираются ли они поделиться подготовленной статьей. Люди, которые пребывали в состоянии сильного возбуждения (бегуны и зрители эмоциональных видео), проявляли больше готовности делиться.

К. Сайтер советует маркетологам использовать этот закон в своих целях и привести читателей в трепет полезной статьей или ошарашить увлекательной историей.

Альтернатива еде и сексу

Мы любим говорить о самих себе, пишет К. Сайтер. Гарвардские ученые выяснили, что реакция мозга на это удовольствие сравнима с реакцией на удовольствие от еды, денег или секса. В некоторых экспериментах люди даже отказывались от денег, чтобы поговорить о самих себе.

Неудивительно, что в социальных медиа это используется на всю катушку. Ученые обнаружили, что 80 % постов в соцмедиа описывают собственные переживания.

К. Сайтер пишет, что, вооружившись этим знанием, маркетологи могут поработать над тем, чтобы меньше говорить о себе, больше слушать и чаще приходить на помощь. Тем самым их продукт получит больше сторонников ***(Как важно быть счастливым: исследования соцсетей, о которых полезно знать каждому маркетологу // Marketing Media Review (http://mmr.ua/news/id/kak-vazhno-byt-schastlivym-issledovanija-socsetej-o-kotoryh-polezno-znat-kazhdomu-marketologu-40980). – 2014. – 26.08).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Исследователи Ф. Сабатини из римского университета Ла Сапьенца и Ф. Саррачино из Центральной службы статистики и экономических исследований Люксембурга доказали, что пользователи социальных сетей быстро становятся несчастнее, чем те, кто полностью игнорирует IT-коммуникации.

В исследовании приняли участие около 50 тыс. человек. Всем задавались одни и те же вопросы: насколько они довольны своей нынешней жизнью, как часто они встречаются с друзьями, доверяют ли сторонним людям и чем обычно занимаются в Интернете. На основании собранных ответов учёные смогли сделать несколько интересных выводов.

Во-первых, люди, как правило, более открыты и удовлетворены своей жизнью, если чаще встречаются со своими друзьями в реальности.

Во-вторых, пользователи, которые много внимания уделяют социальным сетям, склонны с подозрением относиться к сторонним людям.

Кроме того, социальные сети имеют общий негативный эффект на пользователей: те становятся более несчастными и раздражительными из-за проявлений ненависти и дискриминации, частых в сети.

Тем временем власти США собирают и анализируют записи пользователей Twitter, Facebook, Pinterest и других сайтов, чтобы узнать, как происходит установление социальных связей и распространение сообщений в Интернете ***(Социальные сети делают людей несчастными // Блог Imena.UA (http://www.imena.ua/blog/social-networks-negative-effect-study). – 2014. – 3.09).***

***

Центр медиакоммуникаций «Новая Украина» проанализировал тенденции распределения симпатий интернет-пользователей в контексте появления новых мемов, идентифицирующих проукраински и пророссийски настроенное население.

«Картой мира», «картиной мира», «видением мира» или «моделью мира» в психологии, лингвистике, философии называют представления о мире, отраженные в человеческом сознании. Вполне очевидно, что свое отображение «карта мира» каждого из нас находит в тех текстах, которые мы пишем, в том числе и в социальных сетях.

«Карты мира» украинцев в разных частях страны отличаются – это известный факт. Украинское общество традиционно идеологически разделено. У жителей Запада и Востока зачастую разные «карты мира», начиная от политических, мировоззренческих и заканчивая культурными предпочтениями.

В социальных сетях в конце 2013 – в начале этого года была очень заметна картина разногласий между приверженцами и оппонентами Майдана. В ходе зимних событий на главной площади страны в сети существовало две противоборствующие стороны: Евромайдан и Антимайдан. Если тогда идеологические оппоненты на форумах и прочих обсуждениях называли друг друга «майдановец» или «антимайдановец», то сегодня мы наблюдаем новый раздел: в сети прижились новые мемы – «укры» и «вата».

«Укропы», «укры» – пренебрежительное название в сети украинцев, которые поддерживают действующую власть, АТО и проевропейскую ориентацию страны.

«Ватники», «вата» – пренебрежительное название в сети пророссийски ориентированных людей, поддерживающих самопровозглашенные ЛНР, ДНР, сепаратистов и действия России.

Полем для исследования стала социальная сеть «ВКонтакте», так как она дает возможность при мониторинге зафиксировать географическую привязку аккаунтов пользователей, в том числе и с ретроспективой. В этом исследовании, к сожалению, не представлены данные по Крыму: получить статистически достоверные сведения из этого региона на данный момент нам не под силу.

Как измерялось количество «укров» и «ватников» в областях

Для мониторинга был разработан специальный метод исследования аккаунтов пользователей соцсети «ВКонтакте». Были проанализированы самые активные и самые многочисленные сообщества на сайте, которые имеют четкое проукраинское или пророссийское позиционирование. Среди таких сообществ: «Евромайдан SOS», «Крылья Феникса», «Армия SOS», «Евромайдан Майдан АТО» и их оппоненты: «Новороссия», «Юго-Восток Новороссия», «Республика Новороссия Антимайдан», ДНР и им подобные.

Далее были посчитаны аккаунты пользователей, которые входят в сообщества одной направленности – проукраинские или пророссийские по

состоянию на 7 июля 2014 г. (Те аккаунты, которые входили сразу в несколько идеологически противоречащих друг другу сообществ, не принимались во внимание). После этого, с помощью географической привязки аккаунтов, интернет-пользователи были разбиты по областям в количественном и процентном соотношении.

Что показал мониторинг?

Во всех областях, кроме Донецкой и Луганской, преобладает количество проукраински настроенных интернет-пользователей. Западная Украина ожидаемо демонстрирует существенное превалирование «укров» перед «ватниками». Одесская, Запорожская, Харьковская, Херсонская, Днепропетровская, Николаевская и Киевская области показывают заметную долю «ваты», но не «дотягивающую» до половины количества пользователей.

Из общей картины явно выделяется только Донбасс, где в настоящее время происходят активные боевые действия и где количество «ваты» значительно больше, чем «укров».

В ходе исследования, подняв данные замера соцсети «ВКонтакте» от 18 апреля, было сравнено, сколько бывших евромайдановцев и антимайдановцев перекочевало в «укров» и «ватников». Прогнозируемо большинство приверженцев Евромайдана перешли в сообщества, которые придерживаются проукраинских взглядов, а большинство антимайдановцев перешли в сообщества, которые занимают пророссийскую позицию. Но при этом не наблюдается 100-процентный переход пользователей. Это значит, что существует так называемая группа сомневающихся, либо интернет-пользователи просто изменили свое мнение. Вероятно, также появился некоторый процент активных жителей соцсети, которые просто прекратили проявлять свою гражданскую позицию с помощью участия в тех или иных сообществах.

На сегодняшний день в интернет-сообществе, представленном в украинском сегменте соцсети «ВКонтакте», большая часть пользователей занимает проукраинскую позицию. Вместе с тем в восточных и южных областях, как и раньше, заметно количество пользователей с другой точкой зрения.

Это исследование осуществлено в рамках проекта мониторинга информационных технологий MediaTransparency, который реализует Центр медиа-коммуникаций «Новая Украина» в партнерстве с интернет-изданием «Телекритика» ***(«Укры» против «ваты»: составлена карта симпатий интернет-пользователей страны // IT Expert (http://itexpert.org.ua/rubrikator/item/37827-ukry-protiv-vaty-sostavlena-karta-simpatij-internet-polzovatelej-strany.html). – 2014. – 27.08).***

***

В среднем почти 25 % молодых водителей из стран Евросоюза пользуются социальными сетями и делают автопортретные фотографии-селфи за рулём.

Во время исследования, заказанного автоконцерном Ford, удалось установить, что многие из водителей, управляя машиной, не только читают сообщения в социальных сетях, но и сами себя фотографируют за рулём.

Было опрошено 7 тыс. водителей в возрасте 18–24 лет, владеющих смартфонами. Как выяснилось, Германия занимает первое место по количеству водителей, позволяющих себе за рулём отвлекаться на социальные сети (35 %).

Далее следуют Великобритания (32 %), Бельгия (26 %), Румыния (25 %), Франция (23 %), Италия (21 %) и Испания (8 %).

Каждая фотография отвлекает водителя в среднем на 14 с, а беглый просмотр новых сообщений в лентах социальных сетей – на 20 с. При скорости в 100 км/час за это время машина проделывает путь, равный длине пяти футбольных полей.

В случае аварии такие драйв-селфи становятся последними снимками в жизни самих фотографов, а кроме того, могут привести к гибели других участников дорожного движения ***(Социальные сети стали угрозой безопасности дорожного движения // Блог Imena.UA (http://www.imena.ua/blog/drivers-take-selfies-while-driving). – 2014. – 2.09).***

Маніпулятивні технології

РФ использует соцсети для распространения неправдивой информации.

Российские спецслужбы через соцсети, электронную почту и смс-сообщения распространяют неправдивую информацию, чтобы посеять панику среди украинцев и дестабилизировать ситуацию. Об этом заявил председатель СБУ В. Наливайченко по результатам экстренного заседания СНБО под председательством Президента, передает «Укринформ».

«Восемнадцатый специальный центр Федеральной службы безопасности РФ в социальных сетях, через электронную почту и смс-сообщения, через Facebook целеустремленно трое суток рассылает тексты панического характера с целью спровоцировать панику», – отметил руководитель спецслужбы. В. Наливайченко подчеркнул, что неоднократно украинская сторона связывалась с руководством и администраторами Facebook, который используют россияне для распространения неправдивой информации, однако результатов это не дало.

В то же время, по его словам, правительство Украины завершило переговоры с Google относительно предотвращения блокирования Россией канала YouTube и других ресурсов, где выкладывается правдивая информация о ситуации в Украине ***(Украина попросила Google не***

блокировать сайты по требованию России // InternetUA (http://internetua.com/ukraina-poprosila-Google-ne-blokirovat-saiti-po-trebovaniua-rossii). – 2014. – 29.08).

***

Россия начала активно пытаться создавать поводы для дискредитации международного канала Ukraine Today. На Youtube и Facebook появились фейковые страницы, брендированные логотипом канала, с провокационным антиукраинским содержанием на русском языке, пишет Marketing Media Review (http://mmr.ua/news/id/rossija-pytaetsja-diskreditirovat-mezhdunarododnyj-kanal-ukraine-today-41033).

Канал уже обратился к администрации Youtube и Facebook с требованием удалить страницы-клоны. «Мы понимаем, что такое внимание к каналу, который стартовал лишь 24 августа, со стороны России означает, что мы движемся в правильном направлении. Мы также понимаем, что победа Кремля в развязанной им информационной войне против Украины, на данный момент, является для них принципиально важной, и ни денег, ни сил они жалеть не будут. Нам важно, чтобы мир имел возможность получать правдивую информацию о том, что сейчас происходит в Украине и Восточной Европе. Такие действия русских провокаторов лишь подчеркивают, что правда на нашей стороне», – прокомментировала Т. Пушнова, генеральный продюсер Ukraine Today ***(Россия пытается дискредитировать международодный канал Ukraine Today // Marketing Media Review (http://mmr.ua/news/id/rossija-pytaetsja-diskreditirovat-mezhdunarododnyj-kanal-ukraine-today-41033). – 2014. – 1.09).***

***

Не робити перепостів інформаційних «вкидів», «порахувати до 100», перш ніж давати поради щодо військової тактики в соцмережах. Такі поради на своїй сторінці у Facebook опублікував український журналіст, гендиректор НТКУ З. Аласанія.

Він просить українських інтернет-користувачів не поширювати інформаційних «вкидів», які спрямовані на поширення страху. Пояснює також, як працює ця технологія. «Вкид складається з малої частки правди та великої частки брехні. Приманку ви заковтуєте моментально, оскільки кілька “фактів” із вкиду вам вже траплялися, і вони були правдивими. Значить, вирішує ваша підсвідомість, решта також правда», – пише З. Аласанія.

Він також наводить іншу технологію «інформаційної диверсії». Вона полягає в тому, що неправдива інформація поширюється від імені «знайомого мого знайомого, бійця із зони АТО» або ж з «особистого листування». «І кошмар пробирається до вас у душу та розум», – пише З. Аласанія. Він також пояснює, що, намагаючись позбутися страху, людина ділиться ним у соцмережах. Натомість маси людей, аби скинути напруження, розпочинають протести, на що і розраховує ворог, вважає журналіст.

Ще одна проблема, на яку він звертає увагу, це – надмірна стурбованість воєнною тактикою волонтерів-нефахівців. З. Аласанія радить добре подумати, порахувати до 10 чи 100, прийняти холодний душ – лише не підходити до комп'ютера й не поширювати паніки в Інтернеті. Через кілька годин ситуація може кардинально змінитися, і «крик» у соцмережах виявиться абсолютно неактуальним, наголошує він і радить кожному займатися своєю справою ***(Зураб Аласанія радить не реагувати на інформаційні «вкиди» у соцмережах // MediaSapiens (http://osvita.mediasapiens.ua/material/34107). – 2014. – 29.08).***

***

«Исламское государство», джихадистское военизированное движение, захватывающее все новые территории в Сирии и Ираке, открыло несколько аккаунтов в российской социальной сети "ВКонтакте", после того как Twitter и другие мировые соцсети наложили запрет на странички боевиков», сообщает cybersecurity.ru.

Официальный аккаунт «Исламского государства» существовал на серверах vk.com и раньше, в настоящее время добавились странички пресс-служб двух основных отделений движения в Сирии и Ираке.

На просьбу ИТАР-ТАСС прокомментировать эту информацию пресс-секретарь «ВКонтакте» Г. Лобушкин сообщил, что соцсеть блокирует страницы террористической организации «Исламское государство» или любой другой организации, если в них обнаруживается противоправный контент, по заявлениям пользователей или органов власти. «Пока могу сказать, что к нам официальных обращений не поступало», – приводит ИТАР-ТАСС слова пресс-секретаря.

Ранее Twitter заблокировал аккаунты джихадистов, они попытались распространять информацию через другие крупные соцсети, но и там быстро попали под запрет. Исключением оставалась соцсеть Diaspora, однако и она на прошлой неделе ввела санкции против «Исламского государства».

Twitter также блокирует аккаунты самых активных сторонников «Исламского государства».

Присутствие официального представительства движения в мировых соцсетях важно экстремистам, чтобы распространять информацию из первых рук среди своих последователей и симпатизантов по всему миру. Главной целью «Исламского государства» является завоевание мирового господства и повсеместное установление строгих законов шариата.

Большая часть сообщений исламистов посвящена их успехам на фронтах в Сирии и Ираке, боевики публикуют также фотографии массовых казней и изображения тел убитых. По некоторым данным, идея использовать российскую соцсеть была подсказана руководству «Исламского государства» одним из их сторонников в Европе или США: он указывал на то, что «ВКонтакте» редко удаляет материалы со страниц пользователей и закрывает глаза на нарушение авторских прав ***(«Исламское государство» перешло во***

«ВКонтакте» // Медіа-бізнес (http://www.mediabusiness.com.ua/content/view/40437/126/lang,ru). – 2014. – 27.08).

***

Нещодавно в соцмережі Facebook кіровоградці почали тривожитися. Виявляється, у російській соцмережі «ВКонтакте» є група «Кіровоградська народна республіка».

У групі все як має бути: оди В. Путіну, ретрансляції «лідерів Новоросії» і т. п.

Чисельність групи невелика – 153 людини. З них більшість не з Кіровограда, а з Росії. Кількох нечисленних кіровоградців представляють боти (особи, у яких лише кілька друзів і лише один-два записи, акаунт створений навесні), люди, які активно підтримують українську армію (очевидно, від початку група була на кшталт «Котики Кіровограда», а потім її перейменували, змінили наповнення, а учасники й не знають, що в ній зареєстровані).

Проте група регулярно оновлюється. Тож адміністратори її цілком реальні люди ***(В соцмережі є група «Кіровоградської народної республіки» // Гречка (http://gre4ka.info/suspilstvo/12743-v-sotsmerezhi-ie-hrupa-kirovohradskoi-narodnoi-respubliky-foto). – 2014. – 1.09).***

***

Как Twitter используется для информационных войн

С того дня, как в середине «нулевых» самолёт приземлился на воды американского залива и трансляция эвакуации и всех происходивших событий взорвала сервис микроблогов Twitter, прошло уже более пяти лет. Сервис с синей птицей на логотипе долгое время был инструментом оперативного оповещения о резонансных событиях. Но в последнее время он чаще становится инструментом нагнетания паники и ведения информационной войны, чем полезным вспомогательным средством для гражданской журналистики, пишет Marketing Media Review (http://mmr.ua/news/id/sinjaja-ptica-isteriki-kak-twitter-ispolzuetsja-dlja-informacionnyh-vojn-41054).

Хэштег – добро и зло

Практически к любой прямой трансляции с места событий или тематической серии публикаций в микроблогах принято добавлять метки – хэштеги. Иногда о них договариваются заранее, иногда они возникают спонтанно: пресловутый коллективный разум сам вырабатывает наиболее подходящие сокращения, которые после знака «#» помогают маркировать посты от разных пользователей на одну и ту же тему.

Во времена событий, получивших название «революция достоинства» в Украине, тематические хэштеги #Euromaidan, #pray4ukraine и #maidan помогали гражданским активистам и СМИ отметить новости, публикации и

прямые трансляции с места событий, связанные с происходившим в Киеве на майдане Независимости. Эти же теги использовались для освещения гражданских протестов против Президента и правительства в разных украинских городах. В настоящее время популярным стал хэштег, связанный с военным вторжением российских войск в Луганскую и Донецкую области Украины.

Вне политической повестки дня хэштеги применяют различные гражданские и общественные инициативы: кто-то собирает на экипировку и обмундирование для армии и милиции в зоне проведения антитеррористической операции на Востоке Украины (как в случае с тегом #народныйбатальон), кто-то на благотворительные цели (таким стал тег #облийсядляжиття – украинская адаптация Ice Bucket Challenge под руководством инициативной группы «Таблеточки», помогающей онкобольным детям в Охматдет).

Однако, помимо положительного эффекта, хэштеги используются политическими партиями и связанными с ними структурами для «нагнетания» определённой общественной и эмоциональной повестки в информационном пространстве. После зимних гражданских протестов уровень использования микроблогов в роли источника информации существенно возрос. Ситуацию используют не только те, кто пытается помочь стабилизации обстановки в обществе и защите территориальной целостности страны, но и те, кто по своим личным или «общепартийным» причинам не против «раскачивания» происходящего.

Мотивация якобы проста, понятна и даже благородна: показать возникшие трудности в обществе или нестандартную, опасную ситуацию, сконцентрировать большое количество записей с одним и тем же тегом за короткий промежуток времени и вывести заданную тему «в топ». Попадание в тренды Twitter гарантирует привлечение к проблеме внимания новостных агрегаторов, крупных СМИ и западных блогеров.

Наиболее простая (хотя и затратная) тактика – использовать сеть из недавно зарегистрированных и относительно «старых» ботов (которых можно купить целыми тысячами штук за небольшие деньги), поддерживать их активность на нужном уровне достаточное время, чтобы хэштег вышел «в топ». Дальше собирать трафик и запросы по тем ссылкам, которые начинают «вбрасываться» по хэштегу.

Есть тактика и более изощрённая, основанная на понимании особенностей психологии целевой аудитории. Twitter благодаря мобильному приложению, краткости и простоте использования полюбился молодёжи, которая легко подхватывает информационный резонанс. Надавить на нужные эмоции (паника, страх, гнев, возмущение), добавить в материалы с целевым хэштегом больше провокационных фото- или видеоматериалов – и пользователи от 16 до 26 лет сами подхватят нужный хэштег и начнут выводить его в тренды, даже обгоняя ботов по скорости и качеству «выполнения работы».

Информация или имитация?

Есть несколько признаков, которые помогут «старожилу» Twitter отделить явные информационные вбросы или специально раскручиваемый хэштег от незаангажированной реальности. Поскольку за прошедшие пару лет аудитория микроблогов существенно «помолодела» и пополнилась новыми пользователями, не лишним будет напомнить об этих правилах идентификации информации.

Полезная и достоверная информация всегда:

– подкреплена точными ссылками на первоисточник или свидетелей;

– сопровождается фото, видео, документами или иными материалами с места событий;

– содержит чёткую структуру и отсылку к событиям, которые предшествовали освещаемому инфоповоду, либо наступят после него;

– дублируется в нескольких авторитетных источниках, а не только в социальных сетях или в микроблогах обычных, неверифицированных пользователей Twitter;

– подтверждается прямыми включениями или онлайн-репортажами с места происшествия или возникшей ситуации.

Имитация информации или целевой информационный вброс, как правило:

– не содержит видео-, фото- или иных доказательств происходившего (или происходящего в данный момент);

– оперирует большим количеством эмоционально окрашенной лексики для привлечения дополнительного внимания к «инфоповоду»;

– не подтверждается в независимых источниках (сообщения информационных агентств, крупных СМИ, блогов, авторитетных периодических изданий и телеканалов);

– дублируется в огромном количестве микроблогов и блогов, созданных за дни, а то и за часы до конкретного «инфоповода»;

– не имеет отсылки к другим, ранее происшедшим событиям или тем, что ожидаются после.

Как работает технология информационной манипуляции

Чтобы создать панику на любом массовом мероприятии достаточно двум-трём людям начать внезапно бежать и толкаться в густой толпе. Через пару минут побегут десять, потом – несколько десятков, а через 5–10 мин у вас будет малоуправляемая толпа, которая куда-то бежит, затаптывая на своём пути тех, кто попытается её остановить. Причина бегства может быть какой угодно; крик вроде «бомба» или «у него пистолет» – вообще идеальный рецепт для желающих создать панику, хаос и может привести к жертвам в месте массового скопления людей. Технология «посева» нужной информации и эмоционального фона работает аналогично.

Информационная манипуляция в украинском сегменте Twitter сейчас практически вся строится на нескольких тематических направлениях: события в так называемой «зоне АТО», борьба с коррупцией и действия

центральных органов власти. В случае каждого из тематических направлений используются схожие механики как «чёрного», так и «белого» пиара (слаженность и одновременное появление подобных материалов в разных соцсетях, а не только в микроблогах, косвенно указывает на организованный характер информационного вброса и то, что делом занимаются не кустари-одиночки, а люди с хорошим знанием психологии интернет-пользователей).

Сначала появляется один или два «резонансных» скриншота с какими-то данными (как правило, не подтверждёнными ни фото, ни видео, ни документальными свидетельствами) о потерях, жертвах, «распятых мальчиках» или боевых шагающих экскаваторах «уже в 100 км от Киева». Иногда информационная манипуляция заходит несколько дальше и использует механизм публикации «открытого письма», в котором компания-подписант предстаёт едва ли не «безвинным барашком», а вот структура, пришедшая с иском или служебной проверкой, – исчадием ада и символом коррупции и вседозволенности (недавно подобное можно было наблюдать на примере крупного алкогольного ритейлера). Как правило, информация подаётся субъективно и без предоставления публичной доказательной базы. Но это и не нужно: текст составлен таким образом, что «наживка» будет проглочена целевой аудиторией.

Целевая аудитория у таких «разоблачающих» твитов одна – интернет-пользователи уже в шутку окрестили этих людей «диванной сотней», а в англоязычном сегменте Интернета их называют Facebook Warrior. Это люди, готовые на борьбу со всеми несправедливостями мира, но лишь в рамках уютного дивана и собственного профиля в социальных сетях. Возможно, сортировать мусор, красить скамейки или парковать машину по правилам они не станут никогда, зато точно знают, как распределять бюджет, куда надо тратить деньги налогоплательщиков, как управлять армией и что делать с экономикой и курсом доллара.

Отличительная черта «фейсбуковоина» – возраст и социальный статус: подавляющее большинство из них не являются финансово самостоятельными и моложе 30 лет. Явление это характерно не только для Украины или соседних стран. В англоязычном сегменте соцсетей царит примерно такой же наплыв «воинства», только в качестве предмета для бесконечных споров они чаще выбирают феминизм и права женщин, регулирование рынка лекарств и оружия, события поп-культуры, военный конфликт на Ближнем Востоке, вопросы легализации ЛГБТ и тому подобные «щекотливые» темы.

Задача бота или группы пользователей – «скормить» пост-наживку людям из этой целевой группы. Дальше она начнёт передаваться по «сарафанному радио», обрастать эмоциональными комментариями и окраской, дополняться новыми «подробностями». И через каких-то пару часов уже тысячи пользователей будут клеймить правительство за бездействие, требовать отставки генералов, жаждать крови врага или проклинать жителей определённого региона.

Технология информационной манипуляции при помощи микроблогов и соцсетей «на отлично» отработала весной и в начале лета 2014 г. – как в проукраинской, так и в антиукраинской пропаганде: жители уже освобождённых городов на Востоке Украины и мигранты из оккупированного Крыма при первом контакте с украинскими военными, пограничниками и милиционерами были уверены, что континентальная часть страны захвачена некими военизированными формированиями нацистского толка, совершающими акты беспричинного насилия и издевательств по этническому и языковому признаку. В качестве «инструментов убеждения» несколько месяцев подряд в тематических группах, онлайн-сообществах и в микроблогах использовались фотоколлажи, демотиваторы, ссылки на «достоверные фото» с эмоциональными призывами и страшными историями о «хунте». Многократно повторяемые в Twitter, для своей целевой аудитории они превратились фактически в свершившийся факт.

Вторая волна информационной манипуляции, направленная на расшатывание обстановки в обществе, наблюдается с середины лета 2014 г. под кодовой фразой «нас сливают». Именно она чаще всего используется во многочисленных скриншотах постов из соцсетей, которые регулярно публикуются в Twitter. Текст постов, как правило, очень похож и содержит резонансные разоблачения «знакомого, который говорил с другом, который сейчас в зоне АТО» или «позвонил друг брата соседа, в Донецкой области…» – и дальше идёт поток из громких и эмоциональных заявлений о том, что предательство/подкуп/ложь/дефицит оружия/отсутствие приказа приводит к потере территории/независимости/жизней/будущего (подставить нужную комбинацию можете самостоятельно). Доказательств никто не требует, потому что «якорные» формулировки и эмоциональные акценты увлекают неподготовленного читателя – и разбираться уже некогда и незачем.

140 символов – не причина для паники

Информация в Twitter, не опубликованная крупными онлайн-изданиями или новостными агентствами, которым можно доверять (уровня Interfax или AP), всегда требует тщательной проверки. Бот или малоизвестный пользователь без исходных данных о себе – вряд ли достоверный источник информации. Попробуйте начать с нескольких простых действий, прежде чем поддаваться всеобщей информационной истерии.

Проверьте, кто источник и какие у него доказательства. Потребуйте больше информации по тем утверждениям, которые озвучивает тот или иной пользователь.

Задавайте наводящие вопросы. Диалог поможет вам понять, имеете ли вы дело с ботом или с реальным очевидцем событий.

Попробуйте найти ту же информацию через поиск в Google и других поисковиках. Если событие и, правда, произошло, должны быть фото, видео, комментарии, посты с геолокацией; короткие заметки в СМИ и данные от новостных агентств.

Используйте анализ не только постов и реплаев в микроблогах, но и другие социальные сети. Facebook, Instagram, «ВКонтакте» – информация там расходится достаточно быстро.

Сопоставьте по хэштегу источники информации, частоту твитов, страну, которая указана в профиле большинства пользователей или ботов, пишущих с данным хэштегом.

Любую информацию, прочитанную в Интернете (даже если она наполнена достаточной доказательной базой), стоит «делить на два»: эмоциональный компонент и субъективная оценка ситуации никогда не могут быть исключены полностью ***(Синяя птица истерики: как Twitter используется для информационных войн // Marketing Media Review (http://mmr.ua/news/id/sinjaja-ptica-isteriki-kak-twitter-ispolzuetsja-dlja-informacionnyh-vojn-41054). – 2014. – 2.09).***

***

В фотосервисе Instagram появились фейковые аккаунты, полностью копирующие профили реально существующих пользователей. Внимание на новый вид ботов в соцсети обратил редактор интернет-издания The Verge К. Мазза, сам ставший их жертвой.

По словам журналиста, о том, что в Instagram существует его бот-двойник, он узнал от друзей, которые начали спрашивать, не завёл ли К. Мазза себе второй аккаунт.

Оказалось, знакомые редактора стали получать странные уведомления о том, что он якобы отмечает их на фотографиях и в подписях к снимкам. При этом приходили такие уведомления не с его привычного, а другого, нового профиля, полностью копирующего старую страницу.

Вскоре такие же уведомления стали получать и знакомые невесты К. Маззы. Её аккаунт также оказался полностью скопирован ботом – от аватара до самих фотографий и комментариев к ним.

Чем именно руководствуются и какую цель преследуют создатели аккаунтов-двойников, неизвестно. В фейковых инстаграмах не появляются ни спам-фотографии с предложениями выиграть деньги, ни обычные для спамеров снимки с множеством хэштегов. Профили вообще не отличаются от оригинала и просто полностью его копируют.

Исследователь и специалист по кибербезопасности в компании Symantec С. Наранг считает, что боты-двойники могут быть частью существующего в Instagram подпольного рынка по продаже подписчиков и накрутке лайков. «Подобная техника используется, к примеру, в Twitter, где можно за 3 дол. купить от 100 до 1 тыс. подписчиков в зависимости от того, у кого вы покупаете. Такой накруткой в основном пользуются неизвестные фотографы, блогеры или SMM-щики, желающие таким образом показать, что у них большая аудитория», – рассказал С. Наранг.

На полное копирование своих страниц в Instagram жалуются и другие пользователи сервиса, также не понимающие, зачем кому-то нужно просто полностью дублировать всю их информацию и фотографии.

По просьбе редактора The Verge двойники его аккаунта и аккаунта его невесты были удалены из Instagram. Для этого требуется подтвердить свою личность, прислав администрации сервиса копию документов (паспорта или любого другого удостоверения с фотографией) ***(Журналисты обнаружили в Instagram сеть полностью копирующих живых пользователей ботов // InternetUA (http://internetua.com/jurnalisti-obnarujili-v-Instagram-set-polnostua-kopiruuasxih-jivih-polzovatelei-botov). – 2014. – 4.09).***

***

Информация негативного характера, которая распространяется в социальных сетях, часто является «информационным оружием против Украины», заявляет эксперт по вопросам безопасности Ю. Костюченко, передает радио «Свобода».

«От 20 до 45 % информации, которая распространяется в нашем информационном поле, имеет признаки целенаправленной внешней манипуляции и является, по сути, информационным оружием, направленным против нашего государства», – заверил он.

По словам Ю. Костюченко, исследования американских ученых показали, что доля «полностью вымышленных» историй и сообщений в период активизации украинского кризиса может достигать 75 %. Так называемые «ссылки на источники» и «жизненные истории» являются ложными и распространяются с целью запугать и дезориентировать людей.

Признаком таких сообщений является «удар по эмоциям», навязывания определенного мнения и повторение. «На личном уровне мы можем защитить себя и свое окружение от вредного воздействия вражеской пропаганды средствами “интеллектуальной гигиены”. Можно, конечно, попытаться дистанцироваться, но нельзя быть свободным от системного воздействия. Наиболее надежными методами защиты здесь является толерантность и умение думать. Догматизм, ограниченность, радикальность и агрессия делают человека уязвимым к манипуляциям», – отмечает эксперт.

Он советует сохранять спокойствие и критически относиться к информации ***(До 45 % сообщений в соцсетях является информационным оружием против Украины // InternetUA (http://internetua.com/do-45--soobsxenii-v-socsetyah-yavlyaetsya-informacionnim-orujiem-protiv-ukraini---ekspert). – 2014. – 7.09).***

Зарубіжні спецслужби і технології «соціального контролю»

Разработчики систем наблюдения сулят правительствам возможность отслеживать передвижения чуть ли не любого человека, который носит при себе мобильный телефон, утверждает The Washington Post. «И неважно, где находится этот человек – на расстоянии пары кварталов или на другом континенте», – добавляет журналист К. Тимберг, информирует news.eizvestia.com.

Технология эксплуатирует тот факт, что сетям сотовой связи необходимо внимательно отслеживать местоположение своих клиентов, чтобы оказывать им услуги связи. «Системы наблюдения тайно собирают эти сведения о местоположении, чтобы отслеживать передвижения людей на протяжении нескольких дней, нескольких недель или еще дольше», – пишет газета, ссылаясь на документы компаний и слова экспертов.

Самые могущественные разведки мира вроде американской АНБ и британского Центра правительственной связи давно пользуются данными с сотовых телефонов. «Но эксперты говорят, что новые системы позволяют не столь технически продвинутым правительствам следить за людьми в любой стране, включая США, с относительной легкостью и точностью», – пишет газета.

Как пользоваться технологией? «Номер телефона вводится на неком компьютерном портале, а он получает информацию из баз данных о местоположении, которые создаются операторами мобильной связи», – сообщает автор, ссылаясь на документы частных компаний. Система определяет, какую вышку сотовой связи сейчас использует клиент, и устанавливает его местонахождение с точностью до «нескольких кварталов», по выражению газеты, в городе и до нескольких миль – в сельской местности.

Газете неизвестно, правительства каких стран приобрели эти системы слежения. Но некий представитель индустрии сообщил на условиях анонимности, что в последние годы эта техника была приобретена или арендована десятками стран. «Любой мелкий диктатор, если у него хватит денег на покупку системы, мог бы шпионить за людьми в любой точке планеты», – заметил Э. Кинг, замдиректора организации Privacy International, которая остерегает от злоупотребления технологиями слежки.

Эксперты отмечают, что такими технологиями также могут воспользоваться хакеры и криминальные группировки, а также страны, против которых введены санкции. «Технологии действуют в “серой зоне” в правовом смысле. Во многих странах слежка без согласия объекта или ордера суда противозаконна, но в международном праве нет четкого стандарта относительно тайной слежки за людьми в других странах. Не существует и глобальной организации, которая была бы уполномочена выявлять потенциальные злоупотребления», – говорится в статье.

Отслеживание местоположения – все более обычное явление в современной жизни. При желании пользователь обычно может отключить эту функцию на своем мобильном устройстве. Однако системы, сконструированные для разведслужб и полиции, заблокировать трудно или даже невозможно. Частные компании предлагают ведомствам несколько разных технологий. «Одни улавливают сигналы сотовой связи с телефонов неподалеку, другие используют вредоносное ПО, чтобы “обмануть” телефон, принудив выдать его местонахождение», – пишет автор.

По данным газеты, системы, которые подключаются к базам данных, «позволяют правительству практически любой страны следить за людьми за границей, при помощи сотового телефона любого типа, через самых разных мобильных операторов, причем вообще без ведома самих операторов». Системы также могут быть использованы вместе с другими технологиями, которые перехватывают звонки и интернет-трафик, включают микрофоны мобильных устройств и получают доступ к спискам контактов, фотографиям и другим документам.

В распоряжении газеты оказались рекламные материалы нескольких производителей. Например, в рекламной брошюре системы SkyLock, которой торгует американский производитель Verint, говорится, что система предлагает ведомствам «рентабельный новый способ получать глобальную информацию о местоположении известных объектов (слежки. – Ред.)». В брошюре есть скриншоты карт, отражающих слежку, «как представляется, в Мексике, Нигерии, Южной Африке, Бразилии, Конго, ОАЭ, Зимбабве и еще нескольких странах».

В брошюре сказано, что Verint не применяет SkyLock против «телефонов в США или Израиле» (формулировка издания). «Но несколько похожих систем, которые в последние годы продавали компании, зарегистрированные в Швейцарии, Украине и в других странах, наверняка свободны от подобных ограничений», – комментирует газета.

Технология отслеживания пользуется недостатками в защите глобальной сети SS7, которой мобильные операторы пользуются для связи между собой при перенаправлении звонков, sms и интернет-данных. По словам экспертов, защита от несанкционированного доступа к сети слаба и обойти ее легко. «Компании, которые торгуют системами отслеживания через SS7, советуют применять их в тандеме с так называемыми IMSI catchers – все более распространенными шпионскими устройствами, которые ловят сигналы сотовых телефонов прямо из эфира, чтобы перехватывать звонки и интернет-трафик, отсылать фальшивые sms, устанавливать на телефон шпионские программы и определять точное местонахождение», – пишет газета.

IMSI catchers бесполезны, если приблизительное местонахождение объекта неизвестно. Системы, использующие SS7, решают эту проблему ***(Уже продаются системы для отслеживания передвижения пользователей мобильных телефонов // InternetUA***

(http://internetua.com/uje-prodauatsya-sistemi-dlya-otslejivaniya-peredvijeniya-polzovatelei-mobilnih-telefonov). – 2014. – 26.08).

***

Агентство национальной безопасности (АНБ) США разработало собственную поисковую систему наподобие Google.com, к которой имеют доступ более двух десятков силовых струтур, включая ФБР, ЦРУ и Управление по борьбе с наркотиками. Об этом сообщило издание The Intercept со ссылкой на новые секретные документы, обнародованные Э. Сноуденом.

Новость была упомянута в Twitter министром связи и массовых коммуникаций РФ Н. Никифоровым. «АНБ/NSA США разработало поисковик для ваших незаконно перехваченных и сохраненных телефонных переговоров, смс, e-mail», – прокомментировал он.

База данных поисковой системы ICREACH содержит миллиарды записей метаданных, касающихся частных сеансов связи иностранных граждан и миллионы записей, касающихся граждан США, к которым не были предъявлены какие-либо обвинения.

Метаданные, к которым поисковая система дает доступ, включают номера телефонов, уникальные номера SIM-карт, адреса электронной почты и др. Эта информация может быть использована для отслеживания перемещений людей, составления списка их друзей, родственников и знакомых, предсказания последующих действий, выяснения религиозной принадлежности и политических предпочтений.

Используя специальные указатели, пользователи системы могли искать информацию, связанную с определенными людьми. Например, список телефонных номеров, по которым определенный человек звонил за последний месяц. Система обладает максимально простым интерфейсом с поисковой строкой и выдает результаты на отдельной странице.

В одном из документов говорится, что работа над системой ICREACH началась в 2005 г. и была обусловлена необходимостью разведывательного сообщества иметь доступ к метаданным и способностью АНБ собирать такие данные в больших объемах.

Тестовый запуск состоялся в 2007 г. под руководством бывшего директора АНБ К. Александера. Ежегодный бюджет на содержание был определен в интервале 2,5–4,5 млн дол. Когда система заработала в полную силу, неизвестно. Но предполагается, что в конечном счете АНБ удалось перевыполнить план и собрать свыше 850 млрд записей метаданных, о которых говорилось изначально. В отчете за 2010 г. сообщалось, что ICREACH стала основным инструментам для обмена данными среди спецслужб.

Как пишет The Intercept, новые обнародованные документы впервые доказывают, что АНБ в течение многих лет предоставляла прямой доступ к секретным данным различным силовым структурам.

Помимо силовых структур США, доступ к ICREACH имели страны-партнеры, входящие в группу Five Eyes: Канада, Великобритания, Новая Зеландия и Австралия.

По мнению экспертов, опрошенных The Intercept, система ICREACH могла быть использована силовыми структурами США для слежки за подозреваемыми без разрешения суда. Когда они узнавали о том, что подозреваемый действительно нарушает закон, они представляли суду другие улики. При этом реальный источник информации скрывался ***(АНБ США создало собственный «секретный Google» // InternetUA (http://internetua.com/anb-ssha-sozdalo-sobstvennii--sekretnii-Google). – 2014. – 27.08).***

***

Протягом липня – серпня цього року на Чернігівщині співробітники СБУ викрили та припинили протиправну діяльність 12 громадян України, які через мережу Інтернет поширювали матеріали антидержавного змісту.

Встановлено, що порушники, підтримуючи на власних сторінках соцмереж дії терористів на Сході України, відкрито висловлювали заклики брати зброю та вступати до бандформувань, які орудують на Луганщині та Донеччині.

Маючи на меті підбурити населення до протестів – дестабілізувати ситуацію в регіоні, зловмисники активно розповсюджували публікації, у яких висловлювали зневажливе ставлення до воїнів Збройних сил України, відверто принижували національну гідність патріотів, цинічно нав’язували думки про неспроможність української влади забезпечити обороноздатність армії.

Відповідно до ст. 109–110 Кримінального кодексу України цим громадянам були винесені офіційні застереження щодо недопущення протиправної діяльності, спрямованої на посягання на суверенітет, конституційний лад і територіальну цілісність держави ***(СБУ попередила 12-х // Сіверщина (http://siver.com.ua/news/sbu_poperedila_12_kh/2014-08-28-15281). – 2014. – 28.08).***

***

Видео, в котором обращаются к русским матерям от имени украинских солдатов, удаляют со всех соцсетей.

«Я украинец и я воюю за свою родину. Ты знаешь, что твой сын воюет за Януковича, за вора, который ограбил мою Украину. Ты знаешь, что твой сын оккупант и террорист. Русская мама, позвони сыну, и моли бога, чтобы я промахнулся!» – сказано в видеоролике.

Также в видео приводится обращение председателя Саратовского областного союза солдатских матерей РФ Л. Свиридовой к матерям российских солдатов, пишет obozrevatel.com.

«Игрушки закончились! Сегодня найдите своего сына в армии, убедитесь, что он служит там, куда его направили. И если вы такого подтверждения не получили, то судьба вашего сына находится только в ваших руках. Не надо потом будет пенять на власть, общественность. Сегодня вы должны забросить подальше все свои кастрюли и домашние дела и посвятить жизнь поискам своего сына в российской армии».

Как пишут пользователи соцсетей, это видео удаляют по всему Интернету ***(Скандальное обращение украинского солдата к русской матери мгновенно удаляют из соцсетей // Хартия'97 (http://www.charter97.org/ru/news/2014/8/27/113007). – 2014. – 27.08).***

***

Социальная сеть LinkedIn ранее в этом году расширила масштабы деятельности в КНР. Сейчас компания пожинает плоды китайской экспансии – LinkedIn приходится цензурировать аккаунты пользователей. Bloomberg сообщает, что когда пользователь в Китае публикует сообщение, логика которого конфликтует с официальными нормами, компания блокирует этот контент не только в КНР, но и по всему миру, пишет cybersecurity.ru.

Агентство отмечает, что с подобными нормами LinkedIn идет вразрез с официально декларируемыми компанией ценностями – защищать информацию пользователей. В самой компании говорят, что меняют систему блокировки и будут закрывать спорный контент для Китая, но оставлять его для всего мира.

«Дилемма LinkedIn подчеркивает сложности ведения бизнеса в стране с жесткими правилами цензуры. Лишь немногие американские компании добились успеха в КНР. Сервисы Facebook и Twitter вообще закрыты в этой стране», отмечает Bloomberg в авторском материале.

Как правило, LinkedIn уведомляет пользователей, когда на их страницах появляется «неприемлемый» контент, который официальный Пекин должен был бы заблокировать. Независимый журналист Р. Шмитц, публикующий материал для издания Marketplace, отмечает, что в LinkedIn среди пользователей не было вообще никаких заметок относительно годовщины событий на площади Тяньаньмень. В то же время на мировых ресурсах эта тема активно поднималась ***(LinkedIn столкнулась с китайской цензурой в сети // Media бізнес (http://www.mediabusiness.com.ua/content/view/40538/126/lang,ru/). – 2014. – 3.09).***

***

Депутат Госумы РФ Е. Федоров готовит обращение в МВД и Генеральную прокуратуру с просьбой проверить деятельность корпорации Google.

По мнению депутата, американская корпорация, заключив договор со Службой безопасности Украины, предоставляет украинским спецслужбам

персональные данные российских граждан. По словам депутата, центральный офис Google находится в юрисдикции США, которые, якобы, официально занимают позицию по ослаблению России и дестабилизации ситуации в стране.

Таким образом, деятельность Google на территории РФ является прямой угрозой, ни много ни мало, национальной безопасности всей федерации.

Кроме того, Е. Федоров считает, что поисковый гигант ведёт агитацию в пользу Украины, поместив вместо своего логотипа жёлто-голубой дудл 24 августа, в День Независимости Украины ***(Госдума России подозревает Google в шпионаже в пользу Украины // Блог Imena.UA (http://www.imena.ua/blog/rf-changes-googles-orientation). – 2014. – 4.09).***

***

Южнокорейский комитет по оценке игр приравнял онлайн-игры, в которых присутствуют микроплатежи к азартным, и заблокировал все подобные программы в социальной сети Facebook.

Такими методами комитет борется с распространением азартных игр в сети, которые стали настоящей проблемой для Южной Кореи и её граждан.

Если Facebook захочет, чтобы пользователи Южной Кореи опять смогли играть онлайн, ему придётся настоять, чтобы все разработчики игр зарегистрировались в комитете и заплатили соответствующий взнос.

Реакция представителей социальной сети на блокировку всех онлайн-игр пока что неизвестна. Очевидно, Facebook будет способствовать регистрации разработчиков своих игр, чтобы поскорее восстановить возможность играть онлайн.

Ранее стало известно, что правительство Южной Кореи серьёзно рассматривает возможность приравнивания увлечения видеоиграми к алкогольной или наркотической зависимости.

Власти Южной Кореи считают, что видеоигры слишком распространены в стране, и за этой сферой нужно следить так же, как за реализацией и употреблением гражданами крепких напитков ***(В Южной Корее заблокированы все Facebook-игры из-за их азартности // Блог Imena.UA (http://www.imena.ua/blog/ban-hammer-koreas-game-facebook/). – 2014. – 4.09).***

***

Соціальна мережа «ВКонтакте» була включена в реєстр Роскомнадзору в рамках виконання скандального «закону про блогерів», прийнятого в Росії 1 серпня.

Як повідомляє телеканал «Дождь», з відповідною заявою виступив прес-секретар Роскомнадзору В. Ампелонський. Чиновник нагадав, що закон, який прийняли 1 серпня, регулює діяльність блогерів у Росії, і «ВКонтакте» було включено до цього реєстру згідно з положеннями закону як

«організатор поширення інформації». Інтернет-майданчики з таким статусом повинні розкривати інформацію щодо відвідуваності блогерів, їх контакти, зберігати цю інформацію на російських серверах протягом півроку та ділитися даними зі спецслужбами.

Виконавчий директор «ВКонтакте» Д. Сергєєв сказав, що вони дійсно отримали таке сповіщення від Роскомнадзору. За його словами, немає нічого дивного в тому, що соцмережу визнали «поширювачем інформації», адже вона такою і є. Д. Сєргєєв повідомив, що «ВКонтакте» буде діяти винятково в інтересах користувачів і в рамках закону.

Цікаво, що наступними великими майданчиками, які можуть також включити до реєстру Роскомнадзору, стануть Яндекс, Рамблер і навіть Мамба, популярний сервіс знайомств ***(ВКонтакте почав офіційно передавати ФСБ інформацію про своїх користувачів, їх контакти та переписку // UkrainianWatcher (http://watcher.com.ua/2014/09/06/vkontakte-vklyuchyly-v-reyestr-roskomnadzora). – 2014. – 6.09).***

Проблема захисту даних. DDOS та вірусні атаки

Двое исследователей информационной безопасности из Университета Карнеги-Меллона, США, сообщили о создании программного инструмента, позволяющего предугадывать хакерские нападения и тем самым значительно повышающего уровень безопасности охраняемого веб-ресурса, передает The Daily Dot.

По словам К. Соски и Н. Кристина, разработка основана на передовых технологиях сбора и анализа информации. При этом инструмент представляет собой многофункциональный алгоритм классификации, испытания которого проводились на 444 519 веб-сайтах (4,9 млн веб-страниц), заархивированных в WayBack Machine.

В течение года тестирования инструмент предугадал 66 % всех зафиксированных нападений, а доля ложноположительных срабатываний составила всего 17 %. Н. Кристин и К. Соска уверены, что подобный уровень производительности «очень обнадеживает, поскольку позволяет практически предсказывать будущее».

«К примеру, если на определенном веб-сайте фиксируется спад посещаемости, это может свидетельствовать о том, что злоумышленники перенаправляют посетителей ресурса в рамках мошеннической кампании, – поясняют эксперты. – Эта информация способствует предотвращению аналогичных атак на другие ресурсы».

Для проведения наиболее глубокого анализа алгоритм осуществляет сбор таких данных, как версии используемого ПО, время осуществления загрузок, ссылки, активность в комментариях, CSS теги и многое другое.

В перспективе специалисты намерены развивать свой инструмент и предоставить возможность его свободного использования каждым желающим ***(Разработан инструмент информационной безопасности, позволяющий прогнозировать хакерские атаки // InternetUA (http://internetua.com/razrabotan-instrument-informacionnoi-bezopasnosti--pozvolyauasxii-prognozirovat-hakerskie-ataki). – 2014. – 26.08).***

***

Представители антивирусной компании ESET предупреждают о мошеннических операциях по отношению к пользователям App Store. Злоумышленники, маскируясь под рассылку интернет-магазина Apple получают от пользователей пароли к Apple ID.

Схема мошенников довольно незатейлива. Сперва на почтовый ящик пользователя приходит сообщение о якобы совершенной покупке игры World Of Go, по цене 9,65 евро. В письме также находится уведомление о том, что отменить покупку можно, в течение 12 часов после ее совершения, на сайте App Store, для чего следует перейти по ссылке Payment Cancellation, содержащейся в тексте сообщения. Перейдя по ссылке, пользователь оказывается на фальшивом сайте интернет-магазина, где и происходит процесс хищения ключей.

Отличить «фейковый» магазин от реального не так уж и сложно, стоит лишь присмотреться к адресной строке, у настоящего App Store адрес store.apple.com.

Представители ESET просят пользователей быть внимательными, обращать внимание на адресную строку при переходе по ссылкам и в случае возникновения любых вопросов обращаться в службу техподдержки Apple ***(Хакеры выманивают у пользователей пароли от Apple ID // InternetUA (http://internetua.com/hakeri-vimanivauat-u-polzovatelei-paroli-ot-Apple-ID). – 2014. – 26.08).***

***

Во время празднования Дня Независимости, 24 августа сайт Министерства иностранных дел был подвержен DDoS-атаке, сообщает корреспондент proIT.

«Несмотря на праздник Дня Независимости Украины, в 17:00 специалистами Cert-Ua была получена информация о фиксации, начиная с 16:00, аномальной сетевой активности в сторону веб-сайта МИД Украины, в результате чего была нарушена его доступность в сети», – сообщают представители компании «Информационный центр ElVisti».

Мощность фиксированных потоков составила более 3 Гбит/с.

Как сообщают в Cert-Ua, 90,21 % всего количества IP-адресов источников атаки принадлежат сегменту сети Интернет Китая.

Напомним, 22 августа о факте несанкционированного вмешательства в работу информационной системы МИДа сообщал на своей странице в Twitter

министр иностранных дел П. Климкин ***(Хакеры атаковали сайт МИД во время празднования Дня независимости // proIT (http://proit.com.ua/news/telecom/2014/08/26/090955.html). – 2014. – 26.08).***

***

Согласно исследованию, проведенному компанией Alert Logic, большинство кибератак, направленных на страны Западной Европы, осуществляется из России. В свою очередь, Китай стал лидером по количеству хакерских атак, нацеленных на США.

Во время исследования компания внедрила в облачную инфраструктуру приманки с низким уровнем взаимодействия, имитирующие уязвимые операционные системы.

Анализ полученных данных показал, что 40 % хакерских атак, нацеленных на пользователей, проживающих в Северноевропейских странах, осуществлялось из России. Страны Западной Европы, в основном, подвергались хакерским атакам, проведенным из Китая (32 %), США (21 %), Индии (17 %) и России (9 %). 63 % атак на страны Азиатско-Тихоокеанского региона были осуществлены из США.

По словам экспертов, наиболее частыми были случаи инфицирования вредоносной программой Conficker-A, которая похищает конфиденциальные данные пользователя. По словам специалиста Alert Logic С. Коути, эта программа до сих пор используется по ряду причин, в основном, в силу своей легкодоступности, простоты в использовании и эффективности ***(Большинство направленных на Европу кибератак осуществляется из России // InternetUA (http://internetua.com/bolshinstvo-napravlennih-na-evropu-kiberatak-osusxestvlyaetsya-iz-rossii). – 2014. – 25.08).***

***

Киберпреступники используют новое вредоносное ПО, нацеленное на похищение информации у крупнейших европейских компаний, связанных с автомобильным делом. Вредоносная кампания стартовала в начале августа текущего года, а жертвами ее были преимущественно предприятия, предлагающие услуги не только по производству машин, но также их аренде, рекламированию и т. д.

Как пишет в блоге Symantec Л. Пайет, вирус распространялся посредством фишинговых писем, якобы отправленных от имени компании Technik Automobile, о поиске для приобретения автомобилей с пробегом. В письмах содержалось вложение под названием TechnikAutomobileGMBH.pdf.zip. В нем якобы находился список машин, однако на самом деле это был троянский вирус Carbon Grabber.

Вредоносный файл шифрует исполняемый файл и внедряет код в процессы Microsoft Outlook, Internet Explorer, Google Chrome, а также Mozilla Firefox. По утверждениям ИБ-экспертов из Symantec, вирус перехватывает

API-интерфейсы браузера, благодаря чему у злоумышленников появляется доступ к информации.

В компании говорят, что функционал Carbon Grabber напоминает действие вирусов, используемых для осуществления атак «человек по середине». В частности, вредоносное ПО похищает учетные данные для входа в различные веб-сервисы, в том числе онлайн-банкинг и интернет-приложения ***(Новая фишинговая кампания нацелена на автомобильную индустрию Европы // InternetUA (http://internetua.com/novaya-fishingovaya-kampaniya-nacelena-na-avtomobilnuua-industriua-evropi). – 2014. – 26.08).***

***

Пассажирский самолет, направлявшийся из Далласа в Сан-Диего, совершил экстренную посадку по требованию ФБР после того, как в Twitter появилось сообщение о том, что в самолете заложена бомба. Об этом сообщает CBS News.

Инцидент произошел в воскресенье, 24 августа, на борту самолета «Боинг 757» авиакомпании American Airlines, выполнявшего рейс 362 со 172 пассажирами на борту. Решение об экстренном приземлении в аэропорту Финикса, штат Аризона, агенты ФБР приняли после того, как авиакомпания получила предупреждение о бомбе, отправленное хакерами с личного аккаунта в Twitter президента Sony Online Entertainment Д. Смедли, который сам летел этим рейсом.

Самолет благополучно совершил посадку. С его борта эвакуировали всех пассажиров и членов экипажа, после чего лайнер и весь багаж осмотрели полицейские. После досмотра «Боинг» продолжил полет в Сан-Диего.

О том, была ли найдена на борту бомба, ничего не сообщается. Ответственность за взлом аккаунта Д. Смедли, по информации блога газеты Dallas Morning News, взяла на себя группа хакеров, известная как Lizard Squad. Ранее эта группа заявила о причастности к взлому Sony PlayStation Network ***(В США лайнер экстренно приземлился из-за сообщения в Twitter // InternetUA (http://internetua.com/v-ssha-lainer-ekstrenno-prizemlilsya-iz-za-soobsxeniya-v-Twitter). – 2014. – 26.08).***

***

В Facebook отметили рост количества провайдеров, развертывающих шифрование с помощью STARTTLS.

95 % посылаемых Facebook по электронной почте уведомлений, являются зашифрованными. Электронные письма шифруются с помощью свойства протоколов под названием «Совершенная прямая секретность» и строгой проверки подлинности сертификата. Об этом сообщил инженер Facebook М. Эдкинс, занимающийся вопросами неприкосновенности сообщений пользователей.

В мае нынешнего года компания подсчитала количество SMTP-серверов, использующих протоколы TLS. Согласно полученным результатам, 76 % записанных в MX уникальных имен хостов, которые получают электронные письма от Facebook, поддерживают расширение STARTTLS, позволяющее создавать зашифрованное соединение поверх незашифрованного. 74 % из них также используют PFS. В общем счете, зашифрованными были 58 % уведомлений, отправляемых соцсетью по электронной почте.

«Поскольку для развертывания шифрования с помощью STARTTLS требуется участие обеих сторон, мы призывали другие компании к осуществлению следующего шага, – сообщил М. Эдкинс. – В результате последних изменений, предпринятых основными провайдерами, в особенности Microsoft и Yahoo, 95 % наших электронных уведомлений в настоящее время успешно шифруются как с помощью PFS, так и строгой проверки подлинности сертификата» ***(95 % электронных уведомлений от Facebook успешно шифруються // InternetUA (http://internetua.com/95--elektronnih-uvedomlenii-ot-Facebook-uspeshno-shifruuatsya). – 2014. – 26.08).***

***

Представители анонимной сети Tor сообщили, что спецслужбы США постоянно оказывают помощь хакерам.

Так, по данным администрации Tor, некоторые американские и британские сотрудники, занимающиеся предотвращением кибершпионажа, намеренно подрывают усилия своих коллег из Агентства национальной безопасности США и британского Центра правительственной связи.

Соответствующее заявление сделал исполнительный директор Tor Project Э. Льюман. Согласно его заявлению, представители вышеупомянутых государственных органов регулярно сообщают разработчикам секретную информацию о недостатках, которые они находят в анонимной сети. Устранение этих уязвимостей помогает успешно защищать пользователей Tor от слежки.

Ранее в анонимной сети Tor обнаружена уязвимость, позволяющая полностью деанонимизировать любого пользователя. Все детали уязвимости пока что держатся в тайне, поскольку администрация Tor ещё не устранила эту брешь.

Тем временем, в сети нашли сайт-двойник анонимной сети Tor, который распространяет вредоносное программное обеспечение и похищает пожертвования пользователей. Фальшивый пакет Tor Browser находится под управлением злоумышленников. Под видом загружаемого пакета «злой двойник» получает удалённые команды и выполняет преступные действия с данными пользователя ***(Tor получает помощь от агентов АНБ // Блог Imena.UA (http://www.imena.ua/blog/tor-получает-помощь-от-агентов-анб). – 2014. – 27.08).***

***

Как сообщают представители социальной сети Facebook, разработчики компании намерены в ближайшее время выпустить обновление безопасности для своего мобильного приложения для iOS-устройств. Речь идет об опасной уязвимости, эксплуатация которой дает возможность злоумышленникам удаленно совершать звонки со смартфонов iPhone, принадлежащих жертвам атаки. Для этого достаточно вынудить пользователя перейти по специально сформированной вредоносной ссылке.

Брешь была обнаружена исследователем А. Некулизи, по словам которого проблема заключается в реализации функционала набора номера, опубликованного на веб-странице. Последний используется смартфонами на iOS как для запуска приложений, так и для инициации набора номера.

«Когда пользователь нажимает на телефонный номер на веб-странице, iOS отображает предупреждение с просьбой указать, действительно ли пользователь намерен совершить звонок, поясняет эксперт. – Вместе с тем когда пользователь открывает телефонный номер в приложениях, iOS не отображает предупреждений и инициирует набор номера без дополнительных вопросов».

При помощи собственноручно разработанного PoC-кода исследователь доказал, что эта брешь присутствует в клиентах таких крупных служб, как Gmail, Google+, Facetime т. п. ***(Facebook готовит исправление уязвимости, заставляющей iPhone совершать звонки // InternetUA (http://internetua.com/Facebook-gotovit-ispravlenie-uyazvimosti--zastavlyauasxei-iPhone-sovershat-zvonki). – 2014. – 28.08).***

***

В акционерном обществе «Киевстар» сообщают о предотвращении крупнейшей за всю историю компании кибератаки на ее сеть, которая проходила с 11 по 25 августа.

Такую информацию распространила пресс-служба телекоммуникационного гиганта.

«В августе 2014 г. специалисты “Киевстар” выявили и предотвратили крупнейшую в истории компании телекоммуникационную атаку», – говорится в сообщении.

Отмечается, что цель действий злоумышленников состояла в том, чтобы вывести из строя центр управления сетью, заблокировать предоставление услуг для всех абонентов, а также получить доступ к номерам телефонов клиентов.

По информации «Киевстара», группа злоумышленников действовала за границей. Кибератака была направлена против GSM-оборудования оператора и 300 серверов информационных систем ***(«Киевстар» предотвратил крупнейшую кибератаку на свою сеть // InternetUA (http://internetua.com/kievstar--predotvratil-krupneishuua-kiberataku-na-svoua-set). – 2014. – 28.08).***

***

Как следует из сообщения исследователей безопасности из Trend Micro, им удалось обнаружить ряд опасных и легко эксплуатируемых уязвимостей в маршрутизаторах популярного китайского производителя Netis Systems.

Netis Systems является дочерней компанией Netcore Group, штаб-квартира которой расположена Шэньчжэне, Китай, где их продукция продается под торговой маркой Netcore. В остальных странах мира компания известна под брендом Netis. По данным экспертов, маршрутизаторы как от Netis, так и от Netcore содержат бэкдор, использование которого не составляет труда для злоумышленников.

Удаленному злоумышленнику достаточно узнать внешний IP-адрес устройства и предпринять попытку получения доступа через UDP порт 53413. Усугубляет ситуацию то, что запрашиваемый при этой процедуре пароль по умолчанию является одинаковым на всех моделях маршрутизаторов и не может быть изменен.

По словам исследователя Trend Micro Т. Еа, при помощи сетевого сканера ZMap ему удалось обнаружить порядка двух миллионов подключенных к сети уязвимых устройств. Вместе с тем подавляющее большинство этих устройств находилось в Китае ***(В маршрутизаторах Netis Systems обнаружены легко эксплуатируемые уязвимости // InternetUA (http://internetua.com/v-marshrutizatorah-Netis-Systems-obnarujeni-legko-ekspluatiruemie-uyazvimosti). – 2014. – 28.08).***

***

Twitter разработал и построил систему борьбы со спамом BotMaker. Система уже обрабатывает миллиарды событий ежедневно, благодаря чему с момента запуска ключевые показатели спама снизились на 40 %.

Целью любой анти-спам системы является уменьшение количества видимого спама и отсутствие ложных срабатываний. Спам в Twitter отличается от традиционного спама в других системах: для легкого взаимодействия с платформой Twitter предоставляет разработчикам API, а контент публикуется в режиме реального времени. Это означает, что спамеры узнают почти все системы анти-спама Twitter через API. Кроме того, анти-спам системы должны избегать задержки в видимых пользователю операциях. В более традиционных системах, например, в электронной почте, задержка на десятки секунд остается незамеченной.

Три ключевых принципа Botmaker:

– предотвращение создания спама. Усложнение создания спама приводит к уменьшению его видимого количества;

– уменьшение времени, в течение которого спам виден на Twitter;

– сокращение времени реакции на новые спам-атаки.

Для достижения этих целей BotMaker получает информацию о событиях от распределенных систем в Twitter, проверяет данные в соответствии с набором правил, а затем применяет предусмотренные действия.

Правила BotMaker, называемые ботами, разделяются на две части: условия для принятия решения о реакции на события, а также действия, которые следует предпринять в связи с этим событием.

Для того чтобы систему борьбы со спамом могли преодолеть основные записи Twitter (твиты, ретвиты, избранное и подписки), система поддерживает правила, основанные на машинном обучении. Кроме того, инженеры Twitter имеют возможность мгновенно изменять и создавать новые правила.

BotMaker также значительно снижает время реакции на спам-атаки. До появления системы на внесение изменений требовалось несколько часов или дней, теперь процесс занимает считанные минуты.

Разработчики BotMaker после его запуска увидели снижение характеристик отслеживания спама на 40 %.

BotMaker уже используется в Twitter как главный двигатель борьбы со спамом. Кроме того, принципы функционирования BotMaker могут помочь в разработке и реализации систем, отвечающих за управление, поддержку и защиту распределенных систем ***(BotMaker защищает Twitter от спама // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/botmaker_zaschischaet_twitter_ot_spama). – 2014. – 28.08).***

***

Специалисты уполномоченного подразделения Госспецсвязи (CERT-UA) совместно с ООО «Адамант» распознали характер хакерской атаки на сайт Кабинета Министров, состоявшейся 27 августа, сообщает «корреспондент proIT».

В рамках проверки информации уполномоченным подразделением Госспецсвязи (CERT-UA) совместно со специалистами ООО «Адамант» была зафиксирована аномальная активность, направленная на сетевой порт 80/tcp сайта kmu.gov.ua., которая имеет признаки DDoS-атаки типа TCP SYN-flood, сообщили в CERT-UA.

«В случае с этой DDoS-атакой злоумышленники, использовали бот-сети, позволяющие генерировать большое количество запросов в секунду, что заставило сервер открывать соединения и держать их в таком состоянии в течение определенного промежутка времени, что привело к исчерпанию его вычислительного ресурса», – проинформировали специалисты Госспецсвязи.

Сообщается также, что около 10:00 злоумышленники, увидев неэффективность своей атаки, что проявлялось в доступности сайта kmu.gov.ua, приняли меры по частичному удалению «характерного признака» из запросов, которые генерировали боты. После этого, с целью

обеспечения доступности веб-сайта ведомства, были приняты меры по блокированию доступа к объекту атаки с некоторых автономных систем.

В результате проверки было выяснено, что все IP-адреса, с которых осуществлялась атака, были поддельными.

Напомним, утром 27 августа была получена информация о проблемах с доступностью сайта Кабинета Министров Украины, а также нескольких других веб-сайтов, размещенных на едином веб-портале органов исполнительной власти ***(Госспецсвязи отчиталась о ликвидации DDoS-атаки на сайт Кабмина // proIT (http://proit.com.ua/news/gosregulation/2014/08/29/094702.html). – 2014. – 29.08).***

***

Во II квартале текущего года увеличилось количество фишинговых атак на веб-сайты платежных систем и на сервисы, позволяющие зарабатывать криптовалюту.

Согласно исследованию, проведенному компанией APWG, количество фишинговых атак во II квартале текущего года значительно увеличилось по сравнению с данными 2008 г.

Специалисты APWG выяснили, что в среднем в каждом месяце II квартала злоумышленники совершали более 42 тыс. фишинговых атак. При этом количество жертв кибермошенников сократилось на 17 % по сравнению с аналогичным периодом 2013 г. (с 639 до 531).

По данным экспертов, чаще всего фишинговым атакам подвергались недавно появившиеся платежные сервисы, такие как австрийский платежный сервис PayLife, альтернативная платежная система Perfect Money и Payoneer – финансовый интернет-сервис, позволяющий пользователям переводить и получать средства, используя пополняемые предоплаченные дебетные карты MasterCard.

Кроме того, увеличилось количество атак на пользователей системы Bitcoin (в основом биткоин-сервисов Blockchain и Coinbase), а также веб-сайты ритейлеров и сервисные интернет-сайты.

Помимо этого, эксперты APWG предупреждают об увеличении количества потенциально нежелательных программ, таких как приложения adware и spyware. Как правило, такие программы находятся среди контента программных упаковщиков и инсталлируются вместе с нужными пользователю программами.

В целом, по данным специалистов, самым распространенными вредоносными программами остаются трояны ***(Фишеры атакуют сервисы криптовалюты и web-сайты ритейлеров // InternetUA (http://internetua.com/fisheri-atakuuat-servisi-kriptovaluati-i-web-saiti-riteilerov). – 2014. – 1.09).***

***

Интернет-пользователям под видом писем от имени Министерства обороны злоумышленники рассылают вирусы, сообщает «Телекритика».

В письмах подобного рода сообщается, что в связи с ситуацией в стране необходимо ознакомиться с документом, прикрепленным к письму. Подписываются послание якобы министром обороны В. Гелетеем. Говорится также, что этот прикрепленный файл следует обязательно прочитать, в противном случае человеку грозит уголовная ответственность.

При попытке прочитать документ пользователь получит exe-файл, который заражает компьютер вирусом ***(Злоумышленники рассылают письма с вирусами подписанные Минобороны // proIT (http://proit.com.ua/news/internet/2014/09/01/154151.html). – 2014. – 1.09).***

***

Хакери хитрістю змушують росіян встановлювати шкідливу програму Kelihos, а потім атакують їхні комп'ютери. Про це повідомляє securitylab.ru із посиланням на компанію-розробника антивірусів BitDefender.

Зловмисники користуються антиамериканськими та антизахідними настроями російських користувачів. У спам-листах вони пропонують програмне забезпечення, за допомогою якого нібито можна атакувати уряди західних країн у відповідь на санкції.

У спам-повідомленні від імені російських хакерів чи програмістів запевняють: якщо користувач запустить програму на своєму комп'ютері, то таємно атакуватиме урядові структури країн, які запровадили санкції. Насправді ж особа встановлює шкідливу програму Kelihos.

Перейшовши за посиланням, вона автоматично скачує троян, який встановлює три файли. Вони моніторять трафік і можуть отримати конфіденційні дані браузера та приватну інформацію користувача.

За даними експертів BitDefender, останні хвилі спаму пов'язані із серверами в Україні, а також у Польщі та Молдові ***(Хакери використовують гнів росіян щодо Заходу із шахрайською метою // MediaSapiens (http://osvita.mediasapiens.ua/material/34054). – 2014. – 27.08).***

***

31 августа сайт телеканала «112 Украина» был подвергнут мощной DDoS-атаке, источники которой, предположительно находились на территории России, сообщает корреспондент proIT.

Специалистам портала удалось идентифицировать и заблокировать основные источники хакерского вмешательства, хотя атаки различной интенсивности продолжались весь день 31 августа. Также были зафиксированы перебои с работой Интернет в офисе телекомпании.

Сообщается, что за последние несколько дней сайт телеканала «112 Украина» неоднократно подвергался мощным хакерским атакам ***(Российские***

хакеры атаковали сайт телеканала «112 Украина» // proIT (http://proit.com.ua/news/progress/2014/09/01/091432.html). – 2014. – 1.09).

***

Утром 2 сентября сайты посольств Украины в Польше, США, Австралии и Франции временно оказались недоступны, так же, как и сайт Министерства иностранных дел Украины, сообщает «Эспрессо TV». При попытке зайти на сайты этих украинских посольств, в браузере появлялось сообщение «Страница, которую вы ищете, временно недоступна. Пожалуйста, попробуйте позже» ***(Хакеры продолжают атаковать правительственные ресурсы // proIT (http://proit.com.ua/news/internet/2014/09/02/162407.html). – 2014. – 2.09).***

***

Служба безопасности Украины предупреждает, что в течение последних суток из российских информационных ресурсов происходит спланированная спецслужбами РФ информационная диверсия по заражению вредными программными продуктами мобильных телефонов украинских граждан. Об этом сообщает пресс-служба СБУ.

«Пользователям украинских мобильных компаний “Киевстар”, “МТС Украина” и “Астелит” осуществляется массовая рассылка sms-сообщений следующего содержания: “Привет. Тебе фото: https://soloboro.ru/zml/XXX-XXX-XX-XX” или “Привет. Тебе фото: https://motosan.ru/pdc/XXX-XXX-XX-XX”, где X – номер телефона абонента. При переходе по указанной ссылке мобильный телефон сразу же поражается вирусом, который мгновенно распространяется на все имеющиеся в телефонном блокноте контакты», – заявили в силовом ведомстве.

По информации правоохранителей, с помощью этого вируса преступно собирается информация по IMEI инфицированного телефона, баланса счета и персональных данных простых граждан. Именно эти данные могут быть использованы для массовой DOS-атаки на определенные ресурсы.

Специалисты предупреждают, что уязвимыми для этого вируса являются мобильные телефоны с операционными системами Android, Simbian, Windows Mobile.

Также выяснено, что рассылка вредоносных сообщений осуществлялась из столицы Российской Федерации ***(СБУ: Спецслужбы РФ через СМС заражают вредоносными вирусами мобильные телефоны украинцев // Судебно-юридическая газета (http://sud.ua/news/2014/09/03/67514-sby-spetsslyzhbi-rf-cherez-informatsionnie-sajti-zarazhayut-vredonosnimi-virysami-mobilnie-telefoni-ykraintsev). – 2014. – 3.09).***

***

Несмотря на статус самой закрытой от Интернета страны в мире, Северная Корея имеет в своём активе хакеров, которые на сегодняшний день являются весьма серьёзной угрозой для предприятий и правительств стран Запада.

Большинство хакерских атак из Северной Кореи направлены на компании в Южной Корее и США. Тем не менее, аналитики прогнозируют, что уже в ближайшем будущем хакеры Пхеньяна могут начать атаковать предприятия и госучреждения стран по всему миру.

Причиной увеличения количества атак и расширения из географии называют сложные отношения между США, Южной Кореей и Северной Кореей. Ситуацию обостряют санкции и торговые эмбарго, введённые многими правительствами против КНДР.

Впрочем, на сегодняшний день Северной Корее катастрофически не хватает ресурсов для создания полноценной «киберармии».

Согласно данным на июль 2014 г. количество хакеров Северной Кореи составляло порядка 5,9 тыс. человек, при этом, большая их часть входит в состав Корейской народной армии.

Ранее Северная Корея предложила Российской Федерации свою помощь в создании регионального Интернета, по образу и подобию «Кванмен». Северокорейская компания «Пхеньян Кванмен» выслала российской стороне несколько десятков резюме IT-профессионалов ***(Хакеры Северной Кореи угрожают всему миру // Блог Imena.UA (http://www.imena.ua/blog/north-korea-cyberspies). – 2014. – 2.09).***

***

Компания Apple исправила уязвимости в сервисе «Найти мой iPhone» (Find My iPhone), с помощью которого хакеры могли получить доступ к личной информации пользователей, в том числе к скандальным фотографиям обнаженных знаменитостей, сообщает портал ZDNet.

В воскресенье один из пользователей анонимного сайта 4chan заявил о том, что получил доступ к фотографиям с аккаунтов iCloud около 100 знаменитостей. За день до этого код для подбора пароля учетной записи AppleID был загружен на сайт GitHub. Код использовал уязвимость функции Find My iPhone, вследствие чего хакеры могли подобрать пароль к аккаунту методом брутфорс, то есть путем перебора всех возможных вариантов.

Для использования этого инструмента хакерам требовалось знать имя пользователя аккаунта, однако в его роли выступает адрес электронной почты пользователя, который, как правило, не слишком скрывают.

Неизвестно, как именно были взломаны облачные хранилища голливудских звезд, однако, как отмечают в ZDNet, взаимосвязь между двумя этими событиями очень вероятна.

В настоящее время уязвимость исправлена, и попытки подобрать пароль таким методом блокируются Apple ***(Apple исправила уязвимость, с***

помощью которой могли быть взломаны аккаунты знаменитостей // InternetUA (http://internetua.com/Apple-ispravila-uyazvimost--s-pomosxua-kotoroi-mogli-bit-vzlomani-akkaunti-znamenitostei). – 2014. – 2.09).

***

Группа хакеров под названием DERP, или DerpTrolling, создала мощный инструмент для осуществления DDoS-атак с отражением. По данным ИБ-компании Micron21, впервые за историю инцидентов безопасности одна группировка координировала осуществления сразу нескольких типов атак.

Сообщается, что жертвой хакеров стал дата-центр Micron21. Самой атаке эксперты компании присвоили название CDRDoS – Combination Distributed Reflective Denial of Service (смешанный распределенный отказ в обслуживании с отражением).

Особенностью DDoS-атак с отражением является то, что вместо привычного использования UDP-трафика, злоумышленники использовали для увеличения масштабов атаки протоколы NTP, DNS, SSDP и CHARGEN. В Micron21 говорят, что в одном из случаев мощность CDRDoS-атаки составила 40 Gbps.

Отметим, что DDoS-атаки с отражением считаются весьма опасными, поскольку они предоставляют высокий уровень амплификации. Одним из примеров осуществления подобной атаки является инцидент безопасности, в рамках которого жертвой стала компания Spamhaus.

Сами специалисты утверждают, что хакеры создали «супер-инструмент», который дал возможность осуществить CDRDoS-атаку. Более того, они уверены, что новая технология станет «будущим атак типа “отказ в обслуживании”» ***(Хакеры используют новый инструмент для осуществления «смешанных» DDoS-атак // InternetUA (http://internetua.com/hakeri-ispolzuuat-novii-instrument-dlya-osusxestvleniya--smeshannih--DDoS-atak). – 2014. – 2.09).***

***

У мережі «ВКонтакте» зафіксовано розповсюдження вірусу з профілю одного з чиновників України. Вірус розсилається в основному на телефони та соціальні профілі інших чиновників, пише Zaxid.net (http://zaxid.net/news/showNews.do?u_sotsmerezhi_vkontakte_poshiryuyetsya_virus_u_pikantnih_povidomlennyah_vid_ukrayinskogo_chinovnika&objectId=1321152).

Про це повідомила команда реагування на комп’ютерні надзвичайні події України (CERT-UA), яка входить у структуру Державної служби спеціального зв’язку та захисту інформації України.

«Нещодавно нами отримано інформацію про те, що певним посадовим особам України з сервісу VK надходять повідомлення різного підозрілого характеру, метою яких є заманювання користувача на ресурс у мережі

Інтернет, де розміщено шкідливе програмне забезпечення. При цьому вказується досить пікантна причина надходження такого повідомлення – посадовій особі буде складно потім привести її як аргумент, що є елементом соціальної інженерії», – наголошується у повідомленні.

Експертам CERT-UA вдалося з'ясувати, що підозрілий профіль у «ВКонтакте» зареєстрований на особу, що вказала як контактні дані мобільний телефон і поштову скриньку чиновника України.

«Репутація найбільш відомої російської соцмережі страждає ще й тому, що при спробі змінити пароль від облікового запису користувача повідомляють про те, що номер телефону буде змінено на російський через два тижні без повідомлення причини або запиту на це від самого користувача. Дивно, правда?» – додали у CERT-UA.

Держспецзв'язку закликало чиновників за можливості не відкривати такі «пікантні» повідомлення ***(У соцмережі «ВКонтакте» поширюється вірус у «пікантних» повідомленнях від українського чиновника // Zaxid.net (http://zaxid.net/news/showNews.do?u_sotsmerezhi_vkontakte_poshiryuyetsya_virus_u_pikantnih_povidomlennyah_vid_ukrayinskogo_chinovnika&objectId=1321152). – 2014. – 4.09).***

***

По данным исследования, проведенного компанией Panda Security, вредоносное программное обеспечение по-прежнему создается в рекордных количествах. Как отмечают специалисты, во II квартале текущего года было создано 15 млн образцов вредоносного ПО, то есть ежедневно появлялось порядка 160 тыс. вредоносных программ.

По словам специалистов, самыми распространенными вредоносными программами остаются трояны (62,8 %). Второе место занимают потенциально нежелательные программы (PUP) с показателем 24,77 % случаев инфицирования. В то же время эксперты Panda Security отметили уменьшение масштабов заражения рекламными и шпионскими вредоносами (7,09 %), а также различными вирусами (2,68 %) и червями (2,66 %).

Кроме того, аналитики отметили рост показателя глобального инфицирования вредоносным ПО, который во II квартале составил 36,87 % (в основном за счет заражения потенциально нежелательными программами). Больше всего случаев инфицирования было зарегистрировано в Китае (51,05 %), Перу (44,34 %) и Турции (44,12 %).

По словам специалистов, страны Азии и Латинской Америки лидируют по уровню заражения вредоносным ПО. А вот в Европе этот показатель оказался самым низким (Швеция – 22,13 %, Норвегия – 22,26 %, Германия – 22,28 %). Между тем, Япония оказалась единственной неевропейской страной с низким показателем количества случаев инфицирования вредоносным ПО (24,21 %) ***(Ежедневно в мире появляется 160000 новых вредоносных программ // InternetUA (http://internetua.com/ejednevno-v-mire-poyavlyaetsya-160000-novih-vredonosnih-programm). – 2014. – 3.09).***

***

Модификация печально известного вируса Kaptoxa, атакующего портативные кассовые аппараты, была обнаружена экспертами Trend Micro.

Как сообщают эксперты из Trend Micro, они до сих пор периодически встречают различные модификации вредоносной программы BlackPOS, исходный код которой был опубликован в открытом доступе еще в 2012 г. На сегодняшний день инструмент приобрел широкую популярность среди злоумышленников и, по мнению некоторых исследователей, с его помощью была реализована атака на Target.

Новая же модификация вируса, получившая название TSPY_MEMLOG.A, представляет собой во многом усовершенствованное решение. Среди прочих изменений, вирусописатели реализовали функционал маскировки программы под антивирус. Более ранние версии при этом способны имитировать уже имеющиеся на атакуемом устройстве службы.

Кроме того, в TSPY_MEMLOG.A используется функция пользовательского поиска для сбора финансовой информации. Это также помогает избежать обнаружения, поскольку аналогичные вирусы для хищения информации внедряются в системные процессы ***(Новый вариант BlackPOS использует пользовательский поиск для обнаружения финансовой информации // InternetUA (http://internetua.com/novii-variant-BlackPOS-ispolzuet-polzovatelskii-poisk-dlya-obnarujeniya-finansovoi-informacii). – 2014. – 3.09).***

***

Крупные хакерские группировки, ответственные в том числе за взлом сайтов The New York Times и Coca-Cola, проверяли свой вредоносный код на наличие багов через антивирусный сайт Google. Об этом 2 сентября сообщает журнал Wired.

Схему с использованием злоумышленниками противовирусного ресурса американской IT-компании удалось обнаружить блогеру Б. Диксону, специализирующемуся на изучении вопросов кибербезопасности.

По его данным, хакеры проверяли код с помощью сайта VirusTotal – агрегатора, предоставляющего пользователям бесплатный доступ к антивирусному ПО почти 50 сторонних компаний-разработчиков от Symantec до «Лаборатории Касперского». Основанная в Испании компания VirusTotal принадлежит Google с 2012 г.

В течение нескольких лет Б. Дискон отслеживал загружаемые на VirusTotal файлы с кодом, при помощи специального алгоритма выявляя те из них, что содержат в себе вирусы. В итоге ему удалось обнаружить несколько групп хакеров, регулярно проверявших на ресурсе создаваемые ими вредоносные программы.

По именам их документов, датам и IP-адресам, хранящимся в метаданных, блогер установил, что вирусы загружались на проверку одними

и теми же людьми, принадлежащими к хакерским командам из Китая и Ирана.

Одна из таких команд – Comment Crew, также известная, как APT1 – спонсируется китайским правительством и ранее брала на себя ответственность за взлом сайта газеты The New York Times и официального портала корпорации Coca-Cola.

Другая группа – NetTraveler. Команда тоже базируется в Китае и использует VirusTotal для проверки кодов, с помощью которых затем атакует ресурсы Далай Ламы и различных организаций, выступающих за независимость Тибета.

В июне этого года блогеру также удалось обнаружить активную группировку хакеров, работавших с иранских IP-адресов. За несколько месяцев они загрузили для проверки на VirusTotal более тысячи вирусных документов. Для сравнения, хакеры из Китая каждый год проверяли на антивирусном сайте Google около 350–400 документов.

«Обнаружить хакеров было непросто. Сначала, когда я смотрел на все полученные мной данные, я даже не знал с чего начать поиски. Но позже оказалось, что хакеры используют для выгрузки файлов всего два-три IP-адреса. Только спустя какое-то время они, судя по всему, поняли, что за ними могут следить и стали постоянно менять IP», – рассказал Б. Диксон.

За день до публикации в Wired Б. Диксон выложил у себя в блоге исходный код написанной им программы, собирающей метаданные загружаемых на VirusTotal файлов. По словам блогера, он надеется, что к отслеживанию хакеров, паразитирующих на антивирусном ресурсе Google, теперь подключатся и другие исследователи.

Представители Google на момент написания этой заметки никак не прокомментировали сведения об использовании VirusTotal хакерами ***(Хакеров уличили в использовании антивирусного сайта Google для поиска багов во вредоносном коде // InternetUA (http://internetua.com/hakerov-ulicsili-v-ispolzovanii-antivirusnogo-saita-Google-dlya-poiska-bagov-vo-vredonosnom-kode). – 2014. – 3.09).***

***

Новая разновидность бэкдора использует сеть Tor для соединения с C&C-сервером.

Компания Trend Micro заявила об обнаружении нового варианта бэкдора Bifrose, который использовался для совершения кибератаки на неизвестного производителя устройств. Получивший название BKDR_BIFROSE.ZTBG-A, новый бэкдор использует анонимную сеть Tor для соединения с C&C-сервером.

После заражения устройства бэкдор дает возможность злоумышленникам выполнять разнообразные задачи – загружать произвольные файлы, создавать и удалять папки, запускать произвольные

программы, перехватывать клавиатурные нажатия и изображения веб-камер, делать скриншоты, останавливать процессы и манипулировать окнами.

По словам специалиста Trend Micro К. Со, Bifrose в основном используется как кейлоггер, но вредонос способен на гораздо большее количество действий. Эксперт описал в своем блоге, что Bifrose дает воможность злоумышленнику полностью управлять зараженным компьютером без компрометации учетных данных жертвы.

Чтобы выяснить, заражены ли корпоративные сети новой разновидностью Bifrose, достаточно проверить наличие в них трафика Tor. Обычно организации не используют анонимные сети для совершения регулярных операций, поэтому обнаружение трафика Tor в корпоративной сети – достаточно верный признак заражения. Также можно выполнить поиск файла klog.dat, который используется бэкдором для перехвата клавиатурных нажатий, проверить журналы сети и почты ***(Модифицированная версия Bifrose использовалась в таргетированных атаках // InternetUA (http://internetua.com/modificirovannaya-versiya-Bifrose-ispolzovalas-v-targetirovannih-atakah). – 2014. – 3.09).***

***

Исследователи сообщают, что пользователей iOS-устройств можно деанонимизировать и идентифицировать, использовав особую схему кодинга, затрагивающую Facebook, Google, Twitter и ряд прочих сайтов.

Проэксплуатировав уязвимость в этой схеме, злоумышленники могут отправить жертве SMS или сообщение через Facebook, Google Plus, Gmail или Twitter, которое при открытии вынуждает телефон пользователя совершить звонок без подтверждения действия.

С помощью этой бреши также можно инициировать звонок через FaceTime. Если жертва не успеет разорвать связь, злоумышленник сможет увидеть ее лицо.

Опасность заключается в том, что от жертвы не требуется подтверждать свои действия. Все действия киберпреступников могут выполниться в автоматическом режиме.

В Apple уже знают об этой проблеме. В документе, описывающем уязвимость, представители компании рассказали, что, когда пользователь переходит по телефонной ссылке на веб-странице, iOS уведомляет пользователя о попытке совершить звонок и просит его подтвердить действие. Когда пользователь открывает URL-ссылку с телефонным кодом в iOS-приложении, система совершает звонок без отображения предупреждения».

О проблеме стало известно после того, как исследователь безопасности Р. Боргонкар предположил, что разработчики Facebook и Google невнимательно прочитали руководство для разработчиков iOS-приложений.

Р. Боргонкар разместил материал, демонстрирующий, как с помощью Facebook можно проэксплуатировать эту уязвимость. Он сообщил, что

протестировал ее лишь на нескольких крупных приложениях и у него почти нет сомнений в том, что более мелкие разработчики также допустили похожие ошибки ***(Ошибка в iOS-устройствах может деанонимизировать пользователей социальных сетей // InternetUA (http://internetua.com/oshibka-v-iOS-ustroistvah-mojet-deanonimizirovat-polzovatelei-socialnih-setei). – 2014. – 3.09).***

***

Международная антивирусная компания Eset (Словакия) сообщила о распространении нового трояна под видом писем от интернет-магазина.

Как говорится в заявлении Eset, поступившем в редакцию CNews, вредоносное ПО распространяется в спамерской рассылке. В теле письма сообщается, что пользователь успешно оформил заказ, детали которого можно посмотреть в приложении. На самом деле, приложение содержит исполняемый exe-файл с вредоносным ПО, которое детектируется решениями Eset NOD32 как Win32/TrojanDonloader.Elenoocka.

После установки на компьютер жертвы троян загружает из Интернета другие вредоносные программы. В коде Elenoocka содержится шесть URL-адресов для скачивания файлов, в числе которых – разновидность трояна семейства Kryptik, рассказали в компании.

Win32/Kryptik.CKEY создает вредоносные файлы, прячет их среди системных файлов и открывает доступ для заражения другими видами вредоносного ПО. Также жертвы Kryptik могут войти в состав ботнета.

Вирусные аналитики Eset рекомендуют пользователям не открывать вложения в незапрошенных письмах и регулярно проводить сканирование компьютера антивирусным ПО ***(Новый троян маскируется под письма от интернет-магазинов // InternetUA (http://internetua.com/novii-troyan-maskiruetsya-pod-pisma-ot-internet-magazinov). – 2014. – 4.09).***

***

Как сообщают исследователи Akamai Technologies, крупным организациям, использующим компьютерные системы на базе Linux, грозит серьезная опасность в виде заражения вредоносными программами IptabLes и IptabLex. При этом инфицированные такими вирусами сети злоумышленники используют для проведения масштабных DDoS-атак на представителей индустрии развлечений и ряда других.

Стоит отметить, что вирусописатели атакуют неподдерживаемые Linux серверы, в которых присутствуют старые уязвимости, позволяющие получить удаленный административный доступ к системе. В большинстве случаев компрометации подвергаются веб-серверы с уязвимыми версиями Apache Struts, Tomcat и Elasticsearch.

«Мы проанализировали одну из наиболее масштабных DDoS-атак в 2014 г. и выяснили, что она осуществлялась при помощи вирусов IptabLes и IptabLex», – поясняет исследователь С. Шолли.

По его словам, подобные атаки на Linux-системы нельзя назвать тривиальными, поэтому системным администраторам стоит обратить внимание на эту угрозу ***(Системы на базе Linux инфицирует новый DDoS-ботнет // InternetUA (http://internetua.com/sistemi-na-baze-Linux-inficiruet-novii-DDoS-botnet). – 2014. – 4.09).***

***

Исследователь компании AlienVault Д. Бласко сообщил о том, что программное обеспечение, которое используют инженеры компаний-автостроителей и предприятий авиационно-космической промышленности, может быть скомпрометировано вредоносными шпионскими программами типа кей-логгеров.

По словам специалиста, штатный сотрудник одного из предприятий стал жертвой вредоносного ПО после посещения подозрительного веб-сайта, который был создан специально для завлекания служащих этой компании.

Во время посещения веб-сайта, компьютер сотрудника был инфицирован вредоносной программой ScanBox, которая фиксировала нажатие клавиш и похищала учетные данные входа в систему. После этого, все полученная таким образом информация тщательно зашифровывалась и отправлялась на командный сервер злоумышленников.

Д. Бласко пояснил, что во время просмотра пользователем скомпрометированного веб-сайта, вредоносная программа фиксирует все нажатия клавиш, в том числе и при вводе учетных данных, которые могут стать потенциальным источником конфиденциальной информации, и периодически отправляет полученные сведения на командный сервер. Специалист отметил, что таким образом злоумышленники собирают необходимые данные для будущих хакерских атак.

Суть атаки по типу watering hole заключается в том, что киберпреступники заражают вредоносным ПО веб-сайты, наиболее часто посещаемые их потенциальными жертвами. В результате такой атаки скомпрометированной оказывается вся компьютерная сеть компании, в то время как ее сотрудники не подозревают об угрозе ***(Системы автопроизводителей и авиационно-космических предприятий могут пострадать от шпионского ПО // InternetUA (http://internetua.com/sistemi-avtoproizvoditelei-i-aviacionno-kosmicseskih-predpriyatii-mogut-postradat-ot-shpionskogo-po). – 2014. – 6.09).***

***

По данным экспертов из Blue Coat Systems, почти три четверти имен хостов в Интернете существуют не более одного дня, и многие из них используются для вредоносной активности. В течение 90 дней эксперты анализировали 660 млн уникальных имен хостов, запрошенных 75 млн пользователей по всему миру.

Во время исследования эксперты обнаружили, что 71 % (470 млн) имен хостов появлялись только на один день, а то и меньше. Кроме того, 22 % из топ-50 родительских доменов, используемых однодневками, оказались вредоносными. Операторами подавляющего большинства недолговечных сайтов являются легитимные крупные корпорации, такие как Google, Amazon и Yahoo. Тем не менее, большое количество ресурсов используются злоумышленниками для осуществления атак, рассылки спама и управления ботнетами.

Эксперты пояснили, что благодаря динамичности и недолговечности такие сайты сложнее обнаружить с помощью традиционных продуктов безопасности. К тому времени, когда типичный инструмент проанализирует и заблокирует подобный вредоносный ресурс или рассылающий спам электронный адрес, он уже успеет исчезнуть и сменить имя хоста или поддомен. Появление большого количества таких доменов увеличивает шансы того, что продукты безопасности пропустят номер одного из них.

По словам экспертов, несмотря на то, что большинство однодневок не являются вредоносными и создаются для легитимной деятельности, их огромное количество создает благоприятную среду для вредоносной активности ***(Хакеры используют домены-однодневки для вредоносной активности // InternetUA (http://internetua.com/hakeri-ispolzuuat-domeni-odnodnevki-dlya-vredonosnoi-aktivnosti). – 2014. – 6.09).***

***

Социальная сеть Facebook развёртывает кампанию, в рамках которой будет пошагово учить пользователей повышать уровень защищённости персональных данных.

Главной целью программы Facebook является помощь пользователям в управлении публикациями и их распространением в социальной сети.

За обучение людей отвечает голубой динозаврик, разъясняющий настройки приватности, которые следует знать, публикуя частную информацию, медиаконтент или просто тексты.

Электронный помощник появится сразу после входа в учётную запись в Facebook и пошагово объяснит пользователю все настройки приватности – от личной информации до приложений, получающих доступ к данным социальной сети.

Кроме того, на странице каждого пользователя появится отдельный ярлык, ведущий сразу к настройкам приватности ***(Facebook научит пользователей защищать личные данные // Блог Imena.UA (http://www.imena.ua/blog/facebook-privacy-checkup-is-now-rolling-out). – 2014. – 5.09).***

***

У рамках повномасштабної допомоги НАТО Україні, альянс підтримає нас і в галузі протидії кібератак, частота та масштаб яких збільшились у звязку з українсько-російським конфліктом.

Як пише Deutsche Welle, про допомогу Україні заявив генсек НАТО А. Фог Расмуссен за результатами зустрічі глав держав та урядів країн альянсу з Президентом України П. Порошенком. Переговори відбулись у рамках дводенного саміту НАТО, що проходить в Уельсі.

Допомога надаватиметься у сфері логістики, командування та комунікацій, а також у протидії кібератакам.

За даними молдавського порталу ava.md, керувати операцію з протидії кібератакам буде Румунія – країна-член НАТО. Про це заявив президент Румунії Т. Басеску ***(НАТО допоможе Україні протидіяти кібератакам // UkrainianWatcher (http://watcher.com.ua/2014/09/05/nato-dopomozhe-ukrayini-protydiyaty-kiberatakam). – 2014. – 6.09).***