СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(20.10–2.11)

2014 № 20

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(20.10–2.11)
№ 20

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

Разработчик популярной в социальной сети Facebook кнопки Like Б.Тейлор объяснил, почему пользователям не стоит ждать появления кнопки Dislike.

Facebook-сообщество давно ждёт от администрации социальной сети активации кнопки Dislike, которая позволит высказывать своё негативное отношение к той или иной записи, фотографии или ссылке.

Б. Тейлор уверяет, что чаяния получить возможность «не любить» в социальной сети безнадёжны.

Создание такой кнопки обсуждали неоднократно, однако, неприятные последствия и для пользователей, и для социальной сети слишком велики, чтобы добавить подобный функционал.

По мнению Б. Тейлора, появление Dislike спровоцирует негативное отношение к Facebook, поскольку кнопку могут использовать для сведения личных счётов или обычного хулиганства. Более того, даже клавиша Like существует в социальной сети для того, чтобы её пользователи могли поделиться друг с другом той или иной информацией, когда им самим нечего сказать.

Сама по себе кнопка в своей оригинальной задумке не подразумевает, что пользователю действительно близок отмеченный материал.

Ранее социальная сеть Facebook объявила, что с ноября 2014 г. начнёт удалять группы и приложения, поощряющие злоупотребление кнопкой Like ***(Создатель «Like» объяснил, почему никогда не будет кнопки «Dislike» // Блог Imena.UA (http://www.imena.ua/blog/you-ll-never-get-a-dislike-button/). – 2014. – 22.10).***

***

В ходе состоявшейся 22 октября в Сан-Франциско конференции для разработчиков мобильных приложений, компания Twitter анонсировала запуск нового сервиса под говорящим названием Digits, новейший способ входа в приложения с использованием номера мобильного телефона. По сути, создатель популярного сервиса микроблогов хочет заменить старые добрые пароли, с которыми у многих пользователей зачастую возникают проблемы (либо забывают, либо выбирают очень простые комбинации), верификацией с помощью номера мобильного телефона, информируют «Экономические известия» (http://news.eizvestia.com/news_technology/full/281-twitter-anonsiroval-novyj-servis-digits).

Таким образом, Twitter предлагает пользователям забыть об утомительном процессе аутентификации, который подразумевает использование адреса электронной почты и пароля или одной из учетных записей в соцсетя. Все, что нужно – это ввести в поле номер мобильного

телефона и получить код подтверждения в сообщении SMS. Никаких паролей или графических подтверждений.

Сервис Digits не имеет никакой привязки к Twitter, это полностью новый продукт, который разработчики могут внедрить в свои мобильные приложения. «Цифры» являются ключевой частью нового мобильного комплекта средств разработки под названием Fabric, о выходе которого также было сообщено на конференции. В настоящее время Digits доступен в 216 странах на 28 языках. Его могут использовать как клиентские приложения для iOS и Android, так и веб-версии разных служб.

Помимо Digits, Fabric включает еще несколько инструментов, которые разработчики сочтут полезными и используют в существующих приложениях. По крайней мере, так думают в Twitter. В их числе стоит отметить Crashlytics (позволяет вести детальный анализ и отчетность критических ошибок) и MoPub (рекламная площадка). Там также есть то, что называется TwitterKit – аутентификация для входа в Twitter на системном уровне в Android. Это означает, что однажды осуществив вход в Twitter с помощью Android-смартфона, появится возможность авторизоваться во многих приложениях, используя свою учетную запись Twitter ***(Twitter анонсировал новый сервис Digits // Экономические известия (http://news.eizvestia.com/news_technology/full/281-twitter-anonsiroval-novyj-servis-digits). – 2014. – 23.10).***

***

В Интернете запустили социальную сеть, которая платит своим пользователям за каждую запись.

Социальная сеть Tsu делится рекламной выручкой с пользователями, которые написали заметку или пригласили друзей.

Администрация сети отмечает, что в общей сложности ими будет удерживаться всего 10 % доходов от рекламы, а оставшиеся 90 % будут распределяться между пользователями.

В настоящее время социальная сеть доступна в качестве веб-версии и мобильных приложений для iOS и Android. В общих чертах по функциональности она напоминает Facebook.

На стадии бета-тестирования сервис пригласил к раскрутке нескольких знаменитостей, включая рэпера 50 Cent и звезду НБА К. Энтони.

Администрация сравнивает подавляющее большинство современных популярных интернет-сервисов с радиостанцией, которая «ставит в эфир песни всех пользователей, не выплачивая им гонорара».

При этом, по мнению руководства Tsu, весьма необычно, что все пользователи просто так, бесплатно, выкладывают в Интернет ценные материалы, которые монетизируются на 100 %.

Кстати, другая социальная сеть, Netropolitan, позиционируется как «онлайн-клуб для людей, у которых больше денег, чем времени» ***(Появилась социальная сеть, которая платит участникам за публикации // Блог***

Imena.UA (http://www.imena.ua/blog/social-network-tsu-pays-users/). – 2014. – 23.10).

***

Социальная сеть Facebook представила приложение для анонимного общения Rooms.

Его пользователи могут общаться на предложенные темы под псевдонимом, кроме того, им вовсе не обязательно иметь зарегистрированный аккаунт в соцсети, информируют «Экономические известия» (http://news.eizvestia.com/news_technology/full/387-v-facebook-stalo-vozmozhnym-obshhatsya-bez-registracii).

Название приложения в переводе с английского означает «комнаты». Любой желающий может открыть в нем чат, сделать его доступным для всех или же разослать приглашения для участия в нем. Внешне приложение напоминает новостную ленту, в которой, прокручивая, можно выбирать понравившуюся «комнату».

Представитель компании Д. Миллер пояснил, что имена при использовании приложения можно менять, находясь в различных чатах. В «комнатах» также можно размещать фотографии, видео, выбирать цвета для оформления.

Разработчики, по заявлению Д. Миллера, черпали вдохновение из 1990-х годов, когда Интернет переживал расцвет разнообразных площадок для общения, к которым можно было присоединяться анонимно и без регистрации.

Приложение уже доступно пользователям США и Великобритании, однако выпущено пока только для платформы iOS от Apple ***(В Facebook стало возможным общаться без регистрации // Экономические известия (http://news.eizvestia.com/news_technology/full/387-v-facebook-stalo-vozmozhnym-obshhatsya-bez-registracii). – 2014. – 24.10).***

***

26 октября в Дублине руководители налоговых служб Форума по налоговому администрированию (FTA) представляют совместное коммюнике, в котором описаны меры совершенствования налогового контроля. Коммюнике должны подписать налоговые службы 45 стран-участниц форума.

Усиливать контроль планируется через все более тесное сотрудничество налоговых служб: уже согласована стратегия взаимодействия налоговиков 45 стран, для чего, в частности, создается международная платформа JITSIC (Объединенный информационный центр по налоговым уклонениям). JITSIC концентрируется на противодействии практикам избежания налогообложения с применением трансграничных схем, говорится в проекте коммюнике: «Это новая сеть, и она позволит интегрировать уже

существующее между некоторыми из нас сотрудничество в более широкое, охватывающее всех участников форума».

«Обмен информацией будет проходить только по существующим налоговым соглашениям между странами, но общее взаимодействие будет менее формализованным, чем сейчас», – объясняет чиновник, близкий к ФНС. В налоговых органах стран-участниц форума, продолжает он, появятся специальные сотрудники: они будут отвечать за поддержку работы сети JITSIC и оперативное взаимодействие с налоговиками других стран. Это похоже на обмен полезными сведениями, объясняет чиновник: например, налоговая служба какой-то страны проводит проверку трансграничной компании – и специальный сотрудник оповестит об этом иностранных налоговиков и посоветует им присоединиться к проверке.

Основной объект взаимодействия налоговиков через JITSIC – крупные компании с трансграничными сложными схемами.

Это такой Facebook для налоговиков: база данных и сеть представителей в налоговых органах, резюмирует партнер Paragon Advice Group А. Захаров. Пока круг участников самой JITSIC ограничен (Австралия, Великобритания, Канада и США создали, к ним присоединились Германия, Китай, Корея, Франция и Япония) – их можно описать как круг избранных в сфере продвинутого налогового сотрудничества, сравнивает А. Захаров. Участники могут обмениваться информацией о различных схемах уклонения или о лицах, которые рекламируют и продвигают такие схемы, полагает он.

Такое взаимодействие действительно поможет усилить контроль за трансграничными схемами, ожидают юристы. У России был плохо налажен обмен информацией с другими странами, говорил сотрудник ФНС: до трети запросов оставались без ответа, ответы из таких стран, как Кипр, были формальны и бессодержательны. Налоговые службы, получая запрос из России, могли даже спрашивать у проверяемой компании, что ответить российским налоговикам, вспоминал налоговый менеджер компании. Но в последнее время был достигнут большой прогресс. Госдума приняла законопроект, ратифицирующий «Конвенцию о взаимной административной помощи по налоговым делам», она даст возможность обмениваться информацией не только по запросу, но и в новом формате – автоматического или спонтанного обмена: налоговики другой страны сами оповестят Россию о подозрительных действиях ее налогоплательщиков. Также после подписания конвенции ФНС сможет более активно проводить выездные проверки совместно с иностранными налоговиками – несколько таких проверок уже состоялось, рассказывали чиновники ФНС.

Но в обмене информацией важна скорость, подчеркивает федеральный чиновник: получение данных из каждой страны может растягиваться на месяцы, при сложной цепочке – на год и даже больше.

Налоговикам постоянно нужны оперативные данные от иностранных коллег, продолжает чиновник: о бенефициарах, которые тот же Кипр не всегда раскрывает, а без них ФНС не знает, «прокладка» ли иностранная

компания или реально работающий бизнес. От этого зависит, могут ли применяться льготные ставки при выплате заграницу дивидендов и процентов по кредитам. Часто нужны данные, на какой счет пришли средства за акции, кому они были переданы, кто и в какой момент стал директором компании, перечисляет чиновник.

Сейчас налоговики могут просто не успеть собрать данные до окончания предельного срока проверки, сетует источник информации, сеть ускорит процесс ***(В Дублине создают всемирный «Facebook для налоговиков» // IT Expert (http://itexpert.org.ua/rubrikator/item/39032-v-dubline-sozdayut-vsemirnyj-facebook-dlya-nalogovikov.html). – 2014. – 26.10).***

***

Компанія Twitter вберегла сервіс Twitpic від закриття, придбавши його базу даних з фотографіями.

Утім, як повідомляється в офіційному блозі Twitpic, нові знімки користувачі вже не зможуть завантажувати. Twitpic мав закритися 25 жовтня, однак за лічені години до відключення серверів компанія повідомила, що мільйони знімків користувачів залишаться на своїх місцях завдяки Twitter.

Сервіс мікроблогів і найпопулярніший фотохостинг для роботи з ним досягли угоди, згідно з яким перший отримає базу даних та інфраструктуру другого, але не буде їх розвивати. Додатки Twitpic видалені з Google Play і App Store, а заливка нових знімків у сервіс заборонена.

Протягом декількох років сам Twitter не пропонував можливості куди-небудь заливати знімки, тому Twitpic і його аналоги процвітали. Однак після того як сервіс мікроблогів запустив власний фотохостинг, він почав усувати конкурентів ***(Twitter викупив базу даних з фотографіями Twipic // UkrainianWatcher (http://watcher.com.ua/2014/10/27/twitter-vykupyv-bazu-danyh-z-fotohrafiyamy-twipic/). – 2014. – 27.10).***

***

«ВКонтакте» готовит приложение для смартфонов, которое позволит пользователям снимать фото, обрабатывать их с помощью фильтров и загружать в соцсеть. Об этом «Известиям» сообщили несколько источников, знакомых с разработкой. В пресс-службе соцсети от комментариев отказались (http://mmr.ua/news/id/facebook-predlozhila-podelitsja-dohodami-s-izdateljami-mobilnogo-kontenta-41858/).

Пока фотоприложение создают лишь для платформы Android – разработчика для iOS соцсеть еще не нашла. Когда оно будет опубликовано в Play Market (созданный компанией Google фирменный магазин предложений для Android), пока точно неизвестно, рассказывает один из источников.

Фотоприложение «ВКонтакте» будет частично напоминать соцсеть Instagram. У пользователя будет возможность делать фотографии, накладывать на них фильтры и делать минимальную обработку на основе уже созданного соцсетью фоторедактора.

«Делают что-то вроде Facebook Camera», – добавляет другой источник. – О. Илларионов (старший разработчик «ВКонтакте») большой энтузиаст нового проекта. Он выбил под этот проект ресурсы и верит, что сервис понравится пользователям.

Facebook в 2012 г. анонсировала фотоприложение Facebook Camera (FC). В тот момент крупнейшая соцсеть мира занималась приобретением Instagram – популярного во всем мире сервиса, позволяющего делать фотографии на смартфонах, обрабатывать их фильтрами (к примеру, отрегулировать яркость, добавить виньетку или «замылить» второстепенные детали), показывать фото знакомым и комментировать их. В тот момент документы об одобрении сделки находились на рассмотрении в Федеральной комиссии по торговле США. Очевидно, что над приложением Facebook начала трудиться еще до решения о покупке Instagram.

По своей идеологии приложение Facebook отличалось от Instagram. Camera давала возможность пользователю загружать сразу несколько фотографий одновременно (Instagram тогда не позволял этого). Фотографии в FC могли быть не только квадратными. Приложение считывало геометки с фото и показывало, где снимок был сделан. В ленте друзей FC отображались только посты с фотографиями.

Впоследствии сделка Facebook с Instagram была одобрена – компания М. Цукерберга заплатила за фотосервис около 1,3 млрд дол. Из них 300 млн дол. были заплачены наличными. Кроме того, владельцы Instagram получили 23 млн акций соцсети. Таким образом, собственный сервис, дублирующий Instagram, оказался ненужным, и в мае этого года Facebook удалила приложение FC из AppStore (магазин приложений iOS), в Play Market оно так и не появилось.

У «ВКонтакте» уже были попытки создать сторонние сервисы на основе соцсети. Например, сервис по поиску работы «ВШтате» или видеосервис «ВКадре». Однако они не нашли поддержки у пользователей и в результате через какое-то время были закрыты.

По мнению гендиректора сервиса знакомств Teamo А. Бурина, фотоприложение создается, чтобы удержать аудиторию, которая начинает интересоваться другими сервисами.

«Молодые люди постоянно ищут какие-то новые сервисы. Возможно, администрация “ВКонтакте” изучила статистику, и та показала: всё большая часть их аудитории стала пересекаться с фотосервисами. Этих людей соцсеть захотела оставить у себя», – предположил эксперт.

Гендиректор соцсети для детей Tvidi О. Ульянский напомнил, что Facebook уже давно разделяет свой сервис на «дочерние» приложения. К примеру, одним из первых они запустили Facebook Massenger.

«Благодаря мощным каналам связи и новым девайсам с хорошими объективами снимки всё больше гуляют по Интернету. Предпочтение сейчас отдается визуальному контенту. Фотографию отправить проще, чем описать что-то словами. При этом изображение нагляднее, чем текст», – говорит

О. Ульянский. – Удобно, если бы фотоприложение позволяло слать фото не только во «ВКонтакте». При запуске нового сервиса можно обойтись минимумом функций. Но со временем надо будет «прикручивать» новые возможности. Например, создавать анимированные изображения. Или из нескольких фотографий делать презентацию с наложением музики ***(«ВКонтакте» запустит собственный Instagram // Marketing Media Review (http://mmr.ua/news/id/vkontakte-zapustit-sobstvennyj-instagram-41856/). – 2014. – 28.10).***

***

Facebook готова поделиться доходами с издательствами, которые готовы отсылать статьи из своих газет, журналов и сайтов в социальную сеть для размещения непосредственно в мобильном приложении, сообщает New York Times, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-predlozhila-podelitsja-dohodami-s-izdateljami-mobilnogo-kontenta-41858/).

Приложение Facebook ежедневно открывают 654 млн пользователей, и социальная сеть приложила все усилия к тому, чтобы контент загружался быстро. Однако исходный сайт может быть довольно медлительным из-за большого количества публикуемой на нем рекламы, и Facebook надеется, что сможет помочь издателям решить эту проблему, превратив, таким образом, потребление мобильного контента в менее утомительное. Кроме того, социальная сеть предложила поделиться доходами с производителями контента, пишет Business Insider. Появление такой возможности не только подчеркивает растущий авторитет социальной сети (она является основным поставщиком трафика для большинства издательских сайтов), но и говорит о том, что она готова будет поделиться с издателями пользовательскими данными, связанными с потреблением контента.

И действительно, недавно К. Данкан, глава маркетингового отдела News UK (группы, издающей, в частности, газеты The Times и The Sun), написал в своем Twitter: «Предлагаемое Facebook позиционирование от лица потребителя захватывает дух. Амбициозная попытка стать мобильной платформой, способной заткнуть за пояс Google».

Работа над контентом для мобильного приложения была не первой попыткой Facebook наладить отношения с издателями. В 2011 г. The Guardian, The Washington Post, Business Insider и The Independent объединились с Facebook в работе над приложением Social Reader, позволяющим пользователям читать и делиться контентом внутри социальной сети.

Однако уже в 2012 г. большинство из этих издателей стало отказываться от приложения, поскольку выяснилось, что основное взаимодействие с их контентом велось по большей части на платформе Facebook – без какого бы то ни было перехода на исходные сайты СМИ.

В начале этого года Facebook запустила автономное приложение Paper – в качестве ответа на появление таких новостных агрегаторов, как Feedly и

Flipboard. Однако популярным оно оставалось недолго ***(Facebook предложила поделиться доходами с издателями мобильного контента // Marketing Media Review (http://mmr.ua/news/id/facebook-predlozhila-podelitsja-dohodami-s-izdateljami-mobilnogo-kontenta-41858/). – 2014. – 28.10).***

***

Социальные сети все глубже проникают в жизнь пользователей и меняют не только то, как они общаются и получают информацию, но и то, как они употребляют новости. Все больше читателей идут за новостями даже не на главную страницу интернет-издания, а в свою ленту новостей Facebook, выяснили эксперты.

На сегодняшний день примерно каждый пятый человек на земле – около 1,3 млрд людей – хотя бы раз в месяц заходит в Facebook, и вполне закономерно, что огромная социальная сеть повлияла и на индустрию новостей. По данным аналитической компании SimpleReach, через социальную сеть на новостные сайты попадают около 20 % их посетителей. Если говорить о трафике с мобильных устройств, эта доля еще выше, и она продолжает расти.

Facebook удалось изменить саму модель потребления информации – это касается и других сервисов, например Twitter или Google News, однако у истоков перемен стояло именно детище М. Цукерберга. Около 30 % взрослых американцев теперь узнают последние новости из социальной сети, подсчитали исследователи Pew Research Center. Все больше читателей попадают к новостям не через главную страницу сайта, а через рекомендации из социальных сервисов и поисковики.

Социальные сети настолько же сильно меняют новостные сайты, насколько Интернет изменил музыкальную индустрию, говорит старший редактор сайта Washington Post К. Хайк: новостные сайты теперь делают акцент на отдельных текстах, а не на целых выпусках газет и журналов, так же как и музыканты продают не целые альбомы, а отдельные треки. По прогнозам сооснователя исследовательской компании SimpleReach Э. Кима, скоро главные страницы интернет-изданий будут выполнять прежде всего рекламную и имиджевую функции: за новостями читатели будут идти в соцсети.

Впрочем, несмотря на то что социальные медиа выбирают, на какие именно статьи обратить внимание читателей, инженер Google Г. Мappa, возглавляющий команду разработчиков ленты новостей Facebook, подчеркивает, что они не могут заменить собой редакторов.

«Мы не хотим пытаться отредактировать, какой контент вы видите, – рассказал он New York Times. – Вы завели друзей, вы подписались на интересующие вас страницы, и что для вас важно – решать именно вам».

Facebook говорит пользователям: «Мы думаем, что изо всех вещей, с которыми вы связаны, эти окажутся самыми интересными для вас», поясняет Г. Мappa.

Команда Г. Марры, насчитывающая 16 человек, еженедельно настраивает код, определяющий, что демонстрировать пользователю, который заходит в социальную сеть. Подробностей о том, как именно работает этот алгоритм, в Facebook не раскрывают, однако говорят, что он основан на «тысячах и тысячах» параметров, в том числе через какое устройство пользователь сидит в соцсети, сколько лайков и комментариев у записи и сколько времени пользователи проводят, читая статью.

Цель их работы – определить, что больше всего нравится пользователям, и в разных странах результаты отличаются. Индийским пользователям, например, больше всего интересны астрология, Болливуд, крикет и религия.

Примерно 10 % современных пользователей социальных сетей вообще не посещают новостные СМИ иначе как через социальные сети, отмечает гендиректор и владелец компании Liveinternet Г. Клименко.

Помимо трафика безусловным плюсом от социальных сетей для СМИ является четкое указание на интересы посетителей, на то, что им действительно интересно и волнует, подчеркнул Г. Клименко в беседе с корреспондентом «Газеты.Ru»:

«В современном новостном потоке задача определения того, что нужно пользователю на самом деле, превращается в достаточно сложную и не всегда хорошо решаемую задачу. Социальные сети справляются с вычленением интересов пользователей достаточно просто, и те СМИ, которые анализируют трафик из социальных сетей внимательно, безусловно получают бонус при определении наиболее эффективной и привлекательной повестки дня для пользователей».

Влияние алгоритма Facebook на жизнь интернет-изданий огромно. Так, когда в феврале большим приоритетом стали пользоваться ссылки на более качественный контент, несколько «виральных» сайтов, например Upworthy и Elite Daily, получили резкое снижение числа посетителей. Рецепта же для резкого увеличения числа посетителей из соцсетей не существует.

«Ни на формате, ни на контенте переходы из соцсетей сказаться не могут. Потому что эти самые переходы с сайта Facebook на сайты СМИ – не из страниц изданий на Facebook, а из рекомендаций друзей. На эти рекомендации у СМИ есть единственный способ повлиять: публиковать то, что интересно читателю», – рассказал «Газете.Ru» медиааналитик А. Носик.

Уже состоявшимся медиакомпаниям опасно гнаться за социальными сетями: пытаясь понравиться всем, они могут потерять то, что отличает их от остальных, отмечает Э. Ким из SimpleReach. Вместо этого им следует задуматься о том, каким образом читатели будут употреблять контент.

В Washington Post создана специальная команда, которая будет рекомендовать различные версии контента, создаваемые журналистами издания, разным людям, основываясь на информации о том, как они нашли статью, каким устройством они пользуются и даже, если это смартфон, как они его держат.

«Мы ищем другой способ рассказывать, а не просто идеальную форму презентации», – поясняет К. Хайк. Так, людям, которые читают газету со смартфона днем, нужен контент не в той форме, в какой людям, которые сидят дома со своим ноутбуком вечером ***(Социальные сети меняют жизнь новостных сайтов // InternetUA (http://internetua.com/socialnie-seti-menyauat-jizn-novostnih-saitov). – 2014. – 28.10).***

***

Крупнейшая социальная сеть Facebook проводила тестирование функции для администраторов страниц, которая разделяла фанатов на ценных и не имеющих значения.

Тест впервые был замечен читателем Inside Facebook М. Гамба. Пресс-секретарь Facebook подтвердил, что тестирование имело место, но было отменено.

М. Гамба нашел эту функцию в разделе забаненных пользователей в меню настроек страницы. Он мог выбрать из выпадающего меню valuable или irrelevant, но оба варианта привели к нулевым результатам.

Разработчикам социальной сети Facebook стоит внедрить такую функцию, которая показала бы, какие фанаты являются наиболее ценными с точки зрения качества вовлеченности. Администраторы страниц могли бы увидеть, какие фанаты могут быть фальшивыми или низкокачественными – то есть поставившими like только для участия в какой-либо акции.

Facebook давно занимается проблемой фальшивых like. По словам основателя сети М. Цукерберга, команда Facebook нашла способ определять и удалять фальшивые like автоматически ***(Facebook тестировал функцию определения ценности фанатов // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_testiroval_funktsiyu_opredeleniya_tsennosti_fanatov). – 2014. – 28.10).***

***

Около 703 млн пользователей ежедневно заходят в соцсеть Facebook с мобильных устройств – за последний год этот показатель возрос на 39 %. Об этом говорится в сообщении lenta.ru.

Численность ежедневно активной аудитории отражает вовлеченность пользователей – параметр, важный для рекламного бизнеса Facebook. Количество пользователей, которые каждый день заходят в Facebook с мобильных, почти сравнялось с общей ежедневной активной аудиторией сервиса в 864 млн человек. Это отчасти объясняет, почему доля мобильной рекламы в выручке соцсети возросла за год с чуть более чем 40 до 66 %.

Хотя бы раз в месяц соцсетью пользуются 1,35 млрд человек – за последние три месяца аудитория Facebook увеличилась на 30 млн пользователей. Темпы роста числа пользователей Facebook замедляются – последние три квартала соцсеть прибавляла по 40–50 млн новых участников.

Мобильными сервисами соцсети ежемесячно пользуются 1,12 млрд человек – на треть больше, чем годом ранее.

Более активный прирост мобильной аудитории по сравнению с общими показателями играет на руку компании. Развитие мобильных технологий глава Facebook М. Цукерберг называет главным приоритетом соцсети на сегодняшний день. Помимо приложений самой соцсети компания Facebook владеет сервисами WhatsApp и Instagram ***(Ежедневная мобильная аудитория Facebook превысила 700 миллионов // Media бізнес (http://www.mediabusiness.com.ua/content/view/41155/126/lang,ru/). – 2014. – 29.10).***

***

За допомогою створених нідерландським дизайнером Л. Корнет іграшок немовлята можуть завантажувати в соціальні мережі свої фото та відео раніше, ніж навчаться усвідомлено користуватися комп'ютером.

Як пише онлайн-журнал Dezeen, у м'яких іграшках міститься фото- та відеокамера, яка активується за допомогою простих жестів.

Немовля може зняти відео, якщо підніметься в ліжечку, над яким закріплені «розумні» іграшки. Ролик автоматично завантажиться на сторінку Facebook. Якщо ж дитина стисне іграшку-кульку – зробить фото.

Ідея створити таку колекцію виникла в дизайнера після того, як вона помітила, як часто її друзі викладають у соцмережу фото своїх дітей.

За словами дизайнера, для неї було трохи дивним брати участь у житті того, хто цього не усвідомлює. Тому вона розпитала друзів і знайомих, що мотивує їх відображати розвиток своєї дитини у Facebook.

Деякі з батьків активно захищали своє право публікувати фото дітей у соцмережах та повністю контролювати цей процес. Тоді Л. Корнет запитала їх, чи просять вони дозволу у своїх дітей. У відповідь батьки зазначили, що це застереження є слушним.

Дизайнер вважає, що її іграшки дають можливість дитині публікувати свої дописи в соцмережі самостійно ***(Нідерландська дизайнерка створила іграшки, що дозволяють немовлятам користуватися соцмережами // Телекритика (http://osvita.mediasapiens.ua/material/35922). – 2014. – 30.10).***

***

Генеральный директор социальной сети Facebook М. Цукерберг сообщил, что пока не собирается разрабатывать собственную платежную систему. На сегодняшний день для обеспечения потребностей пользователей достаточно сотрудничества с банками и платежным сервисом PayPal.

В последнее время в СМИ периодически появлялась информация о том, что крупнейшая в мире соцсеть планирует выход на рынок платежей и занимается тестированием кнопки «купить», интегрированной в интерфейс сайта. Кроме того, предполагалось, что Facebook запустит сервис P2P платежей на основе своего сервиса отправки сообщений.

«Вместо того, чтобы конкурировать с другими платежными приложениями, мы предпочитаем предоставлять пользователям социальной сети возможность легко и быстро совершать платежи прямо из аккаунта в Facebook», – прокомментировал М. Цукерберг ***(Facebook не будет создавать свою платежную систему // IT Expert (http://itexpert.org.ua/rubrikator/item/39133-facebook-ne-budet-sozdavat-svoyu-platezhnuyu-sistemu.html). – 2014. – 30.10).***

***

Не так давно Twitter запустил аудиокарточки, позволяя прослушивать музыку из сообщений без отрыва от чтения других твитов. Подобная функциональность вскоре появится и для видео. Пользователи смогут просматривать ролики, продолжая листать ленту твитов в приложениях для iOS и Android.

У пользователя будут две возможности. Он сможет просматривать видео в приложении в полноэкранном режиме либо в небольшом окошке. Примерно также фоновый просмотр видео реализован в последних версиях приложения YouTube для iOS и Android.

Таким образом, Twitter хочет способствовать более активному потреблению пользователями мультимедийного контента. Теперь человеку не обязательно бросать свои дела – он может фоново слушать ролик, наблюдая за происходящим, и одновременно постить твиты или читать ленту. Эксперты полагают, что это позволит Twitter реализовать видеорекламу, наконец-то сделав соцсеть прибыльной ***(В Twitter появится режим «видео поверх ленты» // InternetUA (http://internetua.com/v-Twitter-poyavitsya-rejim--video-poverh-lenti). – 2014. – 30.10).***

***

Соцсеть Twitter разработала новое приложение Samaritans Radar, которое выявляет потенциальных самоубийц среди пользователей, сообщает The Guardian.

Онлайн-сервис анализирует сообщения пользователей Twitter. Если среди твитов «тревожные посты», то зарегистрированным в Samaritans Radar друзьям автора этих записей отправляются сообщения с предупреждением и советами, как себя вести в данной ситуации. Сервис реагирует на такие фразы, как «устал быть один», «ненавижу себя», «депрессия», «помогите мне».

Программа пока не способна отличать серьезные твиты от шуточных.

«Приложение не очень хорошо разбирается в сарказме и плохо понимает юмор. В дальнейшем сервис будет усовершенствован», – пишут разработчики.

Предполагается, что пользователи будут сообщать о случаях ложной тревоги и это поможет улучшить работу приложения.

Пока сервис работает только для англоязычных пользователей ***(Twitter начал вычислять самоубийц // IT Expert (http://itexpert.org.ua/rubrikator/item/39107-twitter-nachal-vychislyat-samoubijts.html). – 2014. – 30.10).***

***

Крупнейшая в мире социальная сеть Facebook разрешила доступ к своим сервисам через защищенную сеть Tor. Об этом сообщается в официальном блоге Facebook.

Tor обеспечивает анонимное сетевое соединение, исключающее перехват данных и идентификацию пользователей посторонними. Анонимность трафика достигается за счет распределенной сети серверов. Каждый запрос пользователя проходит через три случайных сервера, за счет чего исключается возможность связать его личность с сайтом, который он посещает, либо контентом, который он отправляет и получает.

Пользователи защищенного браузера Onion – ключевой разработки проекта Tor – смогут заходить в Facebook по ссылке https://facebookcorewwwi.onion. По словам разработчика Facebook А. Маффета, пользователи Tor будут напрямую взаимодействовать с серверами соцсети, минуя локальные буферы.

«Адрес Facebook для браузера Onion позволяет работать с соцсетью через Tor, не теряя криптографической защиты, которую обеспечивает Tor. Для нас важно предоставлять людям инструменты для безопасного использования нашего сайта», – отметил А. Маффет.

Пользователи и ранее могли использовать Tor для захода на Facebook.com, однако при этом они сталкивались с рядом проблем. Одной из наиболее типичных – был запрет на доступ к аккаунту из-за переадресации трафика на сервера в разных странах мира – Facebook воспринимал вход в аккаунт через такое соединение как попытку взлома. Однако теперь пользователи могут спокойно регистрироваться на Facebook и входить в свой аккаунт при подключении через Tor.

По замыслу разработчиков, возможность использовать Facebook через Tor затруднит для хакеров, кибершпионов или представителей власти как выяснение самого факта использования соцсети, так и перехват загружаемых или скачиваемых данных ***(Facebook разрешила доступ к своим сервисам через защищенную сеть Tor // InternetUA (http://internetua.com/Facebook-razreshila-dostup-k-svoim-servisam-cserez-zasxisxennuua-set-Tor). – 2014. – 1.11).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

В Украине идет война, и хотя территория боевых действий ограничена восточными регионами, она влияет и на жителей мирной части страны. Особенно, в Интернете. Только за период с марта по октябрь 2014 г. украинские интернет-пользователи стали вдвое более милитаризованными – возросла их активность на специализированных военных форумах, они все чаще используют военную лексику в соцсетях, пишут все больше постов о войне. Таковы результаты исследования, проведенного Центром медиакоммуникаций «Нова Україна» совместно с интернет-изданием «Телекритика», пишет AIN.UA (http://ain.ua/2014/10/28/547278).

С марта по октябрь почти вдвое возросло количество ежедневных постов на форумах, посвященных оружию, выживанию в условиях войны, военной подготовке (всего было проанализировано 16 самых активных и популярных форумов). Если в начале марта среднее количество постов в день составляло 288, то в конце октябре эта цифра возросла до 552 постов. Причем увеличение происходило скачками – порой количество постов о войне достигало почти тысячи в день.

Любопытно, что при этом сильно снизилась активность на реконструкторских форумах, форумах про страйкбол и пейнтбол, которые были очень оживлены в апреле, перед началом АТО. Количество ежедневных постов на таких форумах уменьшилось с 412 до 127. Аналитики допускают, что часть аудитории начала участвовать в боевых действиях, кроме того, люди стали больше интересоваться настоящим оружием и военной подготовкой, чем военными играми.

Также в ходе исследования были проанализированы 13 млн постов в социальных сетях Facebook, «ВКонтакте», Twitter и LiveJournal в украинском сегменте Интернета на предмет военной лексики в постах. В результате аналитики составили словарь военной лексики, в который вошло около 80 наиболее часто употребляемых слов.

Топ-9 самых популярных военных слов в украинском сегменте соцсетей по состоянию на 1 сентября

бомбить/бомбардировки – 7500 применений
танк – 5800 применений
БТР – 5200 применений
артиллерия/пушки – 5100 применений
хранилище – 2600 применений
миномет – 2500 применений
калаш/АК/автомат Калашникова – 2100 применений
бронік/бронежилеты – 1500 применений
котел – 1100 применений

Если в марте в соцсетях каждая публикация содержала 1,72 таких слов, то уже в октябре эта цифра составила 2,85 слова. Кроме того, самих постов на военную тематику стало в два раза больше: около 28 400 в день в начале сентября, но уже 54 000 – в октябре.

Ранее на AIN.UA выходило исследование Ericsson ConsumerLab, в котором сравнивались интересы украинских, российских, американских интернет-пользователей, а также жителей других стран. В целом то, для чего люди используют Интернет, почти не отличается, в какой бы точке мира не находился человек. Преимущественно это соцсети и веб-серфинг ***(Как растет «милитаризация» украинских интернет-пользователей // AIN.UA (http://ain.ua/2014/10/28/547278). – 2014. – 28.10).***

***

Політики використовували своїх дописувачів у соцмережах під час передвиборної кампанії. Про це під час прес-конференції сказав експерт з комунікацій у соціальних мережах Центру підтримки молодіжних ініціатив «Євромолодь» І. Омелян. Приблизно витрачено від 1 до 2 млн дол. усіма політичними партіями на рекламу та просування в соціальних мережах, а також політичними кандидатами, пише chernivtsi.ws.

Окрім того, він зазначив, що під час виборчої кампанії партії активно використовували думки своїх лідерів у соцмережах. Наприклад, «Народний фронт» активно використовував сторінки А. Авакова та А. Яценюка.

Для прикладу у Яценюка 289 тис. дописувачів у Facebook і 251 тис. у Twitter.

Це півмільйона людей, які мають контакт із кожним інформаційним меседжем, який надсилав Прем'єр-міністр. Вони правильно використали стратегію контексту. Бо в кінці, коли ми зрозуміли, що Прем'єр-міністр має залишитись, суспільство було підготовлене, що коней на переправі не змінюють, вважає експерт.

А ось активність П. Порошенка в соціальних мережах, на думку експерта, на цих виборах порівняно з президентськими зменшилася на 30 %. Більша активність спостерігалася тільки на власній сторінці Президента у Facebook (263 тис. дописувачів).

Партія «Самопоміч» також вміло спілкувалась зі своїм електоратом у соціальних мережах (76 тис. дописувачів). А лідер Радикальної партії О. Ляшко активно використовував «образ воїна», особливо у мережі YouTube (200 тис. дописувачів) та в «ВКонтакте» ***(Політики використовували своїх дописувачів у соцмережах під час передвиборчої кампанії // Чернівці Таймс (http://times.cv.ua/2014/10/29/polityky-vykorystovuvaly-svojih-dopysuvachiv-u-sotsmerezhah-pid-chas-peredvyborchoji-kampaniji/). – 2014. – 29.10).***

Социальные медиа-маркетологи отказываются от использования YouTube для видеоконтента в пользу Facebook. К такому выводу пришли специалисты компании Socialbakers, проанализировав более 180 тыс. Facebook видеосообщений на 20 тыс. страниц Facebook.

В 2012 г. маркетологи даже не рассматривали вариант размещения видео на Facebook. Стандартный процесс для создания видео состоял из публикации его на YouTube, а затем размещения в Facebook. В последнее время тенденция изменилась: контент-маркетологи загружают видеоконтент непосредственно на Facebook. Это означает, что Facebook отбирает трафик у YouTube.

В начале 2014 г. количество видеосообщений YouTube почти в два раза превышало аналогичный показатель его ближайшего соперника. Однако позднее контент-маркетологи предпочли загрузку видео-файлов непосредственно на Facebook, количество таких видеосообщений с мая по июль увеличилось на 50 % и к концу года может превзойти YouTube.

Это серьезная угроза для YouTube, так как маркетологи собираются продолжать использовать сеть, которая обеспечит наиболее эффективную вовлеченность. В настоящее время нет никаких признаков изменения текущей тенденции.

Так как Facebook неизменно проигрывает YouTube в плане увеличения просмотров и вовлеченности, контент маркетологи отреагировали и перешли к нативному видео Facebook.

Месяцем ранее стало известно, что Facebook планирует внедрить рекламу в видеоконтент. Удачная реализация планов социальной сети может подорвать господство YouTube на рынке видеорекламы. Однако существуют сомнения в том, захотят ли пользователи Facebook видеть в начале видео-роликов рекламные объявления. Сейчас представители соцсети и создатели видеоконтента обсуждают, как реклама может быть включена в видео. Вполне вероятно, что какой-то вид рекламной продукции будет развернут уже к концу года ***(Создатели контента переходят из YouTube на Facebook // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/sozdateli_kontenta_perehodyat_iz_youtube_na_facebook). – 2014. – 22.10).***

***

Если вы активно работаете с аудиторией социальных сетей, предлагаем подборку актуальных исследований на тему того, как люди используют соцмедиа и какие особенности поведения и принятия решений при этом можно увидеть у «поколения Facebook», пишет Marketing Media Review (http://mmr.ua/news/id/socialnye-media-7-issledovanij-v-pomosch-marketologam-41789/).

В данной подборке представлены лишь семь исследований, но каждое из них отражает какую-то характерную особенность поведения потребителей, которая будет полезна специалистам по маркетингу в построении рекламных кампаний для соцсетей.

1. Смена точки зрения после публикации записей в соцсетях или постов в блоге.

Чувство сомнения перед публикацией своих мыслей или наблюдений в социальных сетях знакомо многим пользователям. Зачастую это приводит не только к редактированию постов и статусов уже после публикации, но и к полному отказу от первоначальных намерений.

Пара исследователей в Facebook провели исследование явления самоцензуры у пользователей (когда написанные посты так и не публикуются).

За период в 17 дней они отследили онлайн-активность в соцсети более чем 3,9 млн человек. 71 % исследуемых за период наблюдений написали по меньшей мере один статус или комментарий, публикацию которого затем отменили или удалили его. В среднем точка зрения «публиковать / не публиковать» изменилась для чуть более чем четырех статусов и трех комментариев.

По мнению исследователей, склонность пользователей к самоконтролю и самоцензуре растёт по мере того как им становится труднее определить, кто на самом деле их читатели / подписчики в соцсетях. По мере роста гендерной и социальной диверсификации аудитории подписчиков всё чаще человек решает не писать вообще ничего в соцсети, боясь, что его публикация кого-то заденет, оскорбит или может быть неправильно расценена.

Урок для маркетолога: Общение с целевой аудиторией (ЦА) в соцсетях надо строить так, чтобы знать, «чем дышат» люди, подписавшиеся на страницу бренда. Тогда не придётся публиковать «ванильно-нейтральные» посты и статусы «ни о чём».

2. Онлайн-эмоции крайне «заразны».

О том, что эмоциональное состояние и настроение могут передаваться от человека к человеку в относительно закрытой социальной группе, хорошо всем известно (если говорить об офлайн-сообществах). Но не так давно было проведено крупное исследование этого же феномена в соцсетях.

Соавторами работы выступили ученые из Калифорнийского университета и Медицинского колледжа в Сан-Диего, США. Для работы они использовали специальное ПО, которое помогло им проанализировать около миллиарда записей в соцсети Facebook за период более двух лет. Отдельное внимание программа уделяла публикациям в ненастные дни (дождь, ветер), когда частота негативно окрашенных постов резко возрастает.

Сопоставив данные метеослужб и статусы пользователей в социальной сети, исследователи установили, что негативно окрашенное эмоциональное состояние начинало распространяться даже на тех пользователей и регионы,

где в тот момент с погодой всё было в порядке. Недавно результаты «погодного эксперимента» подтвердились ещё раз.

Но не только негатив оказался «заразен» в соцмедиа. Положительные эмоции также распространялись похожим образом, а эффект от них в соцсетях оказался более стойким и продолжительным.

Урок для маркетолога: Умение использовать «эффект эмоциональной волны» позволяет бренду долгое время сохранять положительное впечатление о себе (отсюда и появились все эти «котики» и пожелания «хорошего дня» по утрам).

3. Фото на аватарке формирует эмоциональное восприятие ещё до того, как вас начнут читать.

О том, что «принимают по одёжке» знают все. В соцсетях «встречают» ещё и по выражению лица на аватарке. Недавнее исследование, опубликованное в издании Psychological Science, демонстрирует, что решение об отношении к незнакомому человеку наш мозг принимает за 40 миллисекунд.

В ходе исследования использовались фотографии, сделанные при одном и том же уровне освещённости, но со слегка различными выражениями лица. Результаты доверия / недоверия к незнакомцам распределились в пользу фотографий с проявлением позитивных эмоций на лице. Урок для маркетолога: Выбор фотографий для менеджеров и представителей компании в социальных сетях должен базироваться на таком же A/B тестировании, как при выборе внешнего вида для сайта или общего дизайна для страниц компании в социальных сетях.

4. Публикация новых постов происходит выборочно, характер выбора между «публиковать / не публиковать» отличается в разных странах.

Около четверти пользователей в соцсетях публикуют «всё подряд» или «почти всё», что видят: таковы результаты исследования от маркетингово-аналитической компании Ipsos.

19 % пользователей вообще не публикуют ничего нового в сети. При этом процент тех, кто публикует много контента в своем профиле, отличается в разных странах.

Издание The Washington Post заметило чёткую взаимосвязь между уровнем проникновения Интернета и избыточностью публикаций в сети. Основные «потоки» избыточного контента приходятся на Европу и технологически развитые страны, в то время как Африка, Латинская Америка и часть стран Азии создают мало контента из-за технических ограничений и недостаточного развития скоростного доступа к сети.

Урок для маркетолога: При создании контент-стратегии для соцсетей учитывайте особенности публикации и потребления контента в конкретных странах, что позволит вам избежать проблем с недостаточным охватом целевой аудитории в пределах желаемого целевого рынка.

5. Социальность и «обратная связь» – не просто пустой звук.

Исследование доктора С. Тобин из Университета Квинсленда показывает, что использование соцсетей даёт членам сообщества ощущение большей «связанности» между собой.

В рамках эксперимента одной из групп было предложено просто просматривать статусы друзей в соцсети, в то время как вторая группа продолжала публиковать контент от своего имени без ограничений. По завершению периода для тестов группа, которая два дня могла только просматривать, но не комментировать и ничего не могла писать от своего имени, сообщила, что почувствовала ухудшение эмоционального состояния по сравнению с теми, кто мог активно участвовать в «социальной жизни».

Урок для маркетолога: «Фидбек» и все формы общения с представителями компании и между самими потребителями крайне важны для сохранения положительного эмоционального фона и формирования стойкого ощущения «общины» в сети. Бренд, который просто «вещает» или просто «слушает», но ничего не предлагает взамен, вызывает глухое раздражение.

6. Контент, который вызывает сильные эмоции (счастье, ярость, ужас, негодование), пользователи публикуют повторно в несколько раз чаще любого другого.

Эмоции – одна из ключевых основ современного маркетинга. В очередной раз этот тезис подтверждает исследование Й. Бергера. По его результатам, эмоциональный подъём накапливается в нервной системе человека и требует «выхода». В соцсетях (да и вообще в Интернете) таким «выходом» становится повторная публикация контента, который вызвал ту или иную эмоцию (так называемый «шэринг»).

Эксперимент с видеоклипами, которые не вызывали никаких особенных эмоций, и теми, которые вызывали ярость, страх или чрезмерное умиление, показал, что эмоционально сильный контент участники исследования публиковали повторно для того, чтобы друзья и подписчики тоже увидели этот контент. То же самое происходило и с текстовым контентом.

Урок для маркетолога: Вовлечение возможно только при наличии эмоциональной составляющей.

7. Лимбическая система и проблема oversharing.

Oversharing (публикация избыточного количества контента в социальных медиа) – одно из типичных явлений современности. По данным нейрофизиологов из Гарвардского университета, процесс «овершэринга» затрагивает в человеческом мозгу те же центры активности и процессы получения удовольствия, что и потребление еды, получение денег или секс.

Другие эксперименты показали, что участники готовы даже отказаться от денежного вознаграждения за участие в исследовании, если им просто дадут возможность много рассказывать о себе.

Похожие процессы происходят и в социальных медиа: не менее 80 % постов в соцсетях посвящены лично пережитому опыту.

Урок для маркетолога: Один из основных стимуляторов потребительского интереса – возможность рассказывать о себе и о своём личном опыте, полученном благодаря бренду или вместе с ним. Рассказывать истории о себе должны не вы сами, а ваши клиенты ***(Социальные медиа: 7 исследований в помощь маркетологам // Marketing Media Review (http://mmr.ua/news/id/socialnye-media-7-issledovanij-v-pomosch-marketologam-41789/). – 2014. – 22.10).***

***

Социальная сеть Twitter официально запустит свою кнопку «Купить» для всех организаций в I квартале 2015 г.

Кнопка, позволяющая совершать покупки непосредственно в Twitter-ленте, начала проходить тестирование в прошлом месяце. Первыми испытать ее функциональность могли некоторые предприятия, знаменитости и некоммерческие организации. Кнопка, доступная при просмотре с помощью мобильного устройства, позволяет совершить покупку или пожертвование прямо в сообщении Twitter, пишет Marketing Media Review (http://mmr.ua/news/id/delat-pokupki-v-twitter-mozhno-budet-s-2015-goda-41785/).

Ранее компания заявляла, что она планирует постепенно добавлять большее количество организаций к тем, кому доступен функционал новой кнопки. Однако не было точно известно, когда сервис станет доступен всем пользователям ***(Делать покупки в Twitter можно будет с 2015 года // Marketing Media Review (http://mmr.ua/news/id/delat-pokupki-v-twitter-mozhno-budet-s-2015-goda-41785/). – 2014. – 22.10).***

***

Выручка «ВКонтакте» в III квартале 2014 г. возросла на 6,7 % по сравнению с аналогичным периодом прошлого года и составила 968 млн р. Об этом говорится в сообщении единственного собственника сети Mail.Ru Group, пишет lenta.ru

За девять месяцев 2014 г. выручка социальной сети составила 2,971 млрд р., увеличившись на 9 % за год.

Приобретение компанией «ВКонтакте» было завершено 16 сентября 2014 г., однако в финансовой отчетности Mail.Ru соцсеть будет консолидирована, начиная с 30 сентября. В связи с этим в финансовые показатели компании за III квартал представлены без учета выручки «ВКонтакте», отмечается в сообщении ***(Выручка «ВКонтакте» в третьем квартале возросла до 968 миллионов рублей // Media бізнес (http://www.mediabusiness.com.ua/content/view/41084/126/lang,ru/). – 2014. – 23.10).***

***

Американская компания Twitter Inc., которой принадлежит одноименная сеть микроблогов, увеличила чистый убыток в III квартале в 2,7 раза, несмотря на возросшую более чем вдвое выручку.

Как сообщается в пресс-релизе компании, чистый убыток в июле – сентябре составил 175,464 млн дол., или 29 центов в расчете на акцию, по сравнению с 64,601 млн дол., или 48 центов на акцию, за аналогичный период прошлого года. При этом количество находящихся в обращении бумаг компании возросло почти в пять раз.

Без учета разовых факторов Twitter вышел в минувшем квартале на прибыльный уровень, получив 1 цент на акцию, в то время как годом ранее был зафиксирован убыток в 13 центов.

Выручка в минувшем квартале подскочила до 361,266 млн с 168,58 млн дол. за тот же период прошлого года. Собственный прогноз компании для этого показателя, сделанный в июле, составлял 330–340 млн дол.

Опрошенные FactSet аналитики в среднем оценивали скорректированную прибыль Twitter на уровне 1 цент на акцию при выручке в 351 млн дол.

Количество активных пользователей Twitter (активность учетной записи не реже раза в месяц) по данным на 30 сентября достигло 284 млн человек, что на 23 % превышает показатель на ту же дату прошлого года и на 4,8 % больше уровня на конец II квартала этого года, сообщается в отчетности.

Эксперты ждали подъема до 280–288 млн. Однако темпы повышения показателя в годовом выражении продолжают замедляться: в апреле – июне рост составлял 24 %, в январе – марте – 25 %, а в октябре – декабре прошлого года – 30 %.

По итогам IV квартала Twitter планирует получить выручку в диапазоне 440-450 млн дол. при консенсус-прогнозе аналитиков на уровне 448 млн дол. Выручка по итогам всего 2014 г., по оценкам компании, составит от 1,365 млрд до 1,375 млрд дол.

Котировки акций Twitter в ходе электронных торгов 27 октября упали почти на 10 % после опубликования отчетности. Капитализация компании с начала текущего года сократилась на 24 % ***(Twitter увеличил чистый убыток в 2,7 раза // Finance.Ua (http://news.finance.ua/ru/news/~/337242). – 2014. – 28.10).***

***

YouTube планує ввести можливість платної підписки, що дає можливість програвати ролики без реклами, повідомила гендиректор відеосервісу С. Вожіцкі, повідомляється на порталі організаторів заходу Re/code, пише Корреспондент.net

(http://ua.korrespondent.net/business/web/3437483-YouTube-vvede-platu-za-perehliad-videorolykiv-bez-reklamy).

«Такий крок надасть користувачам більше вибору між різними варіантами споживання відеоконтенту, тим більше, що в нинішній час все частіше люди дивляться відео саме через додатки на мобільних пристроях», – зазначила С. Вожіцкі.

Подібний механізм наразі працює в мобільних додатках: користувач або може завантажити безкоштовний сервіс або гру на свій пристрій з показом реклами, або заплатити невелику суму за версію без рекламних оголошень. Наразі, за словами С. Вожіцкі, компанія думає над тим, як можна реалізувати цю ідею на YouTube.

Про плани YouTube щодо створення музичного онлайн-сервісу, який доповнить основний відеохостинг, стало відомо в червні цього року. Він називатиметься YouTube Music Key, а плата за користування ним становитиме 10 дол. на місяць ***(YouTube введе плату за перегляд відеороликів без реклами // Корреспондент.net (http://ua.korrespondent.net/business/web/3437483-YouTube-vvede-platu-za-perehliad-videorolykiv-bez-reklamy). – 2014. – 28.10).***

***

Объем чистой прибыли американской компании Facebook Inc., которой принадлежит крупнейшая в мире социальная сеть, возрос в июле – сентябре вдвое. Данные показатели превзошли средний прогноз экономистов. Чистая прибыль в III квартале составила 806 млн дол. по сравнению с 425 млн дол., зафиксированными за тот же период 2013 г., сообщается в пресс-релизе Facebook. Выручка возросла примерно на 60 % – до 3,203 млрд дол. против 2,016 млрд дол. в 2013 г., пишет MIGnews.com.ua (http://mignews.com.ua/biznes/4069853.html).

Ранее экономисты в среднем прогнозировали скорректированную прибыль на уровне 40 центов на акцию при выручке в 3,12 млрд дол.

Число активных пользователей социальной сети (активность учетной записи не реже раза в месяц) на конец прошлого квартала составляло 1,35 млрд по сравнению с 1,32 млрд в апреле – июне и 1,19 млрд в конце сентября прошлого года.

Количество пользователей, заходящих в свой аккаунт ежедневно, тем самым формируя дополнительный поток выручки для Facebook, увеличилось в среднем до 864 млн по сравнению с 829 млн во II квартале этого года и 728 млн в III квартале 2013 г.

На рекламу на мобильных устройствах приходится примерно 66 % от общей рекламной выручки компании относительно 62 % во II квартале 2014 г. и 49 % в июле – сентябре прошлого года.

В текущем квартале Facebook намерен повысить выручку на 40–47 % по сравнению с аналогичным периодом 2013 г. – до 3,6–3,8 млрд дол.

(Прибыль Facebook увеличилась почти вдвое // MIGnews.com.ua (http://mignews.com.ua/biznes/4069853.html). – 2014. – 29.10).

***

«ВКонтакте» официально запустил мобильную рекламу.

Пока что рекламодателям доступна реклама приложений из Google Play и App Store, которую увидят пользователи Android и iOS-устройств соответственно. В дальнейшем число мобильных платформ и перечень допустимых к рекламе товаров и услуг увеличится, пишет Marketing Media Review (http://mmr.ua/news/id/vkontakte-zapustil-mobilnuju-reklamu-41876/).

Особенности нового формата рекламы:

- Пользователи видят мобильные объявления в новостной ленте мобильной версии сайта или поддерживаемых мобильных клиентов.
- В настройках таргетинга нет возможности выбрать платформу устройств, пользователям которых будет показана реклама. Она определяется автоматически, исходя из адреса указанного рекламодателем приложения.
- Для мобильных рекламных объявлений доступны все настройки целевой аудитории таргетированных объявлений компьютерной версии сайта. Исключение составляют используемые операционные системы, мобильные устройства и браузеры. Эти настройки устанавливаются автоматически на основе заданной ссылки рекламируемого приложения.
- Для мобильных рекламных объявлений доступен только способ оплаты за показы (настоятельно рекомендуется задать стоимость 1000 показов). Также есть возможность ограничения числа показов объявления 100 показами на одного человека.
- Новый формат уже поддерживает большинство сервисов мобильной аналитики: MAT, AppsFlyer, Adjust, AD-X, Kochava, Flurry и Apperkot ***(«ВКонтакте» запустил мобильную рекламу // Marketing Media Review (http://mmr.ua/news/id/vkontakte-zapustil-mobilnuju-reklamu-41876/). – 2014. – 28.10).***

***

Facebook внес некоторые изменения в процесс получения доступа к Ads API разработчиками. Нововведение призвано расширить возможности для построения более инновационных инструментов объявлений.

В настоящее время существует три уровня доступа: Development, Basic и Standard. Начальный уровень разработки (Development) позволяет тщательно исследовать API и тестировать приложения на платформе Facebook. Базовый уровень (Basic) позволяет осуществлять тест, вносить итерации и строить приложения с количеством внешних аккаунтов до 25. Стандартный уровень (Standard) позволяет использовать неограниченное количество аккаунтов для масштабирования приложения. При этом разработчики могут быть номинированы как Маркетинговые партнеры Facebook (новое название для PMDs).

«Начальный и основной уровни доступа добавляются к существующему стандартному уровню доступа к Ads API, что позволяет начинающим разработчикам внедрять инновации быстрее в этих новых областях, – говорит А. Кулькарни в блоге Facebook. – Новые разработчики, которые хотят изучить FB Ads API и попытаться строить новые инструменты, теперь могут начать работу в Ads API с начальным доступом и, когда будут готовы, подать заявку на доступ к основному и стандартному уровню по мере необходимости».

Новые уровни доступа не влияют на разработчиков Ads API, уже имеющих самый высокий уровень доступа. «Разнообразие в нашей экосистеме Ads API поможет привлечь больше инноваций и расширить возможности платформы Facebook», – отмечает А. Кулькарни ***(Facebook добавляет уровни доступа к Ads API // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_dobavlyaet_urovni_dostupa_k_ads_api). – 2014. – 29.10).***

***

Компании IBM и Twitter заключили партнерство в сфере обработки больших объемов данных, чтобы помочь бизнес-организациям предсказывать рыночные тенденции на основе информации из твитов. Об этом говорится в сообщении IBM, пишет lenta.ru

IBM, известная технологическими разработками в области анализа big data, обучит около 10 тыс. сотрудников тому, как консультировать компании по использованию данных Twitter для принятия бизнес-решений. По замыслу компании, на основе сообщений-твитов со всего мира можно предугадывать рыночные тенденции и анализировать отношение пользователей к тому или иному продукту или бренду.

Корпоративные клиенты компании смогут фильтровать данные по географическому признаку, публичным персональным данным и эмоциям, выраженным в сообщении. Услуга будет доступна клиентам IBM, пользующимся ее «облачными» аналитическими сервисами, а также разработчикам ПО на базе облачных платформ Bluemix и Watson Developer Cloud.

«Мы видим объединение старой и новой технологических компаний. Это уже вторая подобная сделка, анонсированная IBM за последние месяцы. IBM понимает, что у нее нет ответов на все вопросы ее клиентов, тогда как многие другие компании обладают активами, которые отвечают этим запросам», – сказал агентству Reuters аналитик из S&P Capital IQ С. Кесслер.

Ранее Twitter уже предоставлял сторонним компаниям, включая Gnip, Datasift и Dataminr, доступ к архиву своих твитов, который те могли перепродавать своим клиентам. В апреле Twitter купила компанию Gnip, которая предоставляла клиентам пакеты из 50 % или 10 % всех публикуемых на Twitter публичных записей за определенный период либо только сообщения-твиты с упоминанием определенной компании или продукта.

Имея эти данные, заказчик может проанализировать интерес аудитории к своим действиям либо выявить всплески в обсуждениях ***(IBM и Twitter помогут бизнесу предугадывать рыночные тенденции // InternetUA (http://www.mediabusiness.com.ua/content/view/41171/126/lang,ru/). – 2014. – 30.10).***

***

Если вы используете Facebook для продвижения бизнеса, то наверняка стараетесь изо всех сил, чтобы ваши посты заметили пользователи. Сделать это не так легко. Чем же «зацепить» целевую аудиторию? Практические рекомендации дают обозреватели Socialmediaexaminer.

1. Утром лайки – вечером спецпредложения.

Допустим, что вашей странице не хватает лайков и вы думаете о том, где их взять. Есть простое решение – попросите об этом пользователей и обязательно дайте им стимул это сделать.

Именно так и поступила сеть ресторанов Subway, предложившая подписчикам следующие условия: если определенный пост наберет 40 тыс. лайков, компания выпустит промо-код к рекламной кампании, участники которой получат возможность выиграть угощение бесплатными гамбургерами в течение года.

На этот пост Subway затратили минимум усилий, а те, что были, окупились сполна. Запись набрала более 60 тыс. лайков, более 800 комментариев и более 1500 репостов. Это довольно неплохой вирусный эффект для одного поста.

Итак, если вы придумали достойную промо-идею, которую решили раскрутить с помощью поста, запомните несколько ключевых пунктов.

Сделайте свой пост эстетичным

Помните – промо-фото должно манить потребителя.

Напишите ваше предложение прямо на изображении

Люди, прокручивающие ленту новостей на Facebook, не всегда читают тексты в самих постах. Поэтому помещайте предложение, написанное крупным шрифтом, в верхней части изображения. Это поможет привлечь тех пользователей, которые привыкли не обращать внимания на текст.

Не бойтесь просить о чем-либо! А для этого создавайте привлекательный и четкий призыв к действию!

2. Больше ретро!

Люди любят вещи, так или иначе связанные с их юностью. Склонные к ностальгии пользователи охотнее просматривают фото, участвуют в опросах и занимаются другими вещами, которые связаны с разными приятными воспоминаниями. Благодаря именно таким пользователям ролики на YouTube с музыкальными клипами 80-х и 90-х годов и получают сегодня трафик и комментарии.

Именно для ценителей ретро производитель напитков Gatorade и визуализировал хронологию изменения формы своих бутылок. Специально для такой аудитории был разработан и хэштег – #TransformationTuesday.

Сведения о том, когда появилась первая бутылка с Gatorade и какой формы она была, может пригодиться в самый неожиданный момент. Например, сидя в кафе со своими друзьями всегда можно как бы невзначай вспомнить о том, что первый такой напиток выпустили аж в 1965 г.

Если вы решили прибегнуть к визуальному сторителлингу и представить историю продукта или бренда, то помните вот о чем...

Выбирайте тщательно

Если вы показываете эволюцию вашего продукта, то выбирайте наиболее знаковые моменты этого процесса. За мгновение Gatorade демонстрирует разные варианты дизайна бутылок. Это напоминает потребителю о разнообразии продукции и широком выборе.

Все должно соответствовать друг другу

Gatorade показывает развитие своего продукта в рамках одного аромата – лимон-лайма, словно «окрашивая» в него историю компании. Бутылки выстроились по росту и показывают, что средняя высота тары всегда оставалась примерно на одном и том же уровне.

Создайте и используйте собственный хэштег (или мем)

#ThrowbackThursday – популярный хэштег, под которым различные компании и пользователи выкладывают фото «из прошлого». Что касается Gatorade, то по аналогии с данным хэштегом компания создала в Facebook собственный – #TransformationTuesday.

Пример поста с хэштегом #ThrowbackThursday от компании L.L.Bean. Популярность таких сообщений выше, чем у обычных постов из хроники.

3. Отдых – наше все.

Если вы действительно хотите предложить своим подписчикам на Facebook чего-нибудь веселого и расслабляющего, то дайте им картинки с соответствующим содержанием. Причем каких-либо людей на них быть не должно! Такие броские сообщения отлично работают, причем в ряде случаев в них даже не нужно говорить о продукте.

По такому принципу и сделала пост компания Hollister, выпускающая пляжную одежду. Пост с изображением пляжа получил более 32 тыс. лайков, более 300 комментариев и около 500 расшариваний. А ведь одежды от Hollister на картинке нет!

Вот несколько вещей, о которых стоит знать, используя эту тактику.

Задавайте клиентам открытые вопросы

Вопросы помогут получить от пользователей комментарии, что является куда более ценной «валютой», чем лайки. Спросите, например, «что для вас значит отпуск весной?». Большинство людей обязательно вспомнят какую-нибудь связанную с отдыхом историю и с удовольствием поделятся ей.

Краткость – сестра таланта. Поместите простой текст на картинку

Хорошие вещи часто комбинируются, например, «Горячее солнце, Теплый песок. Весенние каникулы». Потенциальные покупатели могут и не отдыхать в данный момент, однако они явно ностальгируют по прошедшему отпуску или мечтают о запланированной поездке на курорт. Так что для передачи приятных моментов используйте несколько коротких и ёмких фраз.

Одним словом помните, что не каждый ваш пост должен быть обязательно о вашем продукте. Уделите время творчеству!

4. Всегда будьте в курсе всего

В мире постоянно что-нибудь происходит, начиная от спортивных соревнований и заканчивая реалити-шоу. Используйте тактику «угнанной новости» – как-нибудь привязывайте популярное событие к рекламируемому бренду.

В конце одного из сезонов American Idol телекоммуникационная компания AT & T спросила у зрителей, за кого из участников они голосовали. Пост получил более 26,5 тыс. лайков, более 1 тыс. перепостов и свыше 15 тыс. комментариев.

Бренд AT & T воспользовался популярностью American Idol у пользователей социальных сетей и на основе этого напомнил о себе. И вот что нужно иметь в виду, если вы собираетесь поступить аналогичным образом.

Не спрашивайте – направляйте

Вы хотите, чтобы люди поделились своим мнением в комментариях. Но этим все не должно завершиться. Предложите пользователям пройти по ссылке на сайт, где они действительно могут проголосовать за участника телешоу. Вам не нужно постоянно следить за комментариями, все необходимое за вас сделают пользователи.

Вопросы должны быть к месту и ко времени

Не размещайте пост с вопросами о соревновании или телешоу во время их трансляций или перед ними. Как вариант – сообщение может появиться за час или два до начала события, однако здесь не обойтись без соответствующей подготовки аудитории, в противном случае пользователи не заметят вашу публикацию.

Не вы здесь главный

Спрашивая пользователей о том, кто был их фаворитом в том или ином соревновании или телевизионном шоу, старайтесь не напоминать лишний раз о себе логотипом или информацией о компании. Люди помнят, что это ваша страница и это вы интересуетесь их мнением – этого достаточно. Просто фокусируйтесь на событии и будьте своего рода посредником в море общего энтузиазма.

Вывод очевиден – следите за тем, что происходит в спорте, культуре, общественной жизни. Ищите вещи, которые можно использовать в рамках продвижения вашего бренда, и делайте их частью вашей социальной стратегии ***(4 способа сделать посты на Facebook более популярными // ProstoWeb***

(http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/4_sposoba_sdelat_posty_na_facebook_bolee_populyarnymi). – 2014. – 30.10).

***

Мобильная рекламная платформа Clickky объявила о заключении договора о сотрудничестве с сервисом микроблоггинга Twitter. Теперь у клиентов платформы появилась возможность размещения рекламы приложений в этой социальной сети с оплатой только за установки.

Не так давно Twitter анонсировал свою новую рекламную платформу нативной рекламы, которая необычайно интересна разработчикам мобильных приложений. Платформа предоставляет рекламодателям возможность создания кастомизированных рекламных блоков внутри приложений, расширенные функции таргетинга, детальную статистику по кампаниям, расширение для OpenRTB, инструменты для запуска настройки рекламных кампаний и многое другое.

«Использование рекламы такого формата сводит к минимуму недовольство пользователей, а значит, что рекламодатель может не переживать о плохом имидже для своего приложения, – сообщается в официальном пресс-релизе Clickky. – Новые форматы объявлений, свежая аудитория, точный таргетинг – это то, что сегодня мы предлагаем в рамках сотрудничества с Twitter. Оплата только за установки (CPI)».

Напомним, в июле 2014 г. Clickky представила новую для мобильного рынка CPE-модель рекламных кампаний, где стоимость зависит от количества привлеченных активных пользователей. При такой схеме работы рекламодатель, запустивший кампанию по модели CPE, не платит за пользователей, которые просто кликнули по баннеру или установили и сразу же удалили приложение. Оплата происходит лишь за пользователей, которые действительно заинтересовались приложением. Иными словами, рекламодатель не платит за установки, он платит только за активных пользователей ***(Clickky начала размещение мобильной рекламы в Twitter'е по модели CPI // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/clickky_nachala_razmeschenie_mobilnoy_reklamy_v_twitter_e_po_modeli_cpi). – 2014. – 30.10).***

***

Сервис для размещения фото и коротких видеороликов Instagram начал демонстрировать пользователям видеорекламу в ленте новостей. Об этом сообщает издание AdWeek.

О планах начать продажи рекламы Instagram заявил еще осенью прошлого года. С конца октября 2013 г. у некоторых пользователей в ленте стали отображаться рекламные фотографии от аккаунтов, на которые они не подписаны. Однако еще полтора года назад Instagram запустил публикацию

коротких видеороликов, и вопрос монетизации функции был лишь делом времени.

Видеорекламу, скорее всего, Instagram продает брендам дороже – формат 15-секундного ролика с автопроигрыванием может чуть дольше удерживать внимание пользователя, чем статичная фотография.

В то же время Instagram обещает тщательно подходить к отбору рекламы, чтобы не нарушить сложившуюся субкультуру сервиса. В число первых брендов, размещающих видеорекламу на Instagram, вошли Disney, Lancome, Activision и Banana Republic ***(Instagram начал демонстрировать видеорекламу в ленте новостей // InternetUA (http://internetua.com/Instagram-nacsal-demonstrirovat-videoreklamu-v-lente-novostei). – 2014. – 1.11).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

За останні 25 років Інтернет проникнув майже всюди та надав людству небачені досі можливості для комунікації. Однак у нього є і темні сторони, а саме – майже повсюдне знущання, цькування та залякування користувачів. Це відчував майже кожен відвідувач мережі – від нього страждають 40 % з них.

Окрім того, що 4 з 10 користувачів павутини були жертвами кіберхуліганів, кажуть у компанії Pew Research Center, спостерігає таке цифрове насилля вдвічі більше людей – близько 73 %. Такі дані аналітики отримали під час свого нещодавнього дослідження, у якому взяли участь 2849 людей, завдяки чому воно стало найдетальнішим з дослідження питання кібернасильства. Вони також з’ясували, що найтяжчі форми знущання – фізичні погрози, переслідування та сексуальні домагання – зазвичай випадають на долю жінок.

«Існує досить широкий арсенал для залякування, – каже директор інтернет-департаменту у Pew Research Center Л. Рейні. – І деякі з них дуже жорстокі».

Спеціалісти поділяють онлайн-знущання на дві категорії залежно від їхнього впливу. До першої входять вигадування різних образливих імен та приниження. Другий тип націлений на меншу кількість інтернет-користувачів та містить у собі переслідування, домагання й погрози.

Приклади залякування

Одним з нещодавніх прикладів такого кіберзалякування може дати GamerGate – інтернет-рух, який захищає культуру відеоігор та вимагає відповідальних рецензій та оглядів на профільних веб-ресурсах. Однак його учасники швидко відійшли від первісних цілей та перейшли до жорстоких нападок на журналістів, розробників та інших користувачів.

Більшість з їхніх жертв – жінки, і вони чули на свою адресу жорстокі погрози в зґвалтуванні, вбивстві, зламі їхніх комп'ютерів та публікації всіх персональних відомостей. Щонайменше дві жінки через активність учасників GamerGate та їхні погрози змушені були покинути свої домівки.

Зупинити кібернасилля

Рівень жорстокості в Інтернеті, особливо проти жінок, досить високий, і активісти намагаються це виправити. Одна з них – С. Бейкер, яка започаткувала ініціативу Take Back the Tech для протидії онлайновому насиллю проти жінок. «У нашій роботі ми бачимо, як кіберзнущання позначаються на жертвах в реальному світі, – каже вона. – Неважливо, чи втілились онлайнові погрози в реальності, вони завжди наносять суттєву шкоду».

За даними Pew Research, над жінками знущаються більше за все. Близько 26 % представниць прекрасної статі віком від 18 до 24 років кажуть, що відчували переслідування в онлайні. А 25 % відповіли, що їх сексуально домагалися.

Багато з цього насилля відбувається в соціальних мережах, і тому такі організації, як Take Back the Tech, дають негативні оцінки Facebook, Twitter та YouTube. Вони вважають, що ці ресурси недостатньо працюють для запобігання кіберзнущанню над жінками.

Самі жертви підтверджують, що більше всього насилля відчувають саме в соцмережах – про це повідомили дві третини респондентів. Іншими місцями є розділ коментарів веб-сайтів (22 %), онлайнові ігри (16 %), електронна пошта (16 %), форуми (10 %), а також сайти онлайн-знайомств (6 %) ***(Жорстокий веб: відчув майже кожен // InternetUA (http://internetua.com/jorstokii-veb--v-dcsuv-maije-kojen). – 2014. – 27.10).***

***

Когда происходит землетрясение, его действие больше, чем просто сейсмические волны. Экстремальные явления, такие как землетрясения, цунами и террористические акты, также порождают волны непосредственных онлайновых социальных взаимодействий в виде твитов, которые предлагают взглянуть на само событие и на более широкие вопросы о том, как сообщества людей реагируют на катастрофы.

В статье «Саинтифик Репотс» постдокторант К. Брелсфорд и ее соавтор С. Лу проанализировали взаимодействие сообществ пользователей Twitter до и после землетрясения и цунами 2011 г. в Японии. Авторы считают, что среди японских пользователей Twitter катастрофа способствовала большому количеству новых подключений и изменений в интернет-сообществах, а

также международному увеличению числа твитов, связанных с землетрясениями. В дополнение к своим выводам авторы описывают новую основу для исследования динамики сообществ в социальных сетях, которую можно использовать для изучения любого рода социальных изменений.

«Хотя мы никому не желали бы пережить стихийное бедствие, когда оно происходит, можно многое узнать о том, как социальные системы адаптируются и изменяются во время стрессовых периодов, глядя на то, как меняются модели взаимодействия людей, – говорит К. Брелсфорд. – К коммуникации в Twitter можно получить доступ и до, и после непредвиденного события, что обеспечивает точный и подробный отчет о том, как изменяются модели взаимодействия и как это влияет на целые сообщества». К. Брелсфорд имеет личный опыт встречи с землетрясением. В январе 2010 г. она была на Гаити, помогая своему брату с образовательным проектом, работая в здании всего в трех километрах от эпицентра землетрясения, около Леоган. Крыша рухнула, и падающая лестничная клетка травмировала ее правую ногу.

«Мои переживания во время землетрясения действительно стали движущей силой этого исследовательского проекта, – говорит К. Брелсфорд. – Тогда на Гаити у меня было наиболее лучшее для той ситуации наблюдательное положение. Я была в сознании, чувствуя, что действительно нахожусь в гуще событий, но не могу ничего сделать, и это было совершенно очевидно для всех, кто видел меня. Так что я увидела многое: как люди вели себя, сотрудничая друг с другом, как относились друг к другу, чего я, вероятно, не увидела бы будучи в стороне и при менее тяжелых условиях. Все это было действительно впечатляющим – координация людей и активация ресурсов, чтобы быстро добиться цели. Так что я подумала, было бы интересно исследовать, как изменяется координация и сотрудничество в сообществах поле экстремальных событий» ***(Как люди реагируют на катастрофу в социальных медиа // Newsland (http://newsland.com/news/detail/id/1453244/). – 2014. – 2.11).***

Маніпулятивні технології

Эбола вдвойне страшней, если много соцсетей: Как работает нагнетание паники

Ранее мы писали об исследованиях, которые подтверждают, что панические настроения среди пользователей соцсетей крайне «заразны». Но сегодня предлагаем поговорить о чём-то весьма заразном в прямом смысле: о вирусе лихорадки Эбола и о том, как СМИ и социальные сети нагнетают обстановку вокруг этой опасной эпидемии. Грозит ли нам всем апокалипсис, и почему сайты фейковых новостей так полюбили «вирусную» тему в последнее время?

В англоязычном сегменте Facebook уже несколько дней гуляет история, собравшая сотни тысяч лайков и репостов: якобы в Техасе семья из пяти

человек в небольшом городке заразилась лихорадкой Эбола. Источник «страшилки» – популярный сайт фейк-новостей National Report, использующий тему опасного вируса в целях привлечения трафика. Беда в том, что более 340 тыс. пользователей соцсети на полном серьёзе поверили в то, что в США вовсю свирепствует африканская хворь.

Паразитирование на человеческих страхах и склонности к панике происходит не первый раз: вспомните вбросы по поводу свиного и птичьего гриппа несколько лет назад. Проблема в том, что если слухи о чупакабре или 500-футовом крабе-убийце смотрятся как типичная интернет-шутка, то для тематики опасных вирусных заболеваний есть и другие причины распространения ложной информации, кроме шуточных, и желания «набить» трафик для своего ресурса. The Verge пишет о феномене фейковых новостных сайтов, которые стали явно «раскачивать» ситуацию с начала октября в целях решения некоторых сугубо личных задач, среди которых – не только нагнетание трафика и привлечение дополнительной аудитории.

Паника – лучший двигатель для подобных «новостей». А если учесть, что в ленте обновлений Facebook материалы об Эболе соседствуют со слухами о боевиках ИГИЛ, стрельбе в школах и нападениях террористов на какие-нибудь автозаправки – можете представить себе, насколько подобная паника эффективно «работает». Пиковый трафик для сайта фейковых новостей, который запустил «утку» в соцсеть, возрос на 2 млн уникальных просмотров – и всё благодаря пользователям социальной сети М. Цукерберга.

Ранее свои плоды от склонности Facebook-пользователей к панике успешно собирали такие проекты, как The Onion News, The Daily Currant и несколько других. Происходящее ещё называют «феноменом Боровитца» (по фамилии колумниста The New Yorker, который первым заметил, что нелепые и панические фейк-новости по охвату аудитории и числу повторных публикаций во много раз превосходят аудиторию тех, кто считает подобные сообщения смешными и шуточными). Фейковый заголовок, который звучит почти как настоящий, порождает такое же внимание к материалу, как и к серьёзному сообщению.

Проблема здесь – в аморальной эксплуатации человеческих страхов и доступа к Интернету огромного количества подростков, пожилых людей, мнительных женщин и других уязвимых категорий интернет-пользователей, склонных воспринимать информацию из сети «за чистую монету».

Зачастую последствия таковы, что даже серьёзные правительственные инициативы (вроде программ медицинского страхования) могут пострадать от «шутки»: тот же ресурс The National Report «пошутил» о том, что участникам программы страхования здоровья, предложенной администрацией Б. Обамы, будут вживлять под кожу RFID-чипы. «Шутка» удалась настолько, что породила даже ряд гражданских выступлений и серьёзных дискуссий в прессе.

Дальше – больше: в ситуации с фейк-Эболой сайт опубликовал «деталь», что источником заражения детских садов в США стал студент из

Либерии (ксенофобия), затем, что в Аризоне появились боевики «Исламского Государства», распыляющие вирус (дезинформация и подрыв доверия к властям). «Шутка» перестала быть шуткой и превратилась в элемент информационной войны против системы здравоохранения США, местных властей и представителей определённых стран.

Facebook используется как ключевой инструмент информационной войны, будучи удобным и эффективным каналом коммуникации. Заголовки и тематические «публикации» здесь мало кто верифицирует, а уровень вовлечённости в скандальные материалы (даже при их полной абсурдности) растёт, как снежный ком.

Редакция The Verge отмечает, что отчасти изменения в новостной и контентной политике Facebook касательно ленты новостей привели к тому, что теперь фейк-новости, слухи и непроверенные данные стали попадаться на глаза намного чаще (просто потому, что подобные материалы чаще «расшаривают»). Сайты фейк-новостей начали скупать рекламу в соцсетях, чтобы трафика становилось ещё больше – и вот результат: об Эболе в США на полном серьёзе говорят даже те, кто понимает, что этот вирус не передаётся воздушно-капельным путём.

Для самой соцсети тоже полезно, что трафик «крутится» вокруг горячих тем вроде ISIS и вируса, от которого ежесуточно умирают сотни человек. Вот только для аудитории пользы нет никакой, кроме растущей паники и домыслов. А пока М. Цукерберг с коллегами не придумали барьеры для фейковой информации, придётся самим пользователям проявить здравый смысл и хотя бы научиться использовать проверенные источники, а не бездумно репостить ссылки, присланные друзьями и знакомыми. В конечном итоге, любой проект фейк-новостей рано или поздно исчерпывает себя, и всем становится очевидно, что перед нами – подделка (пусть и очень умелая) под настоящее СМИ ***(Эбола вдвойне страшней, если много соцсетей: Как работает нагнетание паники // InternetUA (http://internetua.com/ebola-vdvoine-strashnei--esli-mnogo-socsetei--kak-rabotaet-nagnetanie-paniki). – 2014. – 24.10).***

***

Колишній «регіонал» захопив Facebook-сторінку Держкіно і публікує антисемітські гасла

26 жовтня Facebook-сторінка Держкіно змінила свій кавер, і тепер на ньому красується одна з лідерок ВО «Свобода» з гаслом «Україна повинна стати вістрям третьої світової війни».

Прес-служба Держкіно вже повідомила, що агентство втратило доступу до сторінки та не може контролювати публікації, які розміщуються на ній.

У повідомленні також ідеться про те, що сторінка Держкіно у Facebook була створена екс-керівником української кіноасоціації та помічником народного депутата України В. Януковича молодшого – Д. Ржавським. Попри звернення до адміністрації соціальної мережі Facebook та особисто до

Д. Ржавського з вимогою передати адміністрування сторінки, адміністрування так і не було передане Державному агентству України з питань кіно.

У Держкіно всю відповідальність за фальшиві публікації покладають на адміністратора сторінки – Д. Ржавського.

Д. Ржавський зареєстрований кандидатом у депутати від «Опозиційного блоку» ***(Колишній регіонал захопив Facebook-сторінку Держкіно і публікує антисемітські гасла // UkrainianWatcher (http://watcher.com.ua/2014/10/26/kolyshniy-rehional-zahopyv-facebook-storinku-derzhkino-i-publikuye-antysemitski-hasla/). – 2014. – 26.10).***

***

Аккаунт Ю. Бутусова был заблокирован из-за новости, в которой присутствовал снимок, на котором зампред Днепропетровской ОГА Г. Корбан целится из огнемета в мишень с изображением президента РФ.

Стало известно, что в настоящее время Ю. Бутусову вернули доступ к аккаунту, но он не может ни публиковать посты, ни оставлять комментарии.

Главный редактор Цензор.НЕТ обращается к пользователям Facebook с просьбой обратить на эту проблему внимание техподдержки соцсети ***(«Фейсбук» заблокировал аккаунт главреда «Цензор.Нет» Бутусова из-за фото мишени с Путиным, в которого целятся из огнемета // Цензор.НЕТ (http://censor.net.ua/news/309255/feyisbuk_zablokiroval_akkaunt_glavreda_tsenzornet_butusova_izza_foto_misheni_s_putinym_v_kotorogo_tselyatsya). – 2014. – 28.10).***

***

Боевики продолжают подпитывать собственные опасения по поводу тех слухов, которые они сами распространяют в последнее время. Это касается «информации» о том, что силы АТО в ближайшее время начнут широкомасштабное наступление, причем террористы сами придумывают этому «доказательства».

В социальных сетях боевики в последнее время паникуют и оставляют информацию о том, что, в частности, на территории Славянска наблюдается значительное повышение количества украинских военных. Они утверждают, что все санатории там заселены украинской армией, а помимо этого возле города есть лагерь, в котором установлено более сотни палаток, увеличивается концентрация техники ***(Боевики боятся наступления сил АТО // Кировоград-инфо (http://kirovgrad.pp.ua/anti/566-boeviki-boyatsya-nastupleniya-sil-ato.html). – 2014. – 28.10).***

Компания Facebook потребовала от DEA – управления по борьбе с наркотиками США – не использовать фейковые страницы в соцсети. Госорган создает аккаунты несуществующих людей в качестве «приманки» в рамках проведения расследований.

Начальник службы безопасности Facebook Д. Салливан в письме к администрации DEA отметил, что спецслужбы обязаны следовать тем же правилам пользования соцсетью, что и остальные.

Поводом стала жалоба жительницы Нью-Йорка. Агент госоргана создал поддельную страницу с ее именем и разместил на ней фотографии, которые хранились в ее телефоне. По словам женщины, снимки хранились в ее мобильном телефоне, изъятом во время ее ареста в 2010 г. за хранение наркотиков.

Как выяснилось позже, поддельная страница использовалась в ходе расследования DEA. Спецслужбы создают и ведут фейковые аккаунты для общения с предполагаемыми преступниками. При этом, согласно правилам пользования Facebook, в соцсети запрещено создавать страницы несуществующих людей или представляться чужим именем.

За причинение морального ущерба пострадавшая требует 250 тыс. дол. В Министерстве юстиции уже пообещали разобраться с данным инцидентом ***(Facebook запретил спецслужбам создавать «приманки» из фейковых аккаунтов // IT Expert (http://itexpert.org.ua/rubrikator/item/38918-facebook-zapretil-spetssluzhbam-sozdavat-primanki-iz-fejkovykh-akkauntov.html). – 2014. – 20.10).***

***

Роскомнадзор будет проверять интернет-ресурсы, признанные по закону о блогерах организаторами распространения информации, на основании обращений правоохранительных органов. Установить личность владельцев таких площадок поможет полиция, сообщает rbcdaily.ru.

«Хоть каждый день»

Минкомсвязи закончило публичное обсуждение проекта постановления правительства, регулирующего проведение ведомством проверок «организаторов распространения информации». Соответствующее постановление должно быть принято до конца этого года.

Термин «организатор распространения информации» появился во вступившем 1 августа этого года так называемом законе о блогерах. Организаторами являются, в частности, любые коммуникационные сервисы, в том числе мессендежеры и социальные сети.

По закону о блогерах Роскомнадзор должен вести реестр организаторов распространения информации. В него уже попали четыре сервиса Mail.Ru Group (мессенджер «Агент Mail.ru», социальные сети «ВКонтакте» и «Мой

мир», а также электронная почта Mail.ru), три сервиса «Яндекса» (облачное хранилище «Яндекс.Диск», сеть «Мой круг» и электронная почта), сайты знакомств Wamba.ru и Mamba.ru. В конце сентября «Известия» со ссылкой на чиновников Роскомнадзора писали, что регулятор отправил уведомления и зарубежным интернет-компаниям – Facebook, Google, Twitter. В московском офисе Google в конце сентября поясняли РБК, что пока не получали уведомления от регулятора. Теперь в Google отказываются от комментариев. Не комментируют эти вопросы и в Facebook. В штаб-квартире Twitter проигнорировали запрос РБК.

Теперь Минкомсвязи определилось с тем, как оно будет проверять организаторов распространения информации. Такие мероприятия, указано в опубликованном проекте проверок, должны осуществляться в соответствии с Законом «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля...».

В этом Законе прописаны периодичность проверок (например, выездные проверки должны быть не чаще чем раз в три года), публичность (предпринимателей заранее предупреждают о грядующей проверке) и другие процедурные моменты, пояснил РБК юрист адвокатского бюро «S&K Вертикаль» М. Ильин. Впрочем, есть два исключения: проверки по финансированию терроризма и легализации незаконных доходов могут проходить «хоть каждый день и неожиданно», добавил юрист.

С полицией и без

Роскомнадзор будет проверять организаторов распространения информации «на основании обращений органов, осуществляющих оперативно-разыскную деятельность или обеспечение безопасности РФ», уточняется в проекте докумета.

Если такой организатор не включен в реестр, то правоохранительные органы для проведения проверки должны сообщить Роскомнадзору подробную информацию об интернет-ресурсе. Если нужно установить личность организатора распространения информации, к проведению проверки «могут привлекаться уполномоченные сотрудники органов внутренних дел (полиции)», говорится в проекте документа.

Сами проверки могут проводиться как в виде «систематического наблюдения», не предусматривающего очного контакта с проверяемым лицом, так и быть выездными и «документарными».

Пресс-секретарь Роскомнадзора В. Ампелонский не ответил на запрос РБК.

У интернет-сообщества порядок проведения проверок интереса не вызвал. В ходе публичного обсуждения проекта документа на него не поступило ни одного экспертного заключения ***(Российский закон о блогерах позволит привлечь полицию к поиску владельцев сайтов // proIT (http://www.mediabusiness.com.ua/content/view/41073/126/lang,ru/). – 2014. – 22.10).***

***

Українські спецслужби не можуть блокувати соцмережі російських провайдерів. Про це повідомив глава Служби безпеки України В. Наливайченко, – передає ТВі.

«Поки що законодавство дає можливість отримати дозвіл суду на те, щоб заблокувати той чи інший веб-ресурс. Ми вже виходили на адміністраторів Google та інших серйозних мереж – є сприяння. Але з "ВКонтакте" та "Одноклассники" це зробити неможливо», – зазначив голова СБУ.

В. Наливайченко висловив вдячність патріотично налаштованим українцям, що створюють інтернет-спільноти з протидії інформаційній війні.

«Ми відчуваємо ціле співтовариство користувачів різних мереж, патріотично налаштованих людей в Інтернеті – ваша діяльність та єдність вражає», – сказав глава спецслужби.

Він також назвав позитивним моментом об'єктивну роботу громадських організацій Росії.

«Це щиро та ефективно... Особливо, коли це стосується пошуку зниклих безвісти українських військовослужбовців», – додав він ***(«ВКонтакті» та «Одноклассники» не доступні для української спецслужби // Чернівецький Промінь (http://promin.cv.ua/news/2014/10/22/7390). – 2014. – 22.10).***

***

Администрация популярного сервиса Whisper, позволяющего мобильным пользователям делиться друг с другом анонимными записями и личными сообщениями, раскрыла американским спецслужбам информацию о местоположении участников этой сети. Об этом в конце минувшей недели сообщил The Guardian.

По данным британского издания, в распоряжении властей оказались не только координаты владельцев мобильных устройств, которые пользуются Whisper, но и переписка пользователей. Журналисты подчеркивают, что благодаря анонимности сервис стал популярным среди американских военных, которые лишены возможности делиться своими эмоциями и переживаниями в обычных социальных сетях – например, Twitter или Facebook.

В материале The Guardian также отмечается, что за несколько дней до публикации материала администрация Whisper в срочном порядке внесла изменения в пользовательское соглашение. Согласно новым условиям, сервис имеет право на примерное, с точностью до 500 м, определение местоположения пользователя – даже в том случае, если он отключил соответствующую настройку.

Данные о том, где находятся владельцы мобильных устройств, на которых установлено приложение, и их личные сообщения, собирались сотрудниками Whisper в единую базу с возможностью поиска. Записи из этой

базы отправлялись в спецслужбы по запросу. В результате этих действий власти Соединенных Штатах получили возможность узнавать о настроениях военнослужащих. Отслеживание местоположения ведется и в отношении других пользователей, которые, как ожидается, могут создать интересный инфоповод или создать угрозу национальной безопасности.

Вскоре после публикации материала на сайте The Guardian главный редактор Whisper Н. Циммерман обвинил газету во лжи и заявил, что издание «еще пожалеет об этом». Он также добавил, что сервис не хранит никаких пользовательских данных, а сами пользователи являются анонимными ***(Анонимную соцсеть обвинили в слежке за пользователями // InternetUA (http://internetua.com/anonimnuua-socset-obvinili-v-slejke-za-polzovatelyami). – 2014. – 21.10).***

***

Генеральна прокуратура РФ звернулася до Федеральної служби з нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій (Роскомнагляд) з вимогою обмежити доступ до деяких сторінок соціальної мережі «ВКонтакте», які поширюють заклики до екстремістської діяльності. Про це повідомила представник Генпрокуратури М. Гриднєва, пише ZAXID.NET з посиланням на російське агентство ТАСС (http://zaxid.net/news/showNews.do?u_rosiyi_hochut_obmezhiti_dostup_do_chastini_storinok_vkontakte&objectId=1327850).

«Під час моніторингу мережі Інтернет виявлено, що на семи російськомовних сторінках сайту соціальної мережі «ВКонтакте» у відкритому доступі розміщено матеріали, що містять заклики до здійснення екстремістської і терористичної діяльності, доступні для перегляду необмеженій кількості осіб», – розповіла М. Гриднєва.

Зокрема, за її словами, на цих сторінках є тексти та відеоматеріали, пов'язані з діяльністю міжнародних терористичних організацій і груп, які містять заклики до участі в збройних формуваннях Ісламської держави.

«На ресурсах також розміщені агітаційні матеріали із закликами надавати фінансову допомогу терористичним групам із зазначенням номерів мобільних телефонів, QIWI-гаманця і інших платіжних реквізитів», – додала представник Генпрокуратури ***(Карабан О. У Росії хочуть обмежити доступ до частини сторінок «ВКонтакте» // ZAXID.NET (http://zaxid.net/news/showNews.do?u_rosiyi_hochut_obmezhiti_dostup_do_chastini_storinok_vkontakte&objectId=1327850). – 2014. – 27.10).***

***

В своей книге «Когда Google встретилась с WikiLeaks» Д. Ассанж заявил, что технологический гигант – «злой, плохой, санкционированный правительством и поддерживающий разрушения в Интернете». Более того, он назвал компанию «правительственной марионеткой, управляемой руками Х. Клинтон».

Как пишет издание The Inquirer, Д. Ассанж упомянул свою встречу с Э. Шмидтом, его подругой и еще двумя неназванными особами. По словам создателя WikiLeaks, гораздо позже он понял, что его убеждения очень отличались от взглядов остальных участников встречи.

«Тогда я понял, что Э. Шмидт, возможно, является не единственным эмиссаром Google. Официально или нет, но у него была какая-то компания, державшая (ред. – Шмидта) в непосредственной близости к Вашингтону, включая хорошо задокументированные отношения с президентом Б. Обамой. Мало того, что люди Х. Клинтон знали, что партнер Э. Шмидта посетил меня, но они также решили использовать ее в качестве тылового канала», – заявил Д. Ассанж.

Представители The Inquirer обратились к Google за комментариями по поводу книги. Примечательно, что в компании пока никак не отреагировали на выход «Когда Google встретилась с WikiLeaks», однако ранее Э. Шмидт называл Д. Ассанжа параноиком.

«У Джулиана паранойя по поводу некоторых вещей. Google никогда не сотрудничала с АНБ и конечно же, мы выступаем против того, что они делают», – заявил глава Google ***(Джулиан Ассанж назвал Google «правительственной марионеткой» // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/28/assange-vs-google.html). – 2014. – 28.10).***

***

Бельгийские учёные сумели отслеживать перемещения целой страны в течение года, обрабатывая данные сотовой связи.

Исследовательская команда из географов и математиков собирала обобщённые анонимные данные о звонках от главных мобильных провайдеров Франции и Португалии.

В общей сложности, эксперты обработали данные по 20–30 % граждан двух стран. Так, в Португалии учёные собирали информацию о местоположении вышек сотовой связи, принимавших звонок, его продолжительности и индивидуальном номере пользователя.

Во Франции исследователи собирали данные только о дне звонка и местоположении вышек. Бельгийские исследователи отметили, что не собирались шпионить за людьми, и проводили свою работу сугубо в прикладных целях.

В настоящее время, когда 96 % населения планеты пользуется сотовой связью, их метод позволяет отслеживать перемещения людей и плотность населения в отдельных районах гораздо более эффективно, чем с помощью традиционных опросных листов или звонков на городские телефоны.

Например, используя данную методику отслеживания перемещений людей внутри Сьерра-Леоне, и других африканских государств, охваченных эпидемией лихорадки Эбола, ВОЗ сможет разработать более эффективную стратегию купирования болезни.

Аналитики американского Бюро статистики подсчитали, что на сегодняшний день на планете Земля существует больше активных мобильных устройств, чем проживает людей ***(Перемещения граждан целой страны отследили через смартфоны // Блог Imena.UA (http://www.imena.ua/blog/phone-call-pulse-shows-millions/). – 2014. – 29.10).***

Проблема захисту даних. DDOS та вірусні атаки

Принтеры 3 в 1 могут служить платформой для хакерской атаки. Вся информация, распечатываемая, сохраняемая и пересылаемая с многофункциональных устройств, может быть переправлена за пределы организации.

Знаменитый криптоаналитик А. Шамир решил выяснить, каким образом злоумышленники могут похищать информацию, используя вредоносное ПО, внедренное во внутреннюю сеть. Об этом сообщает издание Network World.

Как обнаружил исследователь, в результате освещения внутренней крышки сканнера во время процесса сканирования многократными импульсами света будет получено изображение, состоящее из белых линий на темном фоне. Эти линии соответствуют направленным на крышку импульсам света, а их толщина зависит от продолжительности импульсов.

Исследователь разработал код, напоминающий азбуку Морзе, применяя который, можно посылать импульсы через нужные промежутки времени и интерпретировать полученные линии как двоичную систему, записанную с помощью символов 1 и 0. Вредосносное ПО, сохраняемое на отключенном от сети устройстве, может в нужное время запустить сканирование, а затем интерпретировать команды злоумышленников, обладающих удаленным доступом к устройству. По оценке А. Шамира, один сеанс сканирования обеспечивает утечку сотен бит информации, чего вполне достаточно, чтобы активировать функционалы вредоносного ПО.

Используя лазер в качестве источника импульсов света, исследователь успешно провел атаки с расстояния 200, 900 и 1200 м, а после увеличения мощности лазера получил хорошие результаты с расстояния 5 км. Кроме того, выяснилось, что для хакерских атак может применяться вредоносное ПО, которое активируется световым лучом самого сканера ***(Принтеры 3 в 1 могут служить платформой для хакерской атаки // InternetUA (http://internetua.com/printeri-3-v-1-mogut-slujit-platformoi-dlya-hakerskoi-ataki). – 2014. – 20.10).***

***

В последние несколько недель исследователи безопасности зафиксировали всплеск атак с использованием вредоносных программ,

маскирующихся под интернет-рекламу и рассчитанных на ничего не подозревающих пользователей. Помимо прочих, жертвами вредоносной рекламы стали военные подрядчики США.

По словам исследователей, они зафиксировали новые случаи использования вредоносной рекламы для кибершпионажа за тремя представителями военной промышленности. Для осуществления атак злоумышленники скрыли вредоносный код в рекламных баннерах и видеороликах, всплывающих перед пользователями во время работы в Интернете.

В настоящее время жертвами атак все чаще становятся банки и крупные торговые сети, чьи клиенты оказываются под угрозой похищения персональных данных и мошенничества. Однако исследователи обнаружили, что злоумышленники используют новейшие маркетинговые инструменты для шпионажа. Целью преступников является не похищение кликов и не мошенничество с банковскими счетами, а получение доступа к интеллектуальной собственности компаний, производящих военное оборудование и технику.

В Invincea сообщили, что за последние две недели прошлого месяца было зафиксировано шесть атак с использованием вредоносной рекламы на три компании, одна из которых имеет отношение к аэрокосмической промышленности. При этом исследователи отказались уточнять, какие именно предприятия стали жертвами инцидентов, ввиду их секретной деятельности ***(Вредоносная реклама используется для кибершпионажа // InternetUA (http://internetua.com/vredonosnaya-reklama-ispolzuetsya-dlya-kibershpionaja). – 2014. – 20.10).***

***

Эксперты из Trend Micro К. Уилхойт и Д. Гоголински сообщили о том, что хакерская группировка Sandworm Team осуществляет атаки на промышленные SCADA-системы, использующие продукты GE Intelligent Platforms. Напомним, что об этой группировке стало известно после обнаружения эксплуатации уязвимости нулевого дня в Windows.

По словам исследователей, атаки осуществляются по двум векторам – с использованием файлов .cim и .bci приложения CIMPLICITY. Данное решение разработано GE Intelligent Platforms для работы с системами с человеко-машинным интерфейсом (ЧМИ), которые применяются вместе со SCADA. Эксперты обнаружили, что в ходе атаки злоумышленники внедряют вредоносные файлы в установочную директорию CIMPLICITY, используя среду %CIMPATH %. Поскольку системы с ЧМИ участвуют в управлении многими производственными процессами, исследователи затрудняются определить конечную цель хакеров.

Эксперты из Trend Micro особо подчеркнули, что в настоящее время они зафиксировали только использование CIMPLICITY в векторах атаки, однако никаких доказательств того, что вредоносное ПО используется для

управления какой-либо SCADA-системой или информацией, обнаружено не было.

«Поскольку ЧМИ используется в корпоративных сетях и сетях управления, скорее всего, целью мог быть именно сегмент сети», – сообщили эксперты ***(Sandworm Team осуществляет атаки на промышленные SCADA-системы // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/21/Sandworm.html). – 2014. – 21.10).***

***

Навіть якщо в офісі нікого не має, це не означає, що корпоративні телефони не використовуються. Ними можуть заволодіти хакери, які за декілька днів легко наговорять на п'ятизначні суми. І сьогодні від таких телефонних атак страждають дедалі більше компаній.

Одним з таких постраждалих стала невеличка архітектурна фірма в США із семи робітників, яку створив Б. Фореман. Їй прийшов телефонний рахунок на 166 тис. дол. за розмови впродовж двох вихідних, коли навіть в офісі нікого не було. «Я подумав, що це безглуздо, – згадує Б. Фореман. – Це мала бути якась помилка».

Однак рахунок виявився справжнім: хакери вторглись до телефонної мережі компанії та направляли телефонний трафік на міжнародні дзвінки на платні номери у Гамбії, Сомалі та Мальдівах. Якби цього злому не відбулося, то компанії знадобилося б 34 роки, щоб отримати такий же рахунок.

Подібний тип шахрайства відомий вже декілька десятків років, проте з поширенням Інтернету та маршрутизації дзвінків він отримав друге життя. Зловмисникам стало легше захоплювати контроль, і лише за минулий рік компанії втратили через це понад 4,73 млрд дол. Ще в 2011 р. ця цифра була майже в п'ять разів меншою – близько 1 млрд дол.

Закон у таких випадках не на стороні постраждалих, оскільки телефонний оператор виконав свої зобов'язання і не повинен відповідати за корпоративну безпеку всередині компаній.

Самі ж хакери заробляють на цьому наступним чином. Вони запускають платні номери, вартість дзвінка на які становить 1 дол. або більше. Частину з цих грошей забирає організатор подібних сервісів, а решта – надходить зловмисникам. При цьому хакери часто дзвонять по вихідних, коли офіси порожні та їхню присутність важко помітити. А завдяки тому, що багато офісів використовують віртуальні АТС з потужними серверами, вони можуть одночасно здійснювати сотні дзвінків.

Важка боротьба

Представники індустрії намагаються боротися з цим явищем, проте кажуть, що це дуже складно. Один з таких органів – асоціація з контролю за шахрайством Communications Fraud Control Association, яку очолює Р. Ароноф. Її організація збирає платні номери, які брали участь у шахрайстві, та передає для блокування операторам.

Проте піймати самих злочинців досить важко, тому що для цього потрібна налагоджена міжнародна співпраця, оскільки такі злочини часто коються в різних країнах. Одним з успішних прикладів є арешт у 2011 р. групи з чотирьох осіб, які здійснили шахрайських телефонних дзвінків на 2 млн дол. Затримання організували ФБР спільно з місцевою поліцією Філліпінів.

Платити доводиться

Поки правоохоронці намагаються шукати злочинців, оператори попереджають корпорації краще захищати свою інфраструктуру. Адже комусь платити доведеться, навіть якщо суд визнає саму компанію невинною. «Ми мали заплатити за ті дзвінки, – каже віце-президент американського телефонного оператора TW Telecom Б. Мелдрум. Саме його послугами користувалася компанія Б. Форемана. – Хтось мав заплатити за ті дзвінки».

Сам Б. Фореман каже, що навіть не уявляв про можливий ризик, як і багато інших. Експерти ж попереджають, що будь-який комп'ютер в Інтернеті є мішенню для атак. «Це неминуче, – каже засновник компанії TransNexus Д. Далтон. Його фірма продає програмне забезпечення для маршрутизації дзвінків через Інтернет. – Якщо надати комп'ютеру доступ в Інтернет, він одразу стане мішенню. Люди не усвідомлюють, що їхні телефони можуть принести шестизначні суми збитків» ***(Хакери цілятся в корпоративні телефони // InternetUA (http://internetua.com/hakeri-c-lyatsya-v-korporativn--telefoni). – 2014. – 21.10).***

***

Специалисты в области IT-безопасности продемонстрировали новый метод, позволяющий спрятать вирус в графический файл с расширением .PNG.

Более того, после сокрытия вируса в картинке его «упаковывают» вместе с просмотрщиком в файл .APK для ОС Android. После запуска приложения и открытия графического файла на мобильном устройстве создаётся ещё один установочный файл.

Через него хакеры могут похищать личные данные пользователя, включая текстовые сообщения, фото, список контактов и любую другую информацию.

В настоящее время подобный тип вторжения работает на версии Android 4.4.2. Специалисты уже передали всю информацию разработчикам в Google.

Ранее специалисты по интернет-безопасности компании Citizen Lab обнаружили вирус, который может попадать на компьютеры пользователей просто через просмотр ролика на YouTube.

Хакеры научились модифицировать трафик с YouTube и Microsoft Live, чтобы устанавливать на компьютер пользователя «шпионские» программы

(Хакеры прячут вирусы для ОС Android в графических файлах // Блог Imena.UA (http://www.imena.ua/blog/hideen-virus-in-png/). – 2014. – 21.10).

***

Эксперты из Symantec сообщили о новой фишинговой кампании, жертвами которой становятся пользователи Dropbox. Злоумышленники рассылают электронные письма с пометкой «важно», в которых сообщается о том, что получателю якобы был отправлен слишком большой для пересылки по электронной почте документ. Пользователю предлагается просмотреть документ, кликнув на ссылку в сообщении. Эта ссылка ведет на поддельную страницу авторизации в Dropbox, которая подобно фотографиям и другим файлам хранится в домене пользовательского контента Dropbox.

Соединение со страницей осуществляется через SSL, что делает атаку еще боле опасной. Подделка выглядит практически так же, как настоящая. Отметим, что в данном случае злоумышленников интересует получение учетных данных пользователей не только Dropbox, но также одного из популярных сервисов электронной почты.

После того как пользователь нажал «Вход», его имя и пароль через SSL отправляются PHP скрипту на скомпрометированном сервере. Без использования вышеуказанного протокола пользователь получает соответствующее уведомление безопасности. После сохранения и отправки учетных данных злоумышленникам PHP скрипт перенаправляет пользователя на настоящую страницу авторизации в Dropbox. Примечательно, что некоторые ресурсы на странице не используют SSL, в связи с чем последние версии некоторых веб-браузеров отправляют пользователям уведомления безопасности.

Эксперты из Symantec сообщили Dropbox об угрозе, вследствие чего фишинговая страница была немедленно заблокирована ***(Новая фишинговая кампания нацелена на пользователей Dropbox // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/21/Dropbox-phishing-campaign.html). – 2014. – 21.10).***

***

Китайские власти похищают данные учетных записей пользователей iCloud, используя национальный межсетевой экран «Золотой щит». Об этом сообщается в отчете организации Great Fire, занимающейся мониторингом online-цензуры в Китае.

В Great Wall утверждают, что «Золотой щит» блокирует китайцам доступ к сайту iCloud. Вместо этого они перенаправляются на поддельный сайт, похищающий их учетные данные. Пользователи Firefox и Chrome получают соответствующее предупреждение при переходе на поддельный сайт, но поклонники Qihoo – самого популярного браузера в Китае – даже не поймут, что посетили мошеннический ресурс. Аналогичное перенаправление

происходит и при посещении страницы login.live.com, которая используется для входа в учетную запись Microsoft.

Поскольку атака происходит на уровне национального китайского межсетевого экрана, в Great Fire подозревают, что она осуществляется по заказу правительства государства с целью похищения логинов и паролей пользователей, а также их персональных данных. В качестве подтверждения к отчету были приложены результаты трассировки.

Если пользователь введет свои логин и пароль на поддельном сайте, все его личные данные станут доступны злоумышленникам. Возможно, власти Китая таким образом пытаются обойти новые средства защиты персональной информации, введенные компанией Apple.

Пользователи могут посетить подлинные сайты iCloud и Microsoft Live, используя сервис VPN. Тем не менее, в случае, если VPN блокируется «Золотым щитом», обойти атаку не получится ***(Власти Китая похищают учетные данные пользователей iCloud // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/21/china-collecting-apple-icloud-data-attack-coincides-launch-new-iphone.html). – 2014. – 21.10).***

***

Китайские программисты сообщили о выпуске джейлбрейка для устройств под управлением операционной системы iOS 8.1, релиз которой состоялся 20 октября. Из-за опасности удаления фотографий с мобильных устройств Apple хакеры из Pangu на некоторое время сняли установочный пакет с публикации, однако в настоящее время ссылка для загрузки вновь работает.

Запуск файла возможен только в среде Windows и имеет интерфейс на китайском языке. Данный джейлбрейк предназначен для iPhone 6, 6 Plus, iPad Air 2 и более ранних устройств Apple, совместимых с актуальной версией ОС. Основным минусом является то, что с ним не устанавливается каталог приложений Cydia – его совместимой с iOS 8 версии пока нет.

Некоторые пользователи не рекомендуют спешить с установкой джейлбрейка от Pangu, дав время разработчикам на исправление всех «багов» ***(Китайцы взломали iOS 8.1 через полтора дня после ее релиза // InternetUA (http://internetua.com/kitaici-vzlomali-iOS-8-1-cserez-poltora-dnya-posle-ee-reliza). – 2014. – 23.10).***

***

Специалисты «Лаборатории Касперского» рассказали об интересном новом зловреде, образец которого попал на экспертизу. Это модульный троян Ventir для Mac OS X. Он может поставляться с разным набором модулей, среди которых open source кейлоггер LogKext.

Использование общедоступных компонентов с открытыми исходниками – довольно необычное поведение для вредоносных программ. Обычно вирусописатели стараются написать всё самостоятельно, но зачем,

если существуют готовые модули, подходящие по функциональности? Кейлоггер LogKext – вполне легитимная программа, которая размещается на Github. Правда, некоторое время назад автор забросил разработку, но эту задачу взял на себя другой мейнтейнер, он вскоре обновил кейлоггер для совместимости с OS X Mavericks (10.9).

М. Кузин из «Лаборатории Касперского» пишет, что архив kext.tar загружается на заражённый компьютер, если дропперу Trojan-Dropper.OSX.Ventir удалось получить права суперпользователя.

«В архиве находятся три файла:

– updated.kext

– EventMonitor

– Keymap.plist

Программный пакет updated.kext является расширением ядра (kext) с открытым исходным кодом и предназначен для перехвата нажатий клавиш. Это расширение уже давно детектируется нами как not-a-virus:Monitor.OSX.LogKext.c, а его исходный код (как уже было сказано ранее) в настоящее время доступен любому желающему.

Файл Keymap.plist – это карта соответствия кодов нажатых клавиш их значениям. Файл EventMonitor использует ее для определения значения клавиш по соответствующим кодам, передаваемых ему файлом updated.kext.

Файл EventMonitor – файл-агент, который принимает данные от расширения ядра updated.kext, обрабатывает их и заносит в лог-файл /Library/.local/.logfile.

Кроме кейлоггера, троян-дроппер Ventir может скачивать другие модули: это бэкдор (Backdoor.OSX.Ventir.a) и троян-шпион (Trojan-Spy.OSX.Ventir.a). Последний загружается в систему, если дропперу не удалось получить права суперпользователя.

По словам М. Кузина, своей многомодульной структурой Ventir напоминает небезызвестный Morcut (он же OSX/Crisis), где было примерно такое же количество модулей с похожим назначением. Использование программного обеспечения с открытым исходным кодом существенно упрощает злоумышленникам задачу конструирования новых зловредов ***(Модульный троян для OS X содержит open source кейлоггер // InternetUA (http://internetua.com/modulnii-troyan-dlya-OS-X-soderjit-open-source-keilogger). – 2014. – 22.10).***

***

Российские хакеры обещают разоблачение Кремля

Взломать учетную запись Д. Медведева в Twitter – это верный способ попасть в немилость к российскому высшему руководству. Так что неудивительно, что виновные в этом предпочитают общаться с помощью зашифрованного интернет-чата.

Хакеры заявили, что говорят от имени всей группы. Она в середине августа разместила на ленте российского премьера сообщение, согласно

которому тот ушел в отставку от стыда за действия правительства. В итоге сообщений СМИ о взломе учетной записи Д. Медведева было больше, чем о выступлении В. Путина в этот день на аннексированном Крымском полуострове.

Ответственность на себя взяли хакеры, назвавшиеся членами группы Anonymous International. Они также заявили, что имеют доступ к трем телефонам Д. Медведева, а затем выложили данные с его частного электронного ящика и сделанные с вертолета фотографии. И никакой кипы государственных секретов в сноуденовском стиле. Просто тут были элементы скандальности, оттого что можно легко получить доступ к особо засекреченным данным, и возбуждения, оттого что можно прочитать о закулисной политике и властных схватках.

Каковы их цели? Неясно. Группа, по словам ее участников, формировалась несколько лет. В нее входят более десяти человек, все они граждане России и большая часть живет в России.

«Мы поддерживаем связь электронно и никогда не встречаемся лично», – заявили хакеры.

Политически объединение неоднородно: некоторые – либералы, другие поддерживают идеи времен Российской империи. Тем не менее им удается работать вместе: «Мы не идеалисты, но иногда хочется изменить мир к лучшему».

Впервые об этой группе стало известно 31 декабря прошлого года, когда она выложила текст новогоднего обращения В. Путина до его официального выхода в эфир. Затем она хранила молчание до событий в Крыму, после чего опубликовала список журналистов, награжденных государственными премиями за освещение происходившего.

Также она выложила информацию о подготовке к референдуму и инструктаж российским журналистам о том, как им следует освещать определенные темы. Среди особенно противоречивого контента был обзор работы петербургской компании под названием «Конкорд», которая платила деньги ряду интернет-троллей, чтобы оставлять прокремлевские комментарии в российских и иностранных СМИ. После этого блог группы и ее учетная запись в Twitter были заблокированы в России.

Хакерам нравится хвастаться своим знанием внутриполитических проблем. В день поездки вице-премьера И. Шувалова в Китай они почти буднично объявили, с чем тот будет там выступать. Д. Медведева хакеры назвали на 200 % декоративным главой правительства: они почти год читали его электронную почту и ждали чего-то интересного, но ничего не было.

Хакеры наблюдали и за чиновниками в правительстве и Кремле. По их словам, многие недовольны нынешней украинской политикой России, особенно в сфере экономики и финансов. «Главы министерств верны правительству, но на более низких уровнях назревает бунт. Однако ни у кого нет смелости отстоять свою позицию публично».

И они не только взламывают электронную почту. Весной Anonymous International опубликовал оригиналы документов с подписью пресс-секретаря В. Путина – Д. Пескова, которые были, судя по всему, сфотографированы, пока лежали на столе. Таким образом, хакеры намекают, что у них есть информаторы среди чиновников.

Российские СМИ и блогеры подозревают, что этим проектом пользуются служащие Кремля для внутренних интриг. Хакеры на это лишь говорят, что им неважно, что о них думают люди. Они также заявили, в ближайшие дни опубликуют «новые секреты Кремля». По их словам, у них на руках – «терабайты» документов с интересными деталями о российской истории. В. Путин, наверно, чувствует, что его технофобия теперь оправданна. У него нет никаких учетных записей в социальных сетях. Нет даже мобильного телефона.

Группа также заявляет, что взломала почту вице-премьера А. Дворковича. Если эти сообщения опубликовать, то будет множество частных и корпоративных конфликтов. Вопрос один – почему они их не обнародовали? Это уже отдельная загадка ***(Российские хакеры обещают разоблачение Кремля // InternetUA (http://internetua.com/rossiiskie-hakeri-obesxauat-razoblacsenie-kremlya). – 2014. – 22.10).***

***

В сети обнаружен новый вид вредоносной программы. Она похищает информацию и отправляет её со скомпрометированных компьютеров на «облачный» сервис Google Drive.

Программу использовали неизвестные хакеры в ходе атак, нацеленных на правительственные организации. Вредоносный код уже окрестили Drigo.

Программа собирала все файлы Excel, Word, PDF и Powerpoint, а также, текстовые документы и содержимое корзины с инфицированного компьютера и пересылала похищенные данные в «облачное» хранилище.

Специалисты сумели получить доступ к учётной записи Google Drive, на которую переправлялись краденые данные, и изучить хранилище. Исходя из названий файлов, можно предположить, что хакеры атаковали, в основном, правительственные организации.

Таким образом, Drigo использовалась для разведывательных целей, а это означает, что к её разработке может иметь отношение какое-то правительство.

Руководство Google уведомлено о нецелевом использовании учётной записи облачного сервиса и на данный момент эта запись уже заблокирована.

Тем не менее, принимая во внимание, что вредонос может самообновляться, преступникам останется просто создать новую учётную запись в Google Drive и перенаправить поток краденных файлов туда.

Ранее в сети появилось приложение, выдающее себя за Google Play и похищающее всю личную информацию пользователя, включая данные, необходимые для проведения банковских операций online ***(Обнаружена***

шпионская программа, которая похищает файлы и отправляет их в Google Drive // Блог Imena.UA (http://www.imena.ua/blog/stealing-information-through-google-drive/). – 2014. – 23.10).

***

Эксперты компании AdaptiveMobile сообщают о вредоносной активности нового варианта вымогательского ПО для Android-устройств под названием Koler. В отличие от своего предшественника, обновленный вредонос распространяется при помощи SMS-сообщений.

Стоит отметить, что в остальном функционал Koler такой же, как и у его первой версии – ПО блокирует экран Android-девайса без шифрования файлов или дальнейшей блокировки устройства. Для того чтобы восстановить доступ к гаджету, жертва должна заплатить «штраф».

После инфицирования устройства вирус начинает дальнейшую рассылку сообщений, в которых содержится ссылка bit.ly, на номера из списка контактов жертвы. Само сообщение выглядит следующим образом: «кто-то создал профиль под именем Лука Пелличиари и загрузил несколько твоих фото! это ты? http://bit.ly/xxxxxx».

Интересно, что такой же текст использовался во вредоносной кампании, направленной на пользователей Facebook. Видимо, вирусописатели решили, что SMS подобного рода являются отличной «приманкой».

При переходе по ссылке пользователь перенаправляется на страницу DropBox, которая предлагает скачать приложение PhotoViewer. После установки программы вирус блокирует экран устройства при помощи поддельной страницы ФБР. Последняя сообщает, что причиной блокировки стало наличие на девайсе контента порнографического и зоофилического характера. Разблокировать устройство можно, заплатив выкуп через Money Pak Voucher.

Учитывая тот факт, что Koler полностью блокирует экран гаджета, пользователь не может закрыть окно. То есть у жертвы не остается иного выхода, как заплатить требуемый «штраф» ***(Новая версия вымогателя Koler распространяется по SMS // InternetUA (http://internetua.com/novaya-versiya-vimogatelya-Koler-rasprostranyaetsya-po-SMS). – 2014. – 23.10).***

***

Случаи поражений мобильных устройств вредоносными программами зачастую преувеличены, однако эксперты всерьез бьют тревогу: вирусы, поражающие финансовые приложения и получающие доступ к конфиденциальной информации пользователя, мутируют и несут все более серьезную угрозу. Так, согласно недавно проведенному исследованию Лаборатории Касперского, за год вредоносные программы, поражающие устройства на базе Android, в 60 % случаев были использованы для кражи денег.

За период с августа 2013 г. по июль 2014 г., 588 тыс. пользователей Android-устройств по всему миру стали жертвами финансовых вредоносных программ. Это в шесть раз больше, чем годом ранее. В целом, 57,08 % всех зарегистрированных случаев были связаны с sms-атаками, влекущими за собой снятие средств с мобильного счета. На банковские трояны, напротив, приходилось всего 1,98 % атак.

Эксперты из Лаборатории Касперского обнаружили, что количество мобильных модификаций вредоносных программ резко возросло – из 423 в августе 2013 г. до 5967 в июле 2014 г., то есть в 14 раз. Это указывает на то, что киберпреступники создают несколько вариаций своих мошеннических программ в попытке остаться незамеченными антивирусным программным обеспечением.

«Профессионально разработанный банковский троян может предоставить мошенникам доступ ко всем деньгам жертвы, в то время как sms-вирусы должны проникнуть в большое количество мобильных устройств, чтобы принести преступникам хорошую прибыль. Кроме того, на сегодняшний день далеко не все владельцы смартфонов используют мобильные банковские приложения. Вот почему мы видим такую существенную разницу в количестве атак банковских троянов и sms-вирусов», – сообщается в отчете Лаборатории Касперского ***(Вирусы воруют деньги с Android-устройств // InternetUA (http://internetua.com/virusi-voruuat-dengi-s-Android-ustroistv). – 2014. – 24.10).***

***

Платформа Apple для обмена сообщениями стала целью спамеров, рекламирующих разнообразные товары. Как сообщают специалисты Landmark в своем ежеквартальном отчете, 40 % всего мобильного спама рассылалось именно через iMessage.

Как сообщает эксперт Landmark Т. Ландесман, в компании начали отслеживать спам в iMessage после внезапного роста нежелательных сообщений в прошлом году. В этом году пик активности злоумышленников пришелся на август и сентябрь – тогда каждое пятое сообщение, отправленное через iMessage, было спамом. На основании этих данных Т. Ландесман заявил, что утверждения Apple о защищенности своего сервиса являются необоснованными.

Спамеры также начали использовать альтернативные приложения для обмена сообщениями наподобие WhatsApp, SnapChat или WeChat. Эти программы не требуют специализированного ПО, а их использование совершенно бесплатно. По данным фирмы Analysys Mason, в 2013 г. через вышеуказанные сервисы было отправлено более 10,3 трлн спамовых сообщений, а к 2018 г. их количество может достигнуть 37,8 трлн.

В Apple не прокомментировали ситуацию. iMessage долго считался защищенной платформой, но в последнее время становится ясно, что сервис уязвим к спамерским атакам. По словам Т. Ландесмана, для рассылки спама с

компьютера Mac достаточно простой программы, состоящей из четырех строчек кода.

В прошлом году Apple ввела базовые средства по борьбе со спамом. Так, теперь пользователи могут жаловаться на спамеров ***(Спамеры нацелились на iMessage // InternetUA (http://internetua.com/spameri-nacelilis-na-iMessage). – 2014. – 27.10).***

***

Компании Facebook и Yahoo! разработали механизм, предотвращающий похищение учетных записей владельцев повторно используемых адресов электронной почты, зарегистрированных на веб-сайтах, на которых в прошлом уже были использованы эти адреса.

Служба безопасности Facebook провела анализ воздействия повторного использования электронных адресов на пользователей ресурса и совместно с Yahoo! приступила к разработке методов, направленных на уменьшение потенциального риска. Сотрудники обеих компаний создали механизм, предусматривающий создание нового поля в заголовке конфиденциальных электронных писем, включающее дату, с которой отправителю стал известен адрес получателя.

По этой дате поставщик сервиса электронной почты сможет проверить, осуществлялась ли смена владельцев данной учетной записи, и если да – заблокировать доставку сообщения, поскольку оно, скорее всего, предназначалось для предыдущего владельца.

Новое поле получило название Require-Recipient-Valid-Since (RRVS) и определяется как часть расширения протокола Simple Mail Transfer Protocol (SMTP).

В прошлом году Yahoo! приступила к удалению неактивных учетных записей пользователей, что позволило сделать их номера доступными для повторной регистрации. Практика повторно используемых адресов электронной почты вызвала немало критики со стороны экспертов безопасности. Такой метод действий является отличной лазейкой для злоумышленников, которые могут зарегистрировать удаленный адрес и завладеть учетными записями на сторонних ресурсах, которые используют их для подтверждения запросов изменения пароля ***(Facebook и Yahoo! предотвращают похищение учетных записей повторно используемых электронных адресов // InternetUA (http://internetua.com/Facebook-i-Yahoo--predotvrasxauat-pohisxenie-ucsetnih-zapisei-povtorno-ispolzuemih-elektronnih-adresov). – 2014. – 27.10).***

***

Государственная служба специальной связи и защиты информации не зафиксировала несанкционированных вмешательств в работу электронной информационно-аналитической системы «Выборы».

Об этом на брифинге сообщил председатель Госспецсвязи В. Зверев. При этом, по его словам, DDOS-атаки на систему осуществлялись, но не сказались на ее работе в целом.

Атаки на работу системы «Выборы» происходят до сих пор, достигая до 9,3 гигабайт в секунду.

В. Зверев назвал неоднократно появлявшуюся в СМИ информацию о взломе системы неправдивой. Он также напомнил, что над защитой системы «Выборы» работают Госспецсвязи, Служба безопасности Украины и Центральная избирательная комиссия.

Как сообщало агентство, Служба безопасности Украины совместно с Государственной службой специальной связи гарантирует бесперебойное функционирование информационных систем Центральной избирательной комиссии ***(Госспецсвязи не зафиксировала вмешательств в работу системы «Выборы» // proIT (http://proit.com.ua/news/internet/2014/10/27/153739.html). – 2014. – 27.10).***

***

Как сообщила ИБ-компания Damballa, в III квартале нынешнего года количество компьютеров, инфицированных вредоносным ПО Backoff, резко возросло. Так, с августа по сентябрь нынешнего года число зараженных систем увеличилось на 57 %.

Отметим, что вредоносное ПО Backoff способно получать доступ к оперативной памяти компьютера и похищать данные кредитной карты после того, как жертва расплатилась ею через PoS-терминал.

По словам главы Damballa Б. Фостера, специалистам компании видно 55 % интернет-трафика из Северной Америки, в том числе DNS-запросы. По причинам безопасности они не могут видеть IP-адреса. С помощью кластера Hadoop эксперты анализируют DNS-запросы и, судя по серверу, с которым они контактируют, определяют потенциально вредоносные.

Б. Фостер отметил, что исследователи в Damballa отслеживают набор характеристик доменов и доменных имен, имеющих отношение к Backoff, и фиксируют значительный рост заражений. Эксперт добавил, что сокращение времени между обнаружением вторжения и определением, где оно произошло, имеет «решающее значение» для защиты данных пользователей ***(Количество заражений вредоносным ПО Backoff стремительно растет // InternetUA (http://internetua.com/kolicsestvo-zarajenii-vredonosnim-po-Backoff-stremitelno-rastet). – 2014. – 27.10).***

***

Министерство внутренней безопасности США занято расследованием около двух десятков случаев, которые могут быть связаны с наличием критических уязвимостей в медицинских приборах и оборудовании для больниц. Власти опасаются, что такие устройств могут быть уязвимы для хакеров, сообщает агентство Reuters со ссылкой на источник в правительстве.

Задача по проверке медприборов возложена на Группу реагирования на чрезвычайные ситуации в промышленных системах управления (ICS-CERT). Она изучает, например, инфузионный насос компании Hospira, имплантируемые в сердце устройства (кардиостимуляторы, дефибрилляторы) производства Medtronics и St Jude Medical, системы мониторинга, хирургическое и анестезиологическое оборудование и т. д.

Официального подтверждения проверок нет. Собеседники Reuters на условиях анонимности отметили, что ни одного случая атаки пока выявлено не было, поэтому киберугрозу не следует преувеличивать. Тем не менее, ведомство опасается, что злоумышленники могут получить доступ к медустройствам и управлять ими дистанционно.

Хакеры могут навредить больным, если найдут бэкдор, предназначенный для инженеров сервисной службы. К примеру, они смогут сделать так, чтобы инфузионный насос привел к передозировке пациентов лекарствами, а сердечный имплантат – поразил их смертельным разрядом тока ***(Спецслужбы США ищут уязвимости в медицинских приборах // InternetUA (http://internetua.com/specslujbi-ssha-isxut-uyazvimosti-v-medicinskih-priborah). – 2014. – 27.10).***

***

Как следует из уведомления безопасности разработчиков VMware, в гипервизорах VMware ESXi, предназначенных для использования на предприятиях, была обнаружена опасная уязвимость, позволяющая создавать нелегитимные резервные копии виртуальных машин. При этом брешь затрагивает все версии продукта начиная с 4.x и заканчивая актуальной сборкой.

Важно отметить, что уязвимость находится в механизме Changed Block Tracking (CBT) и существует из-за неверной обработки команды QueryChangedDiskAreas (используется для получения данных относительно занятых дисковых секторов виртуальных дисков). Возвращаемое по данному запросу значение может быть как неправильным, так и вовсе отсутствовать.

Вместе с тем для успешной эксплуатации бреши необходимо, чтобы после включения CBT размер vmdk диска был увеличен до 128 ГБ и более. В этом случае удаленный пользователь может при помощи любого инструмента для резервного копирования, использующего уязвимый механизм, создать нелегитимные резервные копии.

В качестве метода противостояния угрозе до выхода официального исправления разработчики рекомендуют отключить и заново включить механизме CBT ***(Уязвимость в VMware позволяет создавать нелегитимные резервные копии виртуальных машин // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/28/VMware-flaw.html). – 2014. – 28.10).***

***

Специалисты из компании Leviathan Security Group обнаружили вредоносный узел Tor на территории России. Он дописывает бинарный код в конец файлов, которые пользователь скачивает из Интернета. Tor – хороший инструмент для обеспечения анонимного доступа. Но анонимность не означает безопасность.

Исследователи говорят, что такое поведение сервера можно рассматривать как разновидность MiTM-атаки.

Для демонстрации подобной уязвимости разработчики из Leviathan Security Group выпустили программу BDF (Backdoor Factory), которая модифицирует исполняемые файлы, добавляя к ним произвольный код. Автор программы BDF объясняет принцип её работы в демонстрации на видео (выступление записано на хакерской конференции DerbyCon 2014).

О вредоносном российском узле уведомлены координаторы проекта Tor, так что сейчас он помечен как плохой узел (флаг BadExit). Пользователи сети Tor должны принять эту информацию к сведению.

Нужно отметить, что из 1110 выходных узлов в сети Tor это был единственный, который добавлял вредоносный код к бинарникам. Все остальные проверены и не осуществляют ничего подобного. Хотя, это нельзя гарантировать наверняка: узлы могут действовать избирательно и модифицировать только часть файлов, чтобы не проявить себя при проверке ***(Вредоносный узел Tor нашли в России // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/28/tor-russia-modified-binaries.html). – 2014. – 28.10).***

***

Исследователи из Palo Alto Networks сообщили о том, что банковский троян Dridex изменил метод распространения и теперь осуществляет заражение персональных компьютеров, используя макросы Word.

Dridex – последняя версия в линейке банковских троянов Bugat/Feodo/Cridex, она активно используется с июля текущего года. До настоящего времени троян распространялся по электронной почте, но на прошлой неделе организаторы атаки изменили схему, так что теперь они рассылают документы Microsoft Word, содержащие макрос, который скачивает и запускает вредоносную программу.

Как и свои предшественники, Dridex представляет собой типичный банковский троян по образцу Zeus. Его главная функциональность – кража учётных данных для доступа к онлайн-банкингу, так что злоумышленники получают доступ к денежным средствам жертвы и могут перевести их на другой счёт. Dridex использует конфигурационный XML-файл для определения списка сайтов, для которых осуществляется кража учётных данных. Там также перечислены сайты, которые нужно игнорировать.

Исследователи говорят, что схема распространения Dridex изменилась 21 октября. Жертвами атаки являются, преимущественно, пользователи из США.

В частности, замечено девять различных документов Word, с которыми распространяется вредоносный макрос. Макросы скачивают файлы по следующим адресам:

http://gpsbah[.]com/images/1.exe
http://jvsfiles[.]com/common/1.exe
http://jvssys[.]com/js/1.exe
http://mirafarm[.]ro/html/js/bin.exe
http://palitosdepan[.]com/js/bin.exe
http://www.juglarsa.com[.]ar/images/1.exe

Всё это легитимные веб-сайты, которые, видимо, подверглись взлому.

Защититься от атаки можно с помощью отключения макросов Word. Вообще, данный вектор атаки известен уже около 10 лет, так что макросы Word и так должны быть отключены по умолчанию у большинства пользователей ***(Банковский троян Dridex распространяется через макросы Word // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/10/28/dridex-banking-trojan-distributed-word-documents.html). – 2014. – 28.10).***

***

Во вредоносной программе, так называемом трояне-дозвонщике, для мобильных устройств на платформе Android обнаружен механизм самозащиты, благодаря которому пользователь зараженного устройства не может ее удалить. Об этом говорится в сообщении компании «Доктор Веб».

Основным предназначением трояна является совершение дорогостоящих звонков без согласия пользователя. Основная задача подобных программ – установить соединение с определенным телефонным номером (в большинстве случаев принадлежащим развлекательному сервису категории «для взрослых»), за это с абонентского счета пользователя списывается внушительная сумма, поступающая злоумышленникам.

Согласно сообщению, новый Android-троян представляет собой классическую вредоносную программу-дозвонщик, совершающую звонки на премиум-номера. Троян распространяется злоумышленниками под видом эротического приложения и после установки помещает на главный экран мобильного устройства свой ярлык, который не имеет подписи и значка, в результате чего у некоторых пользователей может сложиться ложное впечатление о том, что установка программы не удалась.

В ряде случаев после запуска программа может продемонстрировать сообщение об ошибке доступа к запрошенной услуге, после чего окончательно скрывает следы своего пребывания в зараженной системе, удаляя созданный ранее ярлык и функционируя в дальнейшем в качестве системного сервиса. Помимо ручного запуска через ярлык, троянец

активирует данный сервис автоматически, например, после очередного включения зараженного устройства, поэтому фактически для начала вредоносной деятельности не требуется никакого вмешательства пользователя.

Запускаемый трояном сервис с определенной периодичностью осуществляет звонки на номер 803402470, информация о котором хранится в настройках программы. Однако при необходимости киберпреступники могут изменить целевой номер дозвона, отдав вредоносному приложению соответствующую команду с управляющего сервера, – это позволяет авторам программы заработать сразу на нескольких платных сервисах.

Чтобы уменьшить вероятность обнаружения пользователем нежелательной активности, троянец отключает разговорный динамик мобильного устройства на время «телефонного разговора», а для окончательного сокрытия вредоносной деятельности удаляет из системного журнала, а также из списка совершенных звонков всю компрометирующую его информацию.

Однако главной особенностью этого дозвонщика является его способность противостоять попыткам пользователя удалить угрозу с зараженного мобильного устройства: как только пострадавший откроет раздел системных настроек, отвечающий за управление приложениями, программа заблокирует это действие, переведя пользователя на главный экран операционной системы. Таким образом, ручное удаление троянца становится практически невозможным ***(Обнаружен защищенный от удаления троян-дозвонщик для Android-устройств // InternetUA (http://internetua.com/obnarujen-zasxisxennii-ot-udaleniya-troyan-dozvonsxik-dlya-Android-ustroistv). – 2014. – 28.10).***

***

Американская компания FireEye, специализирующаяся на компьютерной безопасности, полагает, что базирующаяся в России группа хакеров под названием APT28 регулярно похищает данные, касающиеся НАТО и союзников США, информируют «Экономические известия» (http://news.eizvestia.com/news_technology/full/513-gruppa-rossijskih-hakerov-voruet-dannye-nato-fireeye).

«Уже давно считается, что Россия среди других государств является одним из лидеров в том, что касается возможностей осуществления сложных операций в компьютерных сетях», – отмечают специалисты FireEye.

FireEye считает, что хакерская группировка APT28 примерно с 2007 г. осуществляет кибератаки против лиц и структур, связанных с НАТО, чиновников стран Восточной Европы и Грузии. В качестве доказательств этих утверждений FireEye указывает на то, что часть кода программ, которые были использованы в данных кибератаках, написана с примечаниями на русском языке. Специалисты компании считают, что APT28 интересуется главным образом информацией политического или геополитического

характера, а наибольшая активность хакеров приходится на светлое время суток в Москве и Санкт-Петербурге ***(Группа российских хакеров ворует данные НАТО // «Экономические известия» (http://news.eizvestia.com/news_technology/full/513-gruppa-rossijskih-hakerov-voruet-dannye-nato-fireeye). – 2014. – 28.10).***

***

Независимые исследователи обнаружили уязвимость в смартфонах Samsung, позволяющую злоумышленникам удалённо стереть все данные с устройства.

Уязвимость связана с сервисом для защиты и поиска устройства Samsung Find My Mobile. Ради безопасности всем пользователям предлагается временно отключить его.

Дело в том, что при первичной настройке нового смартфона Samsung пользователю предлагается сразу включить утилиту для его поиска и удалённой блокировки.

В данном сервисе нашлась брешь, которая позволяет злоумышленникам дистанционно заблокировать аппарат, или даже полностью стереть все данные, хранящиеся на нём. Приложение Samsung не верифицирует получаемые данные о ключе безопасности.

Таким образом, хакеры могут перехватить управление устройством, организовав атаку типа DDoS, перегружающую устройство сетевым трафиком. Уязвимости подвержена существенная доля владельцев мобильных устройств корейского производителя.

Все данные об уязвимости были преданы в офис Samsung. Корпорация пока что никак не комментирует сообщения исследователей, а эксперты рекомендуют пользователям на время полностью отключить указанный сервис Samsung ***(Уязвимость в устройствах Samsung позволяет дистанционно стереть все данные // Блог Imena.UA (http://www.imena.ua/blog/samsung-data-secure-bug/). – 2014. – 28.10).***

***

Объединенная группа исследователей в области безопасности раскрыла китайскую кибершпионскую группировку, целью которой являются не только США и западные государства, но и китайские диссиденты, сообщает The Washington Post.

Исследователи утверждают, что за последние недели вредоносные программы Axiom были обнаружены на 43 тыс. компьютеров по всему миру, многие из которых принадлежали работникам государственных органов, журналистам, представителям телекоммуникационных и энергетических компаний.

ФБР заявляет, что работа данной группировки под названием Axiom является более сложной, чем работа «Подразделения 61398» Народно-

освободительной армии Китая. В 2013 г. оно было обвинено в массовом шпионаже.

Эксперты согласны с ФБР и отмечают, что в отличие от «Подразделения 61398» Axiom ориентирована на шпионаж за диссидентами, а также промышленный шпионаж и кражу интеллектуальной собственности.

«По всей видимости, деятельность Axiom поддерживается государством и ставит своей целью кражу коммерческих тайн и шпионаж за продемократическими организациями и правительствами других стран, – заявил П. Ламонтаг, директор компании Novetta Solutions, занимающейся вопросами кибербезопасности. – Они используют самые сложные тактики шпионажа, которые мы когда-либо видели в Китае».

Представитель Посольства Китая в США Г. Шуан сказал, что китайское законодательство запрещает киберпреступность и что правительство «сделало все возможное для борьбы с ней» ***(Китайские кибершпионы взломали 43 тыс. компьютеров по всему миру // InternetUA (http://internetua.com/kitaiskie-kibershpioni-vzlomali-43-tis--kompuaterov-po-vsemu-miru). – 2014. – 29.10).***

***

СБУ заблокировало поддельный веб-сайт Центральной избирательной комиссии, сообщает Security Lab.

Вредоносный портал, по заверениям правоохранителей, был создан для перехвата жалоб избирателей.

Как сообщает издание со ссылкой на представителей Службы безопасности Украины, ведомство заблокировало работу фишингового веб-сайта, имитирующего официальный портал Центральной избирательной комиссии (ЦИК). При этом создателями ресурса являются члены хакерской группировки «Киберберкут».

Ранее эти же злоумышленники взяли на себя ответственность за уничтожение сетевой инфраструктуры ЦИК. Тогда хакеры вывели из строя сетевое оборудование украинского ведомства, из-за чего была уничтожена хранящаяся на правительственных компьютерах информация. Позже «Киберберкут» запустил фишинговый ресурс cvk.com.ua, что позволяло перехватывать жалобы избирателей.

По данным СБУ, в день выборов, 26 октября, регулятор получил более 450 заявлений с фото- и видеодоказательствами возможных нарушений ***(СБУ заблокировало поддельный сайт ЦИК // proIT (http://proit.com.ua/news/internet/2014/10/29/102114.html). – 2014. – 29.10).***

***

Студент киевского Политехнического института (КПИ) на основе обнаруженного во «ВКонтакте» бага разработал утилиту, позволяющую установить администратора любого из сообществ соцсети. Ссылка на программу 29 октября появилась в группе «КПИ live».

Утилита, которая получила название «Срыватель покровов», работает на основе API «ВКонтакте». Для того, чтобы получить ссылку на профиль администратора того или иного паблика, достаточно скопировать адрес сообщества в поисковую строку и нажать кнопку «Сорвать покровы».

После этого программа показывает страницу или страницы тех, кто руководит публикацией записей в указанной группе. Рядом с ссылками отображаются также репосты из сообщества, благодаря которым удалось установить личность админа. Если репосты в группе отсутствуют, «Срыватель покровов» не работает.

Баг при репостах, который лёг в основу утилиты, был обнаружен 28 октября другим студентом киевского политеха В. Белогородским.

Как сообщил в своём блоге В. Белогородский, узнать имя опубликовавшего репост админа можно во всплывающем окне с аватарками тех, кому понравилась запись.

В случае с оригинальными публикациями в группах в таком окне отображается стандартный текст со словами «Оценили запись сообщества». Однако, когда речь идёт о репосте, список поставивших «лайк» сохраняет привязку к имени того, кто опубликовал его в паблике.

По словам автора утилиты, созданная им программа «пока работает не всегда правильно» и иногда выдаёт за администратора не связанного с сообществом человека. На некорректное отображение админов жалуются в комментариях и некоторых из опробовавших её пользователей. Проверка, проведённая TJournal, показала, что «Срыватель покровов» работает корректно.

Один из пользователей также заметил, что обнаруженный в соцсети баг на самом деле не является ошибкой, существует уже несколько лет и связан с особенностями кода функции wall.getReposts, «возвращающего список всех, кто репостнул».

Пресс-секретарь «ВКонтакте» Г. Лобушкин сообщил TJournal, что обнаруженный украинскими студентами способ установки личностей админов не является багом. По словам Г. Лобушкина, в настоящее время сотрудники ресурса изучают указанную «недокументированную фичу».

«Это не баг, потому что с уверенностью определить администратора, репостнувшего запись, невозможно. Но спасибо автору за наводку, наши специалисты уже изучают эту недокументированную фичу», – сказал Г. Лобушкин ***(Украинские студенты благодаря багу «ВКонтакте» научились вычислять админов сообществ соцсети // InternetUA (http://internetua.com/ukrainskie-studenti-blagodarya-bagu--vkontakte--naucsilis-vicsislyat-adminov-soobsxestv-socseti). – 2014. – 30.10).***

***

На сайте так называемой «Центральной избирательной комиссии» боевиков «ЛНР» появилось сообщение об отмене незаконных выборов, пишут «Экономические известия».

«Украинские кибервойска отменяют так называемые выборы в “ЛНР” и “ДНР”», – говорится в сообщении от, очевидно, украинских хакеров.

Подписались программисты традиционно: «Слава Украине» ***(Хакеры взломали сайт «ЦВК» террористов и сообщили об отмене незаконных выборов // «Экономические известия» (http://news.eizvestia.com/news_politics/full/863-hakery-vzlomali-sajt-cvk-terroristov-i-otmenili-nezakonnye-vybory). – 2014. – 30.10).***

***

Свыше 200 организаций и около 400 специалистов по информационной безопасности из 29 стран Европейского Союза провели крупнейшие в истории совместные учения по отражению хакерских атак.

Для учений Cyber Europe 2014 были привлечены специалисты из государственного и частного секторов. Целью «противохакерских манёвров» стала проверка эффективности совместных действий при защите от нападения из сети.

Организатором мероприятия выступило Европейское агентство по сетевой и информационной безопасности ENISA.

В ходе учений, которые шли целый день, была проведена симуляция более 2 тыс. отдельных инцидентов в сети, включая DDoS-атаки на веб-сайты, реагирование на сообщения разведки и медиа о хакерских атаках.

Также участники тренировались реагировать на взлом стратегических объектов, утечку конфиденциальной информации, атаки на критическую инфраструктуру и тому подобные события.

Напомним, последние столь массовые учения прошли 26 ноября 2013 г. В «манёврах» Cyber Coalition 2013 под эгидой НАТО было задействовано 33 государства.

В ходе трёхдневных учений были проведены эмуляции кибератак – таким образом, командование НАТО выясняло, способны ли страны-члены альянса защитить свои сети от хакерских атак ***(В Европе состоялись крупнейшие в истории «противохакерские манёвры» // Блог Imena.UA (http://www.imena.ua/blog/cyber-security-exercise-in-europe/). – 2014. – 31.10).***

***

Вирусы-вымогатели, которые шифруют файлы пользователей, требуя денег за расшифровку, терроризируют Интернет уже не первый год. Однако в нынешнем октябре они разбушевались не на шутку – очевидно, совершив новый эволюционный скачок в области автоматизации. В начале месяца массовому заражению вымогательским ПО CryptoLocker подверглись сотрудники крупнейшей австралийской вещательной компании ABC, а также почтовые и другие государственные службы страны. В середине месяца более 100 тыс. американцев были заражены вирусом-шифровальщиком через рекламные баннеры, крутившиеся в роликах на YouTube.

В последние дни октября случилась активизация опасного шифровальщика в российском сегменте Интернета. Пользователи получают по почте вредоносный файл, который представляет собой обфусцированный JavaScript размером 2.5 кб (MD5 ea834605f6bee2d4680aae0936655a30). При запуске троян загружает из Интернета и запускает дополнительные компоненты.

Описание вируса присутствует на Virustotal, там же в комментариях приводится и деобфусцированная версия скрипта.

После того как пользователь откроет приложенный файл и запустит вредоносный скрипт, его информируют о том, что его документы, фото, базы данных, а также другие важные файлы «были зашифрованы с использованием криптостойкого алгоритма RSA-1024».

Далее пользователю предлагается подробная инструкция по спасению своих цифровых активов, которая сводится к следующему набору действий:

1. Ваши файлы зашифрованы. Отправьте нам письмо с KEY и UNIQUE в течение суток.

2. Нашли KEY.PRIVATE и UNIQUE.KEY на своем ПК, взяли пару зашифрованных файлов – отправили на почту paycrypt@gmail.com

3. Через некоторое время получаете ответ с гарантиями, инструкцией и стоимостью. Посетите наш Twitter. Посмотрите, что все получают ключи.

4. После оплаты получаете ключ дешифрования, ПО и инструкцию по дешифрованию.

Наиболее интересным в этой инструкции является пункт 3, в котором указана учетная запись в Twitter, публично разглашающая информацию об адресах электронной почты жертв атак (http://twitter.com/keybtc). Это не только позволяет продолжать монетизацию (например, с помощью рассылки спама на адреса жертв, часть из которых указывало служебные адреса электронной почты), но может и нанести существенный вред репутации пострадавших ***(Вирус-вымогатель CryptoBot «сдает» своих жертв через Twitter // InternetUA (http://internetua.com/virus-vimogatel-CryptoBot--sdaet--svoih-jertv-cserez-Twitter). – 2014. – 2.11).***

***

Международная антивирусная компания ESET подготовила необычный рейтинг ботнетов.

В состав «армии зомби» – ботнета – могут входить миллионы зараженных вредоносным ПО компьютеров, которыми дистанционно управляют киберпреступники. «Зомби-сеть» используется для DDoS-атак, рассылки спама, накрутки кликов, кражи персональных данных – без ведома жертвы. При этом зараженные машины атакуют «здоровых» в лучших традициях постапокалиптических фильмов.

Storm

В 2007 г. червь Storm «зомбировал» до 10 млн компьютеров по всему миру. Это первая, но далеко не последняя в истории человечества атака подобного масштаба.

Операторы Storm впервые использовали тактику, которая до сих пор в ходу у киберпреступников. Вредоносное ПО распространялось в письмах с заголовками в стиле «ШОК! ВИДЕО!» и с применением методов социальной инженерии. Схемы заражения, равно как и вредоносный код, постоянно менялись.

Кроме того, создатели Storm первыми получили финансовую прибыль от ботнета – их армия продавалась по частям и использовалась в разных вредоносных кампаниях. «Боевые зомби» атаковали даже информационные сети антивирусных вендоров и веб-ресурсы о безопасности.

Conficker

Поведение «зомби-сетей» невозможно прогнозировать – ботнет скромных размеров может в любой момент превратиться в миллионную армию «зомби».

В 2008–2009 гг. ботнет Conficker объединил до 15 млн «зомби-машин». Совокупная вычислительная мощь сети превосходила возможности существующих суперкомпьютеров. Создатели ботнета могли использовать его для DDoS-атак на интернет-ресурсы, кражу данных и спам-рассылки.

В борьбе с Conficker участвовали ведущие антивирусные вендоры, включая ESET. Им удалось значительно сократить численность «армии зомби». Но вирус мутирует, и сегодня, шесть лет спустя, опасность заражения все еще существует.

Zeus

Как известно из кино, зомби-апокалипсис настанет быстрее, если вирус будет заражать не только людей, но и животных. Создатели ботнета Zeus руководствовались схожим принципом – пока компьютеры на базе Windows пополняли «армию зомби», мобильное вредоносное ПО осуществляло кражу данных онлайн-банкинга с устройств на Symbian, Windows Mobile, Android и Blackberry.

В 2012 г. ботнет был повержен, но, по законам жанра, «восстал из мертвых», реконструированный на базе оригинального кода. Летом 2014 г. с новым ботнетом Gameover Zeus справились специалисты ФБР и партнеры ведомства.

Но история продолжается – создатели ботнета работают над его возвращением, а тем временем по схеме Zeus распространяется небезызвестный троян-вымогатель Cryptolocker.

Flashback

Ботнет Flashback шокировал людей, убежденных в том, что вирусов для Mac OS X не существует. Доказывая обратное, его создатели «обратили в зомби» более 600 тыс. машин по всему миру, используя уязвимость нулевого дня в плагине Java.

Получив в свое распоряжение значительную долю компьютеров Apple по всему миру, создатели армии «яблочных зомби» попытались зарабатывать деньги на кликах. Идея провалилась, так как «зомби» не проходили фейсконтроль систем обнаружения мошенничества.

Пока в мире остаются зараженные трояном Flashback компьютеры Mac, нельзя с уверенностью утверждать, что эпидемия в прошлом. Кто знает, что придумают создатели этой «армии зомби».

Windigo

На первый взгляд, ботнет Windigo не представляет особой опасности – он «всего лишь» крадет учетные записи пользователей и использует «зомби-машины» для рассылки спама. С другой стороны, его создатели собирали свою «армию» почти три года, не привлекая внимания специалистов по информационной безопасности.

Жертвы Windigo – порядка 25 тыс. веб-серверов под управлением Linux, а, значит, и веб-сайты, которые ежедневно посещают миллионы человек. «Зомби» Windigo атакуют всех – пользователи Windows перенаправляются на набор эксплойтов, Mac-юзерам демонстрируется реклама сайтов знакомств, а с iPhone осуществляется переход на «взрослый» контент.

«Армия зомби», названная в честь духа-людоеда в мифологии индейцев-алгонкинов, продолжает поиск новых жертв в полном соответствии с привычками вечно голодного вендиго.

Некоторые ботнеты рейтинга считались неопасными, некоторые – уничтоженными. На самом же деле все они остаются в тени, ожидая шанса на возвращение. Эксперты ESET напоминают, что «зомби-сети» опасны для всех типов устройств, вне зависимости от используемого программного обеспечения. Защиту от «зомби» обеспечит дробовик современное антивирусное ПО с функцией ботнет-защиты ***(Рейтинг самых опасных «зомби-сетей» // InternetUA (http://internetua.com/reiting-samih-opasnih--zombi-setei). – 2014. – 2.11).***

***

Исследователи продолжают наблюдать за тем, как хакеры эксплуатируют уязвимость ShellShock для осуществления своей деятельности. Так, сразу две фирмы издали предупреждения безопасности, связанные с этой брешью – Trend Micro обнаружила атаки, нацеленные на SMTP-серверы, в то время как в Akamai заявили о создании ботнетов, жертвами которых становятся пользователи с необновленной версией bash. Обе компании разместили отчеты в своих блогах.

В то же время исследователи из Solutionary Security Engineering Research Team (SERT) опубликовали отчет, в котором сообщается о том, насколько быстро хакеры изменили методы атак для эксплуатации ShellShock. В нем сообщается, что 67 % трафика с сигнатурами ShellShock было связано с известными вредоносными источниками. Это означает, что

хакеры модифицировали собственные атаки для эксплуатации новой бреши. Более того, такие сигнатуры начали детектировать в первые 24 часа после обнародования деталей уязвимости.

Количество атак постоянно увеличивается и, как предсказывали исследователи, на первых порах наибольшая активность исходила от DDoS-ботнетов, эксплуатирующих ShellShock. Как сообщили специалисты Akamai, хакеры используют уязвимость в bash для создания ботнет-сетей. В большинстве таких сетей для контроля жертв используется протокол IRC. К такому же мнению пришли в Trend Micro, доказав, что преступники используют электронную почту для доставки вредоносного кода на SMTP-серверы, который устанавливает на них IRC-боты JST Perl Irc Bot. Для этого хакер посылает электронное письмо, содержащее вредоносный код в полях Subject, From, To и CC, на потенциально уязвимый сервер. Во время обработки такого сообщения происходит выполнение встроенного пэйлоада, после чего на сервер загружается IRC-бот, через который злоумышленник может получить полный контроль над взломанным сервером.

Единственный способ остановить распространение ботнетов – установить исправления, устраняющие уязвимость ***(Хакеры используют ShellShock для атак на SMTP-серверы и создания ботнетов // InternetUA (http://internetua.com/hakeri-ispolzuuat-ShellShock-dlya-atak-na-SMTP-serveri-i-sozdaniya-botnetov). – 2014. – 2.11).***

***

Согласно данным опроса, проведенного компанией Check Point, большинство IT-компаний (97 %) признают, что с трудом справляются с угрозами безопасности. При этом 87 % опрошенных считают, что наибольшую опасность представляет небрежное использование мобильных устройств сотрудниками предприятий. В опросе приняло участие 700 IT-компаний из США, Великобритании, Германии, Канады и Австралии.

Несмотря на то что небрежное использование мобильных девайсов является одним из самых серьезных факторов риска для безопасности компаний, 91 % респондентов отметили, что за последние два года количество подключений персональных мобильных устройств к корпоративным сетям только возросло.

Кроме того, в 2014 г. увеличились объемы ущерба, нанесенного компаниям в результате инцидентов мобильной безопасности. 42 % респондентов признались, что такие инциденты теперь обходятся их организациям не менее чем в 250 тыс. дол.

Факторами риска, вызывающими наибольшую обеспокоенность у IT-специалистов, оказались потеря или похищение информации (82 %), инфицирование вредоносными ПО (61 %), нарушение требований с последующими штрафами (43 %), а также стоимость замены потерянных или похищенных устройств (32 %) ***(97 % IT-компаний признают, что с трудом справляются с угрозами безопасности // InternetUA***

(http://internetua.com/97--IT-kompanii-priznauat--csto-s-trudom-spravlyauatsya-s-ugrozami-bezopasnosti). – 2014. – 2.11).

***

Злоумышленники научились похищать персональные данные американских подростков, используя фото их первых зарплатных чеков в Instagram. Об этом сообщает журнал Oystermag.

У американских подростков вошло в моду фотографировать свои банковские чеки с первой зарплатой и выкладывать их в Instagram, снабжая фотографии хэштегом #myfirstpaycheck.

С помощью этих фото злоумышленники копировали персональные данные и дизайн чеков и впоследствии использовали их для открытия поддельных счетов, а также обналичивания новых фиктивных платёжных документов.

Федеральные прокуроры штата Миннесота выдвинули обвинения против 28 человек, участвовавших в сговоре с целью наживы на поддельных чеках из Instagram. Как сообщает CNN, в общей сложности обвиняемые украли более двух миллионов долларов.

Несмотря на произошедшее, фото чеков, снабженные хэштегом #myfirstpaycheck, продолжают появляться в социальной сети Instagram.

Утечки личных данных студентов происходили и ранее. 21 октября в сеть попала информация более 100 тыс. пользователей сервиса NeedMyTranscript.com. Об этом сообщает газета The Washington Post.

Веб-сайт NeedMyTranscript.com используется для быстрого получения и отправки записей из учебных заведений. Среди попавшей в сеть информации были имена студентов, их домашние адреса, номера телефонов, даты рождения, адреса электронной почты, девичьи фамилии матерей и последние цифры номеров социального страхования ***(Мошенники нашли способ красть личности подростков через Instagram // InternetUA (http://internetua.com/moshenniki-nashli-sposob-krast-licsnosti-podrostkov-cserez-Instagram). – 2014. – 1.11).***

***

За год мощность DDoS-атак возросла в четыре раза, в соответствии с новым отчётом Q3 2014 State of the Internet от компании Akamai. Эта компания публикует ежеквартальные отчёты о глобальных тенденциях в Интернете. За прошедшие месяцы с начала года ей пришлось защищать своих клиентов от атак, среди которых 17 штук превысило 100 ГБ/с, а самая серьёзная достигла 321 ГБ/с.

«Размер и мощность DDoS-атак в этом году превысила все возможные пределы», – говорит Д. Саммерс, вице-президент подразделения безопасности в Akamai. Он добавил, что в III квартале прошлого года не было зарегистрировано ни одной атаки больше 100 ГБ/с, тогда как в III квартале текущего года таких было шесть штук.

В общей сложности, количество DDoS-атак в этом году возросло на 22 %, а их мощность увеличилась на 366 %, то есть более чем в четыре раза, если сравнивать два аналогичных квартала в этом и прошлом году.

Даже по сравнению с прошлым II кварталом мощность DDoS-атак увеличилась очень значительно: на 80 %. При этом злоумышленники используют более продвинутые техники. В частности, в 53 % случаев применялись многовекторные атаки. Специалисты Akamai связывают это с большей доступностью программ с простым интерфейсом, с помощью которых запускается DDoS. Таким образом, этой деятельностью может заниматься больше людей. Ситуация усугубляется увеличением количества коммерческих заказов на такие атаки. К тому же, неблагоприятную обстановку создаёт наличие немалого количества уязвимых устройств, в том числе смартфонов, кабельных и DSL-модемов, планшетов и других гаджетов, принимающих участие в DDoS-атаках ***(DDoS-атаки за год стали мощнее в 4 раза // InternetUA (http://internetua.com/DDoS-ataki-za-god-stali-mosxnee-v-4-raza). – 2014. – 31.10).***