СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(25.02–10.03)

2014 № 5

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(25.02–10.03)
№ 5

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

Компанія Gemius Україна представила ТОП-20 сайтів Уанету за січень 2013 р. ТОП-5 сайтів з минулого місяця не змінилися: Google.com, Mail.ru, Vk.com, Yandex.ua, Youtube.com.

Facebook перебуває на 8-му місці, «Одноклассники» – на 9-му.

Близько 6 млн українців у січні хоча б один раз відвідували Facebook та 11 млн – «ВКонтакте».

Згідно з даними gemiusAudience (fusion panel), розмір інтернет-аудиторії в січні 2014 р. перевищив 17,8 млн осіб (real users, 14+). Дослідження складено на основі 7083 анкет software-панелістів та 46 648 анкет cookie-панелістів.

Fusion-панель (змішана панель) у дослідженні gemiusAudience – об'єднує cookie-панель і software-панель.

Охоплення – відсоткове співвідношення кількості відвідувачів (реальних користувачів), що здійснили принаймні один перегляд сторінки на вибраному сайті за цей часовий інтервал, до загальної кількості інтернет-користувачів за цей часовий інтервал ***(Близько 6 млн українців в січні хоча б 1 раз відвідували Facebook та 11 млн – «ВКонтакте» // UkrainianWatcher (http://watcher.com.ua/2014/02/26/blyzko-6-mln-ukrayintsiv-v-sichni-hocha-b-1-raz-vidviduvaly-facebook-ta-11-mln-vkontakte/). – 2014. – 26.02).***

***

Социальная сеть Facebook откажется от собственного сервиса электронной почты. Об этом сообщает интернет-издание The Verge.

Пользователи соцсети стали получать уведомления о предстоящем закрытии почтовых ящиков на @facebook.com. Направленные по одну из таких адресов письма теперь автоматически перенаправляются на основный e-mail пользователя, который указывается им при входе в Facebook. Если пользователь не указал при регистрации электронный адрес и для входа в соцсеть вводит номер своего телефона, система перенаправлений работать не будет.

В самом Facebook подтвердили планы по постепенному закрытию почтового сервиса. Окончательно электронные почтовые ящики @facebook.com будут удалены в марте. По словам представителя компании, закрыть сервис решили из-за его непопулярности. «Большинство людей не пользовались своими @facebook.com-адресами», – заявили в соцсети.

Собственный почтовый сервис появился в Facebook в 2010 г. Главной особенностью сервиса была его способность объединять в одном месте все внутренние сообщения, отправляемые в самой соцсети, SMS, электронные письма, а также тексты бесед из чатов. Представляя @facebook.com, основатель Facebook М. Цукерберг заявлял, что не собирается конкурировать с другими почтовыми сервисами, а считает @facebook.com «дополнительной

почтой». Помимо стандартных адресов @facebook.com в соцсети также действовали и короткие адреса @fb.com. Ими пользовались сотрудники социальной сети ***(Facebook закроет собственный почтовый сервис // InternetUA (http://internetua.com/Facebook-zakroet-sobstvennii-pocstovii-servis). – 2014. – 25.01).***

***

В Таджикистане запустили социальную сеть под названием «Парта.tj». Как отмечается на главной странице ресурса, сайт призван стать универсальным средством для общения, а также поиска друзей и одноклассников.

Чтобы зарегистрироваться на «Парте», достаточно ввести фамилию, имя, дату рождения, пол и страну проживания. При этом в качестве места жительства можно указать только Таджикистан. Далее пользователю предлагается указать адрес электронной почты, придумать пароль и загрузить аватар на свою личную страницу.

На момент написания этой заметки в соцсети было зарегистрировано немногим более 800 человек. Первым пользователем сайта, судя по всему, стал его администратор: страница с адресом parta.tj/u1 принадлежит человеку с именем Admin Admin. Второй пользователь соцсети – житель города Исфара А. Шокиров. При этом в его профиле указан мобильный телефон с префиксом +7983. Подобный префикс используется российским оператором МТС в некоторых регионах Сибири, что позволяет заключить, что молодой человек скорее всего не проживает в Таджикистане.

Пользовательский интерфейс «Парты.tj» во многом копирует внешний вид другой популярной соцсети – «ВКонтакте». К примеру, таджикский ресурс использует в оформлении цвета и шрифт российского сайта. Кроме того, тексты служебных сообщений во многих разделах «Парты» полностью идентичны таким же сообщениям во «ВКонтакте». Так, в разделе «Видео» указывается, что «вы можете хранить неограниченное количество видеофайлов». Точно такой же текст можно увидеть и в соответствующем разделе «ВКонтакте».

О намерении создать для жителей собственную национальную социальную сеть неоднократно заявляли власти Таджикистана, однако этот проект так и не был реализован.

Зарубежные соцсети (Facebook, «ВКонтакте» и Twitter) часто подвергаются в Таджикистане блокировке. В ноябре 2013 г. в стране также временно был ограничен доступ к видеохостингу YouTube. Отключение сайта совпало с проведением в стране выборов президента ***(В Таджикистане запустили «клон» «ВКонтакте» // InternetUA (http://internetua.com/v-tadjikistane-zapustili--klon---vkontakte). – 2014. – 25.02).***

***

Ericsson и Facebook объявили о создании совместной Инновационной Лаборатории (Innovation Lab), которая будет поддерживать инициативу Internet.org.

Инновационная Лаборатория проекта Internet.org, результат сотрудничества Ericsson и Facebook, обеспечит условия и экспертный опыт для оптимизации приложений, сетей, устройств и сервисов для 5 млрд будущих интернет-пользователей.

Новая лаборатория, открытие которой запланировано на вторую половину 2014 г. на территории Facebook в Менло-Парке (Калифорния), будет заниматься решением самых важных вопросов для достижения цели Internet.org – сделать доступ в Интернет возможным для всех.

Опираясь на возможности сервисов Ericsson Device и Application Verification, а также технологическое лидерство компании в развитии мобильных сетей, Ericsson обеспечит Facebook и разработчиков приложений возможностью смоделировать условия для работы в разных сетях во всем мире. Это позволит им построить и протестировать работу новых мобильных приложений и услуг.

«Благодаря этой лаборатории у разработчиков появится возможность смоделировать работу в разных сетевых средах, которые характерны для новых рынков, обеспечивая им условия для тестирования и оптимизации работы своих приложений в разных условиях, – прокомментировал Д. Парих, вице-президент Facebook по проектированию инфраструктуры. – Это уникальная возможность, которую предоставляет Ericsson, и мы рады, что они вместе с нами взяли на себя лидирующую роль в развитие этой инициативы».

Лаборатория поможет избавиться от ключевых физических препятствий, которые существуют на пути предоставления доступа в Интернет повсеместно. На сегодняшний день разработчики имеют возможность работать в сетевой среде лишь с физическим присутствием в ней. Учитывая, что пользователи по всему миру работают в разных сетевых средах (2G, 3G, 4G, Wi-Fi) на множестве мобильных операционных систем и широком круге устройств, сложности, с которыми сталкиваются разработчики, могут стать непреодолимы. Совместная инновационная лаборатория упростит доступ к разнообразным сетевым средам с целью их тестирования и оптимизации в одном месте.

Проект Internet.org, анонсированный в августе 2013 г., был создан с целью обеспечить доступ в Интернет для двух третей населения планеты, которые еще не подключены к сети, и предоставить им такие же возможности, которыми пользуется уже подключенная треть населения. Ericsson имеет более чем 100-летний опыт работы, направленной на преодоление цифрового неравенства, и реализации программы Technology for Good.

«Цель Internet.org соответствует нашему многолетнему видению, согласно которому коммуникация – базовая потребность человека, – отметил Й. Уиберг, старший вице-президент сетевого подразделения Ericsson. – Создание лаборатории позволит обеспечить уникальные условия для тестирования и, в конечном счете, оптимизации приложений независимо от сети, устройства или операционной системы. Сотрудничество с разработчиками даст Ericsson бесценные знания об их требованиях к сетевой среде, которые мы сможем использовать для обеспечения дальнейшего развития сетей с наилучшей производительностью по всему миру».

Услуга, которая представлена в рамках Mobile World Congress 2014, позволит разработчикам приложений, производителям устройств и чипсетов, а также другим игрокам рынка мобильных и фиксированных телекоммуникационных услуг, проводить тестирование и проверку устройств и приложений в фиксированных сетях и мобильных сетях 2G, 3G и LTE ***(Ericsson и Facebook создали лабораторию для развития проекта Internet.org // ITnews (http://itnews.com.ua/news/71738-ericsson-i-facebook-sozdali-laboratoriyu-dlya-razvitiya-proekta-internetorg). – 2014. – 25.02).***

***

Социальная сеть Facebook объявила о закрытии двух версий Messenger для операционной системы Windows и браузера Firefox. «Сожалеем, но отныне мы не можем поддерживать Facebook Messenger для Windows», – сказали в компании, не пояснив причины такого решения. Сервис прекратит работу 3 марта.

Менее чем через сутки компания заявила, что в следующий понедельник она также «убьет» версию Messenger для Firefox. Для загрузки уже недоступны ни установочный файл Windows-приложения на официальном сайте, ни расширение для браузера в магазине Mozilla.

Messenger вышел в августе 2011 г. Он совместим с операционными системами Android, iOS и BlackBerry. Приложение работает отдельно от основного клиента Facebook и представляет собой коммуникационный хаб, объединяющий в себе сообщения, электронную почту и групповой чат.

Очевидно, «настольные» клиенты не пользовались должной популярностью у пользователей, поэтому компания решила их закрыть, а освободившиеся силы бросить на поддержку мобильных версий Messenger для iOS/Android, которые регулярно обновляются (последний апдейт датируется 20 февраля). Кроме того, несколько дней назад на выставке MWC 2014 было объявлено о том, что вскоре Messenger выйдет на платформе Windows Phone ***(Facebook избавляется от «настольных» мессенджеров // InternetUA (http://internetua.com/Facebook-izbavlyaetsya-ot--nastolnih--messendjerov). – 2014. – 28.02).***

***

Сообщество профессионалов LinkedIn официально выходит на китайский рынок. Известно, что социальная платформа будет продвигаться на территории Китая под брендом «Лин Ин» и, по оценкам специалистов, сможет привлечь до 140 млн новых пользователей.

Отметим, что попытки ближайших конкурентов LinkedIn – Facebook, Twitter и Google запустить бета-версию сайта на китайском языке не увенчались успехом. Что же касается LinkedIn, то сегодня социальной сетью пользуются всего 4 млн китайцев, хотя она доступна в Китае уже более десятка лет.

Учитывая, что в настоящее время общее число пользователей LinkedIn составляет 277 млн человек – официальный выход на рынок Китая позволит социальной платформе существенно расширить аудиторию.

«Наша цель – предоставить китайским профессионалам возможность общения с их коллегами и партнёрами из более чем 200 стран. За последние пять лет в Китае наблюдался устойчивый рост ВВП, было создано свыше 50 млн рабочих мест в городах, и значительно возрос доход на душу населения жителей страны. Сегодня Китай – одна из наиболее важных, в экономическом отношении, стран в мире. Учитывая такой быстрый рост и развитие китайской экономики, внедрение китайской версии нашего сайта – это значительный шаг в достижении нашей глобальной цели – объединения профессионалов всего мира», – заявляет в блоге Д. Вейнер, CEO LinkedIn.

Он также отмечает, что существующая в Китае цензура противоречит политике LinkedIn, которая решительно поддерживает свободу слова. Однако если LinkedIn откажется от выхода на данный рынок, – это ограничит не только экономические возможности для граждан Китая, но и их права и свободы, а специалисты США и других стран не смогут общаться и обмениваться опытом со своими китайскими коллегами.

Д. Вейнер также заверил, что компания будет предпринимать активные меры по защите прав и охране персональных данных своих пользователей ***(Социальная сеть LinkedIn выходит на рынок Китая // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/sotsialnaya_set_linkedin_vyhodit_na_rynok_kitaya). – 2014. – 5.03).***

***

Будущее социальных сетей

Тотальная мобилизация – свершившийся факт. Этому способствовали широкое распространение скоростной беспроводной связи, доступность и миниатюризация устройств, увеличение времени их работы без подзарядки. Хотя значительное увеличение емкости батарей и снижение энергопотребления – все еще вопрос будущего, появление доступных гаджетов, которые удобно постоянно держать при себе, и распространение широкополосной связи сыграли свою роль в том, чтобы человечество «пересело» с компьютеров на смартфоны и планшеты. Чем больше у

пользователей возможностей быстро и желательно бесплатно выйти в Интернет, тем чаще они этим пользуются.

Совершенно естественно, что распространение мобильных устройств влияет на развитие социальных сетей. Крупные соцсети – «Мой Мир», «Одноклассники», «ВКонтакте», Facebook и др. – переносят свои объемные возможности в мобильные приложения.

В то же время мы наблюдаем рост нишевых социальных сервисов, «заточенных» под мобильные устройства, которые не стремятся собрать все функции, а созданы для конкретной аудитории с определенными запросами. Например, BAND: разработчики позиционируют его как приложение для объединения реальных друзей и близких в социальные группы. Также в индустрии есть социальные сервисы, которые не являются сетями в строгом смысле этого слова, но при этом обеспечивают обмен информацией между пользователями. Хороший пример такого явления – Instagram, приложение для обмена фотографиями, которое затем обросло дополнительными возможностями.

Конечно, нишевые сервисы – это не те социальные сети, которые мы увидели восемь лет назад (осенью 2006 г. администрация Facebook открыла доступ для всех пользователей Интернета). Однако это социальные сети в том смысле, что пользователи приходят туда в поисках общения, информации, самовыражения, обмена эмоциями и мнениями. Рост популярности и добавление функций приводит к перераспределению пользователей между существующими интернет-сервисами. Например, многие люди, которые давно пользуются Instagram, могут не иметь аккаунта в возможно громоздких и непонятных для них Facebook или «ВКонтакте».

Раньше пользователи обращались к социальным сетям для того, чтобы восстановить или поддержать контакт с друзьями, одноклассниками, сокурсниками, родственниками из другого города и т. д. Основной целью при этом было пообщаться с теми, с кем они знакомы в реальном мире. Люди продолжают общаться в соцсетях, но теперь они намного активнее пользуются всеми остальными функциями: вслед за общением на первый план вышли общие интересы, пользователи начали делиться контентом – музыкой, фотографиями и др. Социальные сети превратились из средства взаимодействия в точку входа в Интернет, место, где пользователь получает основную массу информации.

Это заметно по тому, как пользователи работают с аккаунтами в социальных сетях. Например, меняется соотношение постов с фотографиями и ссылками. Фотоконтент по-прежнему очень популярен в соцсетях, однако ситуация меняется. Теперь пользователи активнее делают перепосты, делятся ссылками на другие материалы в сети. Тенденцию отмечают и используют крупные игроки рынка, которые видят будущее именно в том, что их клиенты будут использовать социальную сеть как канал для потребления контента. Примером этому может служить новое приложение от Facebook под названием Paper, смещающее акцент с собственно общения на получение

новой информации. Тенденция также хорошо заметна в «Моем Мире»: в сети растет количество контентных групп с интересным содержанием, и внимание пользователей смещается с личных записей на редакторские, полупрофессиональные материалы и статьи.

Разработчики приложений ныне отдают предпочтение так называемому flat-дизайну. Под этим подразумевается максимальное «уплощение» интерфейса и использование простых и легких для восприятия форм, которые облегчают восприятие собственно информации, размещенной на ресурсе или в приложении. На самом деле стремление к «уплощению» было всегда, а то, что в настоящее время оно превратилось в один из трендов индустрии – просто очередной шаг к закреплению за контентом главенствующей роли. Собственно, тренд заключается как раз в том, что разработчики переносят акцент с элементов управления на сам контент. Можно для сравнения взять игру 1995 г.: мы увидим маленький экранчик с ажурным интерфейсом вокруг.

В «Моем Мире» мы также внимательно следим за происходящими изменениями в привычках пользователей и меняемся вслед за ними. Недавно мы провели редизайн «Моего Мира», основываясь на статистике использования: какие элементы интерфейса задействованы, какие нет. Мы убрали лишние элементы и улучшили навигацию по имеющимся активностям и контенту. На пике популярности в сети остаются игры, а за ними следует видео. При этом обработка и хранение фотографий остаются одной из самых популярных активностей не только в «Моем Мире», но и в других соцсетях.

Через некоторое время мы можем ожидать большой скачок популярности видео, которое пока только набирает обороты. Видеороликам необходима экосистема, в которой заняты несколько игроков. Для просмотра требуется наличие подходящего устройства, сервиса, способного воспроизвести фильм, а также медиасреда, основное свойство которой – высокая скорость и доступность соединения, позволяющие смотреть видео всегда и везде, без серьезных затрат. Немаловажны также договоренности с производителями видеоконтента. В роли последних могут выступать как крупные студии вроде голливудских компаний, отдельные люди, выкладывающие ролики на YouTube, или действующие лица онлайн-трансляций с Ustream. Все это влияет на применение видео как канала информации: для того чтобы все игроки пришли к согласию между собой и пользователь мог получить контент, требуется время. Этот процесс уже идет, клиенты интернет-сервисов обучаются применять этот канал, и в России момент насыщения этой отрасли наступит примерно через два года. В других частях мира ситуация складывается по-своему: в Японии и Южной Корее это очень популярная форма подачи контента, в Европе – еще нет.

Периодически в интернет-сервисах появляются тренды, которым пророчат огромную популярность, а на поверку эта преждевременная слава оказывается сильно преувеличенной. Один из таких трендов – геолокация, о

которой несколько лет назад твердили, что она станет ключевой «фишкой» приложений. Но не сложилось: эта функция заняла место среди других обычных дополнений, однако сама по себе не стала определяющей. В 2009–2010 гг. пророчили бум «геймификации», однако этого также не произошло.

В течение последующих двух лет настоящим фаворитом в сфере социальных сервисов станет уже упомянутый видеоконтент. Кроме того, популярность должны набрать приватные сети, в которых количество читателей ограничено самим пользователем по тем или иным показателям. Такая функция есть в Google+, однако ее интерфейс очень сложен. В принципе, во всех крупных социальных сетях можно настроить приватность таким образом, чтобы разделить свою аудиторию по некоторым признакам, однако для этого нужно приложить массу усилий. Неизбежно должны появиться и набрать популярность сервисы, где функции создания приватных групп уделено основное внимание. Возможно, они вырастут из групповых чатов или придут со стороны социальных сетей: откуда они в итоге появятся – покажет время ***(Алаев Д., руководитель социальной сети «Мой Мир»: Будущее социальных сетей // ComNews (http://www.comnews.ru/node/80959). – 2014. – 4.03).***

***

Разработанное социальной сетью Facebook приложение «Мессенджер», предназначенное для электронной переписки, вышло на устройствах на базе Windows Phone. Об этом 5 марта сообщается в блоге операционной системы.

Бесплатную программу, которая доступна на 31 языке, включая русский, можно загрузить в интернет-магазине. «Мессенджер» позволяет отправлять друзьям из соцсети сообщения, фотографии, геометки и «картинки-стикеры».

На Windows Phone «Мессенджер» появился на два года позже, чем на конкурирующих платформах. Кроме того, в программе есть не все функции, доступные на Android и iOS: так, нельзя совершать звонки и отправлять голосовые сообщения.

За последний год на Windows Phone были «перенесены» многие популярные программы из Google Play и App Store: например, приложение для обмена видеороликами Vine, фотоприложение Instagram и навигатор Waze.

Платформу Windows Phone корпорация Microsoft развивает с 2010 г. Крупнейшим производителем устройств на этой ОС является Nokia. В сентябре Microsoft объявила, что купит мобильный бизнес финской компании ***(Мессенджер Facebook заработал на Windows Phone // Версии.com (http://www.versii.com.ua/news/298762/). – 2014. – 6.03).***

***

Пользователям «ВКонтакте» стала доступна новая система уведомлений о непрочитанных сообщениях. Об этом на своей странице сообщил пресс-секретарь социальной сети Г. Лобушкин.

По его словам, вместо уведомления о непрочитанных сообщений теперь пользователи будут видеть уведомления о непрочитанных диалогах. Например, если в меню слева будет виден значок «+1», значит, пользователю пришли сообщения от одного абонента или из одного чата. Значок «+2» означает, что у него есть два диалога с непрочитанными сообщениями.

Непрочитанные сообщения, как и ранее, помечаются другим оттенком, отмечает Г. Лобушкин. Кроме того, к ним добавилась иконка, отображающая количество непрочитанных сообщений в каждом из чатов. Зайдя в тот или иной диалог, пользователь будет автоматически перемещен к первому из непрочитанных сообщений.

На сегодняшний день новая система, которая «окончательно обесценивает старую систему сообщений», доступна не всем пользователям, а только небольшой ее части – увидеть работу новых сообщений может примерно миллион участников соцсети.

В ближайшее время нововведение появится как в мобильных клиентах «ВКонтакте», так и на мобильной версии сайта. После этого старый интерфейс личных сообщений будет окончательно отключен, подчеркивают администраторы ресурса ***(«ВКонтакте» запустил новую систему переписки // InternetUA (http://internetua.com/vkontakte--zapustil-novuua-sistemu-perepiski). – 2014. – 7.03).***

***

Социальная сеть «ВКонтакте» рассматривает возможность присоединения к так называемому антипиратскому меморандуму Роскомнадзора.

Как заявил вице-президент социальной сети Д. Сергеев, в настоящее время руководством компании проводятся переговоры и консультации с представителями надзорного ведомства и правообладателями. По некоторым данным, подписание документа может состояться уже в мае 2014 г., в рамках Петербургского международного экономического форума.

То, что соцсеть не исключает возможности подписания меморандума, «Ленте.ру» подтвердили и в пресс-службе компании. «Мы рассматриваем такую возможность, но говорить об этом пока рано», – сообщил пресс-секретарь «ВКонтакте» Г. Лобушкин.

Антипиратский меморандум был подписан по инициативе Роскомнадзора рядом крупных компаний в декабре 2013 г. Основная цель меморандума – упростить сотрудничество представителей IT-сферы и правообладателей в области защиты авторских прав. Меморандум обязывает компании разместить на своих сайтах информацию с призывом отказаться от пиратства и уважать интеллектуальную собственность, а также принимать

меры в отношении пользователей, систематически нарушающих законодательство.

Со стороны правообладателей к меморандуму присоединились Первый канал, ВГТРК, ТНТ, «Национальная Медиа Группа», компания «Амедиа» и ряд других компаний. Со стороны IT-индустрии документ подписали Mail.ru, RuTube, а также интернет-кинотеатры Ivi, Stream и Megogo. Крупнейшие поисковики «Яндекс» и Google отказались от подписания меморандума, заявив, что у них существует собственная процедура взаимодействия с правообладателями ***(«ВКонтакте» задумался о подписании антипиратского меморандума // InternetUA (http://internetua.com/vkontakte--zadumalsya-o-podpisanii-antipiratskogo-memoranduma). – 2014. – 7.03).***

***

Социальная сеть Facebook начала обновление внешнего вида своей новостной ленты (News Feed). Сообщение об этом 7 марта появилось в официальном блоге Facebook for Business.

Изменения коснутся размера фотографий, отображающихся в ленте (в новой версии они станут больше) и использующегося на странице шрифта. Также сменится и общий фон News Feed – посты и ссылки с трендами в ленте по-прежнему будут отображаться на белом фоне, однако остальные элементы (к примеру, колонка с ссылками на профиль пользователя, группы и события) теперь будут показываться на сером фоне.

Суть изменений авторы блога описали так: «Макет и навигация, которые понравились людям, сохраняться, но изменится шрифт и картинки станут больше».

Как отметили представители соцсети, размеры рекламных блоков новостной ленты останутся прежними. В целом, внедрение редизайна займет несколько недель и затронет только версию соцсети для браузеров – дизайн мобильных версий ресурса останется прежнем. При этом, по словам администрации Facebook, алгоритм отображения постов в News Feed останется неизменным.

В марте 2013 г. Facebook уже объявлял о масштабном визуальном редизайне новостной ленты. Тогда соцсеть также анонсировала увеличение размера фотографий и видео в ленте, а также появление в левой части страницы вертикальной панели управления. Тем не менее, как теперь сообщили в соцсети, та версия была признана неудобной и от нее решено было отказаться.

Новостная лента Facebook News Feed появилась в социальной сети в 2006 г., спустя два года после запуска сайта. До этого, заходя на ресурс, пользователи попадали на страницу с собственным профилем. Вместо этого решено было стартовой страницей сделать раздел с новостями, в котором собирались все посты друзей, обновления их статусов, комментарии, сообщения о событиях, днях рождения и т. д.

Изначально появление ленты было встречено многими пользователями негативно. Пользователи жаловались на «замусоренность» Facebook слишком большим количеством информации и угрожали отказаться от пользования соцсетью. если компания не вернет прежний дизайн ***(Facebook объявил о редизайне новостной ленто // InternetUA (http://internetua.com/Facebook-ob-yavil-o-redizaine-novostnoi-lenti). – 2014. – 7.03).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Сервіс мікроблогів Twitter візуалізував на карті світу обговорення користувачами соцмережі подій в Україні. Посилання на візуалізацію в ніч на 3 березня було опубліковане в микроблозі @TwitterData, пише Корреспондент.net (http://ua.korrespondent.net/ukraine/events/3313958-u-Twitter-opublikuvaly-svitovu-kartu-obhovorennia-podii-v-ukraini).

Складена Twitter карта охоплює твіти про політичні протести в Україні, відправлені користувачами сервісу з 1 по 25 лютого 2014 р.

Судячи з візуалізації Twitter, найбільша кількість твітів, пов'язаних з подіями в Україні, припадає на останній тиждень лютого. Окрім самої України, події Майдану в ці дні також активно обговорювалися в США, Великобританії, Німеччині, Франції та Росії.

У зв'язку з подіями в Україні, у Twitter з'явилася ціла низка акаунтів і хештегів, пов'язаних з Майданом. Одним з найпопулярніших акаунтів став мікроблог @euromaidan, що зібрав близько 100 тис. передплатників ***(У Twitter опублікували світову карту обговорення подій в Україні // Корреспондент.net (http://ua.korrespondent.net/ukraine/events/3313958-u-Twitter-opublikuvaly-svitovu-kartu-obhovorennia-podii-v-ukraini). – 2014. – 3.03).***

***

Після того як 24 лютого сесія Кіровоградської міської ради змінила назву центральної площі міста ім. Кірова на Героїв Майдану, вулицю Дзержинського на вул. Чміленка, вул. Медвєдєва на вул. Ельворті та вул. Орджонікідзе на вул. Кавалерійська, у соціальних мережах активно обговорюється питання заміни назви міста Кіровоград.

Наші кореспонденти вибрали всі ті назви, що сьогодні пропонують кіровоградці, і не лише, на заміну теперішній. Наразі список виглядає так: Єлисаветград, Єлисавет, Златопіль, Інгульськ, Байгород, Буго-Гардієвськ, Лелеківськ, Тобілевичі, Майдан, Чміленківськ, Степоград, Калнишевськ ***(Список назв, які пропонують в соціальних мережах на заміну Кіровограду // Весь Кіровоград***

(http://www.kirovograd.net/shortly/2014/2/25/spisok_nazv_jaki_proponuyut_v_socialnih_merezhah_na_zaminu_kirovogradu.htm). – 2014. – 25.02).

***

Відомий український журналіст М. Найєм став першим в Україні користувачем Facebook, якого читають понад 100 тис. користувачів.

Велику частину нових прихильників М. Найєм здобув за останні три місяці. З листопада 2013 р. він додав близько 70 тис. нових фолоферів.

Протягом тривалого часу М. Найєм перебував на другому місці в рейтингу українських користувачів Facebook, трохи поступаючись В. Кличку. Але в грудні В. Кличко перевів свою сторінку з приватного профілю в сторінку (на сьогодні В. Кличко має близько 70 тис. прихильників на своїй сторінці). З того часу М. Найєм є безумовним лідером рейтингу ***(Мустафа Найєм: першим в Україні набрав 100 тис. фоловерів у Facebook // UkrainianWatcher (http://watcher.com.ua/2014/03/04/mustafa-nayyem-pershym-v-ukrayini-nabrav-100-tys-foloveriv-u-facebook/). – 2014. – 5.03).***

***

Офіційна сторінка «новоспеченого» голови Рівненської облдержадміністрації С. Рибачка з'явилася в соціальній мережі «ВКонтакте». Акаунт має поки що мінімум інформації – дату народження, освіту, сімейний стан. Про це повідомляє портал ERVE.UA.

За інформацією видання, акаунт «ВКонтакте» веде, як це часто буває, не сам голова, а його прес-секретар. Інформація про останнього – хто він, чи вона – поки що невідома. Але обіцяють найближчим часом цю особу розсекретити – після офіційного призначення.

Поки що офіційне представництво голови ОДА «ВКонтакте» виглядає не надто привабливо. Всі пости від голови – це публікації про нього на рівненських сайтах, у тому числі є чимало посилань на ERVE.UA. Тому цілком можливо, що вже найближчим часом групами С. Рибачка в соцмережах почнуть займатися наймані профі, як це часто буває.

Куди популярніша сторінка С. Рибачка в мережі Facebook, яка була започаткована давно. Там він має понад 440 друзів і вочевидь веде її особисто. Але, сподіваємося, це лише до моменту нового призначення, адже на посту голови ОДА, маємо надію, у нього на соцмережі часу не буде ***(Рибачок записався в соцмережі // ІА «Ервеюей» (http://erve.ua/news/politics/ribachok_zapisalsya_in_simeri_photo_fact_0703/). – 2014. – 7.03).***

***

На сторінці Міністерства оборони у Facebook усіх небайдужих просять підтримати листами українських військовослужбовців.

«До нас надходить дуже багато ваших листів з теплими і щирими словами підтримки для наших військовослужбовців. Ми ці листи

обробляємо, сортуємо, відправляємо до прес-служби ВМС ЗСУ, військових частин. Крім того, зараз налагоджуємо зв'язок з радіо, аби вони озвучили ваші листи в ефірі. Виставляємо дещо тут, бо наші хлопці іноді "заходять" в онлайн і читають все, що їм пишуть», – ідеться в повідомленні міністерства.

Водночас у відомстві зазначають, що хочуть використати всі можливі канали.

«Можливо, серед вас є хтось, хто проживає неподалік заблокованих військових частин і має можливість роздрукувати деякі листи, щоб передати нашим героям? Якщо ви маєте бажання допомогти, надішліть листа на адресу lustu_vijskovum@ukr.net, з вами зв'яжуться», – зазначають у Міноборони ***(Українці підтримують військових через Facebook // InternetUA (http://internetua.com/ukra-nc--p-dtrimuuat-v-iskovih-cserez-Facebook). – 2014. – 5.03).***

***

Исследование компании Gemius показывает, что в результате политических событий, которые в настоящее время разворачиваются в Украине, был отмечен рост интернет-трафика на Facebook и Twitter, а также на сайтах служб новостей и необщественных телевизионных станций. Своими позициями поступились такие местные игроки, как «ВКонтакте» и «Одноклассники», а также веб-страницы общественных телевизионных станций.

Ночь 21 ноября 2013 г. была началом акции протеста на площади Независимости в Киеве, которая вскоре переросла в Евромайдан – волну демонстраций и протестов, которая накрыла почти всю Украину, затронув и Интернет.

Так как политические волнения повлияли на интернет-трафике соцсетей и сайтов СМИ?

Ключевая роль социальных медиа

В октябре 2013 г. на Facebook.com заходило только 29 % украинских интернет-пользователей, что почти в два раза меньше, по сравнению с показателем посещения соцсети «ВКонтакте» (61 %). Однако в январе 2014 г., индекс посещений возрос до 32 %.

Популярность Twitter тоже возросла – данным сервисом микроблогинга, в январе 2014 г., пользовались более 13 % интернет-аудитории. До начала протестов, в октябре 2013 г., этим сервисом интересовались всего 10 % украинских пользователей.

В то время, когда международные сервисы набирали популярность, самая популярная в Украине соцсеть «ВКонтакте» – немного сдала свои позиции (особенно под конец 2013 г.).

В октябре прошлого года, то есть до начала акции протеста, VK.com посетили более 61 % интернет-аудитории (61,27 %), а вот в декабре 2013 г. этот показатель снизился до почти 58 %.

Однако, после январских событий на Майдане, сайт всё же вернулся на прежние позиции, и более того – показал лучший результат посещаемости в 62 %.

Что касается сайта odnoklassniki.ua, то здесь события на Майдане не оказали на него никакого заметного влияния.

Повышенная активность на сайтах новостей

Ежедневный анализ активности интернет-пользователей на протяжении ноября, декабря и января показывает, что в ходе событий на Евромайдане, время, проведенное пользователями в соц-сетях, увеличилось. Это хорошо заметно при анализе трафика сервиса Twitter (39 мин., проведенные в октябре 2013 г., против 1 ч. 26 мин. за январь 2014 г.).

То же самое касается и новостных сервисов. В январе 2014 г., приблизительно 51 % интернет-пользователей заходили на данные веб-сайты, что почти на 5 % больше, чем до начала акции протестов (46 %).

Наблюдая за последними новостями, пользователи потратили 3 ч. и 3 мин., что тоже почти в два раза больше, чем время, потраченное в октябре – 1 ч. и 31 мин.

Вместо традиционного телевидения – прямые онлайн-трансляции и потоковое воспроизведение

Во время упомянутых событий украинские онлайн-телеканалы также вышли из тени. Ещё недавно, в октябре и ноябре 2013 г., популярность этих сервисов была очень слабой. В декабре 2013 г., например, только 10 % со всех интернет-пользователей посещали веб-сайты некоторых ведущих ТВ-станций. А вот в январе 2014 г. этот показатель явно возрос, и составил порядка 15 %.

В то же время популярность веб-сайтов общественного телевидения всё время падала. В октябре 2013 г. их посетили около 14 % интернет-пользователей, тогда как в январе уже следующего года показатель был меньше 12 % ***(Исследование: Как события Евромайдана отразились на трафике соцсетей и сайтах СМИ в Украине // Блог Imena.UA (http://www.imena.ua/blog/euro-soc). – 2014. – 5.03).***

***

У соцмережах українців закликали підняти прапор країни – безстрокова акція єдності.

У всіх областях країни стартує акція під назвою «Україна піднімає прапори». Про початок акції оголосили в соціальних мережах прихильники єдиної і неподільної країни, пише ZN.ua.

«Кожен, кому небайдуже – приєднуйтесь і покажіть, що ми – українці», – ідеться в заклику.

У повідомленні організаторів акції підкреслюється, що два найважливіші кольори можуть замінити тисячу слів. «Повісь прапор. Не так важливо, яким він буде – великим полотнищем на балконі або маленьким

прапорцем з магазину канцтоварів на антені авто. Настільним прапорцем на підвіконні, біля вікна, або синьо-жовтою стрічкою на сумці. Ось позиція і небайдужість. Ось перемога над зневірою, якої через край. І от віра в майбутнє України – в те, що вона єдина і неподільна», – ідеться в повідомленні.

Акція починається 7 березня і може тривати стільки, скільки українці вважатимуть за потрібне.

Для того, щоб взяти участь в акції, достатньо вивісити український прапор у себе на балконі чи у вікні, встановити в автомобілі. Акція безстрокова ***(У соцмережах українців закликали підняти прапор країни – безстрокова акція єдності // InternetUA (http://internetua.com/u-socmerejah-ukra-nc-v-zaklikali-p-dnyati-prapor-kra-ni---bezstrokova-akc-ya--dnost). – 2014. – 8.03).***

***

Українські військові в Криму створюють сторінки своїх частин у соцмережах. У соціальній мережі Facebook з'явилася сторінка гарнізону «Бельбек» та корабля «Донбас».

Сторінка авіаційного гарнізону «Бельбек» набрала вже понад 600 лайків, а сторінка моряків має понад 1200 читачів ***(Українські військові в Криму створюють сторінки своїх частин у соцмережах // Galnet.org (http://galnet.org/news/115557-ukrajinski-vijskovi-v-krymu-stvoryuyut-storinky-svojih-chastyn-u-sotsmerezhah). – 2014. – 10.03).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

4 марта Facebook начинает выкатывать новую структуру рекламных кампаний, которая поможет рекламодателям упростить процесс организации, оптимизации и измерений результатов рекламных объявлений, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-menjaet-strukturu-reklamnyh-kampanij-38558/).

Прежняя структура рекламных кампаний состояла из двух уровней – кампании и объявления. Новая структура состоит из трех уровней – кампании, группы объявлений и объявления.

Каждая кампания будет соответствовать определенной рекламной цели, например, повышение узнаваемости бренда или привлечение трафика на сайт. Кампании призваны помочь рекламодателю оптимизировать и измерять результаты для каждой цели через многочисленные группы объявлений и рекламные объявления.

Каждая кампания включает в себя несколько групп объявлений, каждая из которых имеет свой бюджет и расписание. Также можно организовать группы так, чтобы они соответствовали разным сегментам аудитории,

например, «пользователи, которые живут недалеко от магазина». Это поможет контролировать бюджеты, которые тратятся на каждую аудиторию, решать, когда они увидят объявления, и измерять их действия.

В каждой группе есть несколько рекламных объявлений, каждое из которых содержит разные картинки, ссылки, видео или текст. У рекламодателя сохраняется возможность таргетировать объявление и задавать ставки на данном уровне.

Новая структура станет доступна рекламодателям во всем мире во всех инструментах создания рекламных объявлений до конца марта (в Менеджере рекламы и Power Editor появится обучающее руководство). Обновление произойдет автоматически. Все существующие кампании будут переведены на новую структуру. Переход не повлияет на показы и расходы для существующих рекламных объявлений, и у рекламодателей сохранится доступ ко всем историческим данным по существующим кампаниям и объявлениям ***(Facebook меняет структуру рекламных кампаний // Marketing Media Review (http://mmr.ua/news/id/facebook-menjaet-strukturu-reklamnyh-kampanij-38558/). – 2014. – 28.02).***

***

Facebook всерьез задумывается о покупке Titan Aerospace, компании, которая занимается производством дронов, работающих на солнечной энергии. Устройство способно находиться в воздухе до пяти лет.

Согласно Techcrunch, Facebook хочет использовать дроны в качестве точек доступа к Интернету. Изначально проект планируют стартовать в станах Африки. Компания-производитель подтвердила, что ведет переговоры с Facebook.

Новый проект перекликается с инициативой Internet.org, благодаря которой, планировалось расширение количества пользователей Интернетом в развивающихся странах.

Как это обычно бывает, Facebook и Internet.org не стали первопроходцами в данной области. Google уже какое-то время изучает возможность доставки Интернета воздухом. Поисковой гигант использует для реализации своей идеи воздушные шары. Проект Loon предлагает 50 желающим доступ к Интернету через воздушные шары, работающие на солнечных батареях. Экспериментальный проект проводят в южном полушарии, в основном на территории Новой Зеландии.

Покупка Titan Aerospace обойдется Facebook в 60 млн дол. (все же дешевле недавней покупки WhatsApp) ***(Facebook ведет переговоры о покупке дрон-компании // Vido.com.ua (http://vido.com.ua/article/8104/facebook-viediet-pierieghovory-o-pokupkie-dron-kompanii/). – 2014. – 4.03).***

***

Корпорация Microsoft рассказала о грядущих обновлениях платформы Dynamics CRM, которую можно устанавливать локально, использовать в виде облачного сервиса Dynamics CRM Online или как гибридное решение.

Разработанный софтверным гигантом программный комплекс повышает продуктивность сотрудников внутри и вне организации и облегчает взаимодействие отделов продаж, маркетинга и обслуживания клиентов с помощью современных технологий, интегрированных в единую рабочую среду. Отличительными особенностями продукта являются развитые аналитические возможности, ролевой интерфейс, расширенные функции планирования, контроля деятельности подразделений и сотрудников.

Новая версия платформы Dynamics CRM будет дополнена системой мониторинга Social Listening и приложением Unified Service Desk. Первый инструмент позволит пользователям системы следить за уровнем лояльности к продуктам, брендам или конкурентам компании в социальных сетях, и анализировать текущую ситуацию на рынке в реальном времени. Второй продукт призван повысить эффективность работы сотрудников организации за счет автоматизации повторяющихся задач и возможности добавления новых данных о клиенте в одном рабочем окне.

Эксперты Microsoft уверены, что мониторинг социальных сетей должен стать неотъемлемой частью современной CRM-системы. Во избежание высоких затрат на управление взаимоотношениями с клиентами, Social Listening будет предлагаться как часть лицензии облачного решения Dynamics CRM Online без дополнительной оплаты.

Более подробную информацию о платформе Dynamics CRM и ее обновлениях можно найти по ссылке microsoft.com/dynamics ***(Microsoft дополнит Dynamics CRM функциями мониторинга социальных сетей // InternetUA (http://internetua.com/Microsoft-dopolnit-Dynamics-CRM-funkciyami-monitoringa-socialnih-setei). – 2014. – 4.03).***

***

Facebook ужесточил правила размещения на страницах соцсети постов с рекламой огнестрельного оружия. Сообщение об этом 5 марта появилось в официальном блоге компании.

Представители ресурса заявили о введении сразу нескольких новых правил. Так, любой пост с предложением купить оружие теперь должен обязательно содержать текст, напоминающий пользователям о необходимости соблюдать федеральное и региональное законодательство. Видимость подобных страниц, даже при наличии такого текста, для пользователей младше 18 лет будет ограничена.

Кроме того, запрещенными теперь официально признаны любые записи, призывающие при покупке оружия тем или иным образом обходить закон. К примеру, в тексте поста нельзя указывать, что продавец не требует от покупателя прохождения обязательной предварительной проверки. Также,

при получении любого сообщения о том, что на страницах социальной сети продается оружие, администрация Facebook обещает связываться с автором поста и посылать ему сообщение с напоминанием о новых правилах.

Как отметили в Facebook, нововведения затронут как саму соцсеть, так и принадлежащий ей фотосервис Instagram, часть пользователей которого также использует платформу сервиса для рекламы и продажи оружия. В конце 2013 г. в Instagram также объявили об ужесточении правил в отношении постов, рекламирующих наркотики и содержащих предложения о покупке запрещенных веществ. Все фотографии с соответствующими хэштегами блокируются за нарушение правил пользования сервисом.

По данным Buzzfeed, введение новых правил произошло спустя 10 дней после начала переговоров администрации соцсети с представителями общественных движений, выступающих за ужесточения контроля за оборотом оружия в США. К переговорам Facebook, судя по всему, подтолкнули два случая незаконной продажи огнестрельного оружия с помощью сайта, о которых стало известно в феврале. Виновными в незаконном распространении оружия были признаны житель Огайо, продавший ружье 15-летнему подростку из Кентукки, и житель Айовы, попытавшийся купить на Facebook оружие у работавшего под прикрытием сотрудника полиции.

В свою очередь американское Бюро по алкоголю, табакокурению, огнестрельному оружию и взрывчатым веществам (Federal Bureau of Alcohol, Tobacco, Firearms and Explosives) подтвердило Buzzfeed, что фактически продажа через Facebook огнестрельного оружия остается в США легальной. Как сообщили представители ведомства, пользователям социальной сети не запрещено публиковать записи с предложениями о продаже оружия, если эти предложения не содержат признаков нарушения законодательства. В самом Facebook продолжают настаивать, что сайт не несет полной ответственности за нарушение пользователями закона, так как не имеет площадки для непосредственной продажи огнестрельного оружия и вообще каких бы то ни было товаров. В компании подчеркивают, что соцсеть является всего лишь средством связи между людьми, в том числе между продавцами и покупателями ***(Facebook ужесточил требования к постам с рекламой огнестрельного оружия // InternetUA (http://internetua.com/Facebook-ujestocsil-trebovaniya-k-postam-s-reklamoi-ognestrelnogo-orujiya). – 2014. – 6.03).***

***

Компания Optimove представила новый инструмент для маркетологов, позволяющий отслеживать поведение пользователей приложений для Facebook в режиме онлайн. Этот продукт поможет специалистам разрабатывать целевые кампании, направленные на удержание посетителей.

Продукт предназначен для маркетологов, менеджеров по работе с клиентами и специалистов по удержанию аудитории в сфере онлайнового

бизнеса. Разработку можно использовать в комбинации с инструментом Facebook Custom Audience; она охватывает электронные письма, текстовые сообщения, push-уведомления, баннеры, рекламу внутри приложений, колл-центры. При этом не используются данные, которые позволяют идентифицировать пользователя, что снимает вопросы о приватности.

Кроме того, в Optimove разработали программный интерфейс (API), с помощью которого разработчики могут отслеживать взаимодействие пользователей с приложениями практически в реальном времени, исследовать и использовать полученную информацию с пользой.

Программа сортирует посетителей на группы по поведенческому признаку и прогнозирует их дальнейшие действия, что становится хорошим подспорьем для проведения узкоспециализированных маркетинговых кампаний; можно показывать рекламу дифференцированно для разных сегментов пользователей, отслеживая пользователей с наиболее релевантной ежедневной активностью.

В заявлении компании подчеркивается, что программа даст новый виток рекламе в вебе, позволив ей работать не только на привлечение, но и на удержание клиентов.

Инструменты, разработанные Optimove, можно адаптировать и изменять в соответствии с нуждами сферы бизнеса; каждая маркетинговая кампания становится экспериментом, в котором результат измеряется финансовыми показателями, а плата за услуги зависит от количества пользователей ***(Optimove отслеживает поведение пользователей приложений Facebook // InternetUA (http://internetua.com/Optimove-otslejivaet-povedenie-polzovatelei-prilojenii-Facebook). – 2014. – 10.03).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Facebook вызывает пищевое расстройство. К этому неординарному выводу пришли недавно ученые из Соединенных Штатов Америки, проведя небольшой анализ данных, собранных по ходу наблюдения за тысячей человек женского пола.

Как стало известно по ходу проводимого исследования, часто посещение страниц в социальных сетях пагубно сказывается на системе пищеварения. Длительность эксперимента была ограничена всего лишь тремя неделями, за период которого добровольцы, проводившие не менее

четырех часов в день за компьютером на страницах в социальных сетях, сильно страдали от проблем с пищеварением.

Другим, не менее неординарным выводом, сделанным учеными, явилось то, что социальные сети негативно влияют на межличностные отношения людей, вызывая сначала споры и затем и полный разрыв. Основополагающим фактором, сказавшимся на успешности данного исследования, явился пример ежедневного посещения молодыми людьми социальных сетей, начисто забывающими при нахождении на страницах об элементарном времени обеда и важных делах ***(Facebook вызывает пищевое расстройство // Newsland (http://newsland.com/news/detail/id/1335659/). – 2014. – 8.03).***

***

Шесть сценариев общения в Twitter

Ежедневно совместными усилиями мы публикуем 500 млн твитов. У многих пользователей тысячи фолловеров. И у нас всего 140 символов для того, чтобы выразить себя. Не хотелось бы вас разочаровывать, но, оказывается, мы совсем не оригинальны, общаясь в Twitter.

Недавно компания Pew Research Center опубликовала исследование, которое доказывает, что беседы в Twitter делятся на шесть типов. Всего лишь на шесть…и в них не входят @упоминания, @отклики и личные сообщения. Но в этом есть и свои преимущества. Используя полученные в ходе эксперимента данные, можно лучше понять, как общаются ваши фолловеры и как построить стратегию продвижения самым выгодным образом.

1. Две группы людей с противоположными мнениями.

Обсуждают противоречивые темы, основываясь на разных источниках информации. Стараются не вступать в спор с теми, кто с ними не согласен. Чаще всего разговаривают о политике или о других подобных тематиках. Получается эффект «эхокамеры»: высказывания приводят не к дискуссиям, а к поддакиванию и поддержке единомышленников.

2. Сплоченная компания.

Под этот сценарий подходят закрытые сообщества, посвященные профессиональным мероприятиям, конференциям, а также объединениям по интересам и хобби. Участники тесно связаны друг с другом идеологически, обмениваются информацией, идеями и мнениями.

3. Обсуждения брендов.

Такие диалоги формируются вокруг брендов и знаменитостей. Популярные темы привлекают достаточно крупные аудитории Twitter, генерируют массовый интерес, но низкую сообщаемость.

4. Новости и события.

Обсуждения формируются вокруг мировых событий и популярных новостей. Информационная поддержка привлекается со стороны всевозможных новостных ресурсов. Зачастую, вступив в такое обсуждение, новости можно узнать раньше, чем они появятся в официальных источниках.

5. Вещательная сеть.

Подобные обсуждения чаще всего провоцируются СМИ, экспертами отрасли или известными медиа-личностями, которых постоянно ретвитят их преданные фолловеры.

6. Клиентская поддержка.

Данный сценарий общения предполагает собой диалог бренда, государственного органа или другой компании с покупателем или клиентом. Предприниматели отвечают на вопросы и жалобы, а другие пользователи могут присоединиться и поддержать разговор на волнующие темы ***(6 сценариев общения в Twitter // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/6_stsenariev_obscheniya_v_twitter). – 2014. – 5.03).***

***

Более половины опрошенных пользователей (68 %) не готовы свободно высказывать свою точку зрения в сети, поскольку эта информация может, в том числе, быть использована в коммерческих целях, следует из отчета Ericsson ConsumerLab.

В опросе Ericsson ConsumerLab принимали участие 3311 человек в США, Мексике, Швеции, Египте, Пакистане и Таиланде, что является репрезентативным для 215 млн пользователей Интернет в возрасте от 15 до 69 лет.

Согласно опросу, 89 % респондентов при регистрации на различных площадках указывают действительные сведения о себе, но при этом 59 % обеспокоены возможным отслеживанием личных данных третьими лицами, а 56 % – проблемами конфиденциальности передаваемой в сеть информации. Тем не менее, большинство пользователей (81 %) не использует выдуманных имен или ников, комментируя что-то в социальных сетях.

Хотя 93 % участников опроса уверены в том, что используют некую стратегию защиты информации, а 70 % интересуются проблемами информационной безопасности, больше половины опрошенных (68 %) испытали на себе вирусные заражения ПК, а 11 % пострадали от мошенничества.

Несмотря на сильную обеспокоенность вопросами безопасности в сети, только 4 % опрошенных сказали, что это заставило их снизить свою активность в Интернете; 44 % пользователей с осторожностью относятся к передаваемым данным, а также анализируют используемые веб-сервисы; 10 % респондентов уверены, что проблемы безопасности в сети их не коснутся.

В рамках опроса выяснилось, что 48 % пользователей будут готовы изменить своё поведение в сети, узнав, что их персональная информация попадает в руки незнакомых людей. Только 39 % опрошенных снизят активность в сети, если узнают о слежке финансовых институтов или агентств безопасности ***(Большинство пользователей опасаются***

высказываться в соцсетях // InternetUA (http://internetua.com/bolshinstvo-polzovatelei-opasauatsya-viskazivatsya-v-socsetyah). – 2014. – 9.03).

Маніпулятивні технології

В социальной сети Facebook набирает обороты очередной фейковый розыгрыш. За последние несколько часов около 3 тыс. пользователей Уанета поделились новостью об открытии украинского представительства Amazon.

«Amazon.com теперь и в Украине! Поэтому мы проводим беспрецедентную акцию, посвященную нашему открытию! Первым 50 тыс. подписчикам, поделившимся этой записью, будет выдан подарочный сертификат на сумму в 300 дол. с бесплатной доставкой на 6 покупок», – сообщает единственная запись на странице несуществующей компании «Цифровой мир».

Сама страница «Цифровой мир» была создана за несколько часов до акции, официального объявления от компании Amazon про старт продаж в Украине тоже не было. Контакты администраторов страницы и компании «Цифровой мир» в Интернете отсутствуют. Все это дает основания полагать, что розыгрыш – фейковый. Вероятно, таким образом недобросовестные SMM-щики формируют ядро аудитории для очередной развлекательной группы, как это недавно сделали администраторы сообщества «Жить в Киеве», обещавшие победителю акции квартиру.

Аналогичная по содержанию акция проходила в эти же дни и в Рунете, пишет Tjourlan.ru. Доверчивым пользователям Instagram и «ВКонтакте» пообещали подарочные сертификаты на 150 дол. с бесплатной доставкой, если число подписчиков аккаунта достигнет 10 тыс. После того как аккаунт наконец-то набрал необходимое число подписчиков, авторы страницы объявили о сборе e-mail адресов для рассылки подарочных сертификатов. Еще спустя какое-то время владельцы аккаунта попросили перевести им денег на телефон и электронные кошельки.

История закончилась тем, что администраторы «ВКонтакте» и Instagram закрыли группу Amazon Russia в социальных сетях ***(На те же грабли: тысячи пользователей поверили, что Amazon дарит украинцам $300 за «лайк» // AIN (http://ain.ua/2014/02/25/514103). – 2014. – 25.02).***

***

В соцсетях сообщается о подготовке потасовки между «крымскими татарами» и славянским населением. Предполагается, что готовится провокация для эскалации конфликта в Крыму.

В Симферополь из Феодосии направляется колонна из четырех грузовиков с людьми кавказской внешности, сообщается в группе «Крым-S0S» в социальной сети Facebook.

Из сообщения следует, что «в центре Симферополя готовится инсценировка потасовки между этими людьми и славянским населением» города.

В группе подчеркивают, что это провокация для эскалации конфликта в Крыму.

Напомним, 28 февраля меджлис крымско-татарского народа официально заявил, что не признает сформированное 27 февраля 2014 г. правительство Крыма и подтвердил, что не ведет каких-либо переговоров с представителями сомнительно сформированного Совета министров АРК. Таким образом, крымские татары поддерживают правительство Украины, возглавляемое А. Яценюком ***(В соцсетях сообщается о подготовке потасовки между «крымскими татарами» и славянским населением // Левый берег (http://society.lb.ua/life/2014/03/02/257897_sotssetyah_soobshchaetsya_podgotovpo.html). – 2014. – 2.03).***

***

Російські боти взялися за український Facebook уряд

Більшість представників новоствореного українського уряду є представленими у Facebook та інших соціальних мережах. Найактивнішими з них є міністр економіки П. Шеремета та міністр внутрішніх справ А. Аваков.

П. Шеремета активний як у Facebook, так і Twitter. І, напевно, поки що єдиний міністр, який навіть сам чекіниться.

А. Аваков дуже активний у Facebook. Для нього в останні дні Facebook став майданчиком для звітування щодо проробленої роботи та повідомлення оперативної інформації.

Варто зауважити, що російські боти досить активно взялися за А. Авакова. Усього за чотири години він отримав понад 2 тис. коментарів, з них більше половини – боти, які активно відстоюють проросійські позиції, розміщують відверто неправдиву інформацію про діяльність новопризначених міністрів та ситуацію в Криму. Якщо проаналізувати коментарі – більшість із них мають кілька чітко виражених інформаційних ліній. Хоча є там й користувачі з реальними акаунтами з Росії. Правда, відстоюють вони ті ж інформаційні лінії, що й боти ***(Російські боти взялись за український Facebook-уряд // UkrainianWatcher (http://watcher.com.ua/2014/02/28/rosiyski-boty-vzyalys-za-ukrayinskyy-facebook-uryad/). – 2014. – 28.02).***

***

Наверное, никогда украинские пользователи столько не читали о политике в онлайне. К сожалению, среди массы информации в сети сложно выделить правдивую. В последнее время в украинском Интернете заработало сразу два проекта, которые объявили целью проверять новости и факты из СМИ и социальных сетей.

Один из сайтов – stopfake.org, авторы этого проекта объявили, что будут заниматься «борьбой с неправдивой информацией о событиях в Украине во время крымского кризиса». К сожалению, информации на сайте о проекте фактически нет. Команда обещала рассказать ain.ua о себе позже: «Мы сейчас разберемся с хостингом, а потом ответим на вопросы. Нас жестко ддосят».

Один из самых громких фейков воскресенья, попавший в публикации сайта: репортаж российского «Первого канала» о том, что тысячи украинцев якобы массово переезжают в Россию. Только судя по сюжету, используют для этого хитроумный маршрут: через Польшу. Ведь для иллюстрации использовалось видео с пропускного пункта в с. Шегини, которое находится в Львовской области на границе с Польшей.

Еще один пример воскресного фейка на сайте: опровержение гибели россиян в Крыму – именно эта причина побудила российский Совет Федерации одобрить просьбу президента по использованию войск на территории Украины. Данные о гибели российских граждан опровергли дважды, причем как с российской, так и с украинской стороны.

Также в Уанете уже действует блог fakecontrol.org. «Наша команда решила создать этот проект, чтобы по мере сил помогать очищать информационное пространство от очевидных фейков, уток и манипуляций», – говорится в описании проекта. В настоящее время в команде проекта шестеро людей, но никто не является профессиональным журналистом, большинство связаны с IT. Участники FakeControl ведут проект за собственные деньги: «Мы верим, что это позволяет оставаться максимально нейтральными». Политические взгляды в команде не обсуждаются. Связаться с редакцией можно через Facebook-профиль, также у проекта есть страница во «ВКонтакте».

Последняя из проверенных на фейковость новостей – о «крике о помощи» из общежитий «Беркута». В сообщении якобы семьи сотрудников «Беркута» обращаются ко всем неравнодушным с просьбой подвезти продуктов, пополнить мобильные, перевести средства на WebMoney и т. д. в Общежитие № 4 ГУ МВД Украины в г. Киеве по просп. Краснозвездный 152 а. Команда сайта связалась с общежитием: «Нам сообщили, что у них все есть и помощь им не нужна… Наш вывод: информация фейк и попытка заработать денег на чужом горе».

Кстати, участники проекта иногда используют способы, которые будет несложно позаимствовать любому пользователю, желающему проверить новость. К примеру, проверить в Google, «Яндекс» или в специальных сервисах происхождение картинки, иллюстрирующей новость. Подборку таких сервисов редакция готовила ранее ***(В уанете запустились сразу два сайта, которые разоблачают фейковые новости // IT Expert (http://itexpert.org.ua/rubrikator/item/34211-v-uanete-zapustilis-srazu-dva-sajta-kotorye-razoblachayut-fejkovye-novosti.html). – 2014. – 3.03).***

***

В сети появилась еще одна инициатива, направленная на борьбу с антиукраинской пропагандой Кремля, – AntiRUp.com.

«Нам нужно усмирить пропагандистскую машину Кремля. Создана группа для непосредственного реагирования на эту брешь: AntiRUp.com.

Мы будет сотрудничать с EuroMaidanPR и другими. Запад должен знать, что не существует противостояния между Востоком и Западом; нет также речи и о том, что украинцы ущемляют этнических русских. У группы две команды: тактическая, задача которой – анализировать и координировать, и «нагнетательная», задача которой – распространять сообщения. Если у вас нет времени участвовать непосредственно, вы можете помочь, указав на пропагандистские материалы команде AntiRUp.com», – говорится в сообщении активистов ***(В сети появилась еще одна инициатива, направленная на борьбу с антиукраинской пропагандой Кремля – AntiRUp.com // Marketing Media Review (http://mmr.ua/news/id/v-seti-pojavilas-esche-odna-iniciativa-napravlennaja-na-borbu-s-antiukrainskoj-propagandoj-kremlja-antirupcom-38627/). – 2014. – 4.03).***

***

В социальных сетях появились сообщения о масштабных пророссийских митингах 5 марта. К «борьбе за Украину» приглашают подключиться жителей России

Объявление о наборе добровольцев опубликовала группа «Гражданская Самооборона Украины» в соцсети «ВКонтакте». «Мы отправляем людей в Донецк и Харьков как важнейшие центры сопротивления. Также можно отправиться в Одессу... Выезд в Донецк происходит из Ростова-на-Дону, выезд в Харьков – из Белгорода. Тебе нужно указать дату твоего приезда в эти города, где получишь дальнейшие инструкции», – говорится в объявлении. Организаторы подчеркивают: «Помни, ты обычный турист, ничего лишнего не нужно».

При этом группа «Молот правды» анонсирует масштабный митинг юго-востока «Ни шагу назад» с требованиями «назначить дату референдума, попросить Россию о помощи, о введении российских войск». «Суббота была только началом революции юго-востока», – говорится на странице. Как известно, в минувшую субботу в Харькове «мирный митинг», на котором также были замечены «гастролеры» из Белгорода, закончился побоищем с незаконным водружением российского влага на Доме советов.

Параллельно в соцсетях распространяется информация о масштабной операции «Русская весна». Пользователи предупреждают о запланированном государственном перевороте. «В планах агрессоров в случае удачного расклада ситуации избрать “народных мэров”, которые должны будут заявить о переподчинении всей вертикали власти местным советами сделать официальные заявления к Путину, с просьбой ввести войска РФ на территорию областей для «поддержания правопорядка». Эта спецоперация

будет осуществляться с помощью активистов Молодежного единства, Оплота, Сопротивления и других движений + титушек. Цель – установка местного марионеточного правительства по крымскому сценарию с присутствием российским войск», – говорится в сообщении ***(Дашкевич Е. В восточной Украине снова организовывают масштабные митинги и зовут на них россиян // Медиа группа «Объектив» (http://www.objectiv.tv/030314/93941.html). – 2014. – 3.03).***

***

У соціальній мережі «ВКонтакте» з'являються несправжні сторінки сайту stopfake.org, що присвячений розвінчуванню кремлівської пропаганди.

Невідомі особи створили групу нібито від імені сайту stopfake.org. Цікаво при цьому, що слова fake в адресі групи немає – vk.com/stop_fuck. Станом на ранок 4 березня група заблокована. Незадовго до блокування у неї був 41 підписник.

Існує ще одна група з назвою #StopFake. Адміністратори також позиціонують її від імені згаданого сайту.

Водночас на самому ресурсі stopfake.org повідомляється справжня адреса в соцмережі «ВКонтакте» – vk.com/stopfakenews. Діє також сторінка у Facebook за адресою facebook.com/stopfakeukraine.

Волонтери сайту stopfake.org повідомляють, що на їхній ресурс постійно здійснюються потужні DDos-атаки ***(У соцмережі «ВКонтакте» з'являються несправжні сторінки від імені сайту Stopfake // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/28276). – 2014. – 4.03).***

***

Не зважаючи на зміну влади в Україні та розформування спецпідрозділу «Беркут», прихильники В. Януковича нікуди не зникли і все ще продовжують свої віртуальні бої в соціальних мережах.

Наразі, «бійці диванної армії» закликають В. Путіна вводити війська в Україну, намагаються заблокувати соціальні спільноти прихильників Євромайдану і закликають участників спільнот збільшувати чисельність груп.

Базуються вінницькі антимайданівці в основному в соціальній мережі VK.com.

Наводимо список вінницьких спільнот у соціальних мережах для ознайомлення.

Антимайдан.НАСТОЯЩИЕ УКРАИНЦЫ. ВИННИЦА (141 участників)
http://vk.com/club65186015
Наразі постить новини щодо Росії
- – -
ВИННИЦА ОБЪЕДИНЯЕМСЯ! ЗАЩИТИМ РОДНОЙ ГОРОД! (141)
http://vk.com/public65178938

Фактично клон попередньої і по змісту і по матеріалу

- – -

АнтиМайдан Винница (260 участників)

http://vk.com/public65186886

Контент аналогічний попереднім группам

- – -

Закрита група «Подолье (Platinum Team)» (31 участник)

http://vk.com/club62237855 ***(Віртуальний Антимайдан по-вінницьки не здається // Винницкий бизнес портал (http://vinbazar.com/news/drugoe/virtualnii-antimaidan-po-vinnitski-ne-zdayetsya). – 2014. – 4.03).***

***

«Не заправляюсь на Лукойле» – под таким названием поляки создали Facebook-группу, к которой присоединилось более 10 тыс. участников. Nie tankuję na Lukoil-u набрало за два дня более 10,7 тыс. последователей.

«Бойкот сети заправок Лукойл! Не финансируем войну! Не финансируем российский капитал!» – объяснили создатели Facebook-группы свою инициативу. По их словам, они предпочитают уплатить на несколько «грошей» больше за литр бензина и поддержать польского производителя, чем поддерживать «ненависть, насилие и человеческую смерть», сообщил сайт mmtrojmiasto.pl.

«Я за бойкот этой заправки. Всегда, когда кто-то получает по карману, то начинает задумываться, какая этому причина», – убежден один из участников группы. «Касается ли это также российского газа в наших кухнях и печах?» – задал вопрос один из посетителей упомянутой страницы. На что ее создатели ответили, что есть разница в ситуации, когда есть выбор или нет ***(Поляки объявили бойкот «Лукойлу» // Дело (http://delo.ua/ukraine/poljaki-objavili-bojkot-lukojlu-229128/). – 2014. – 4.03).***

***

С момента обострения ситуации на полуострове в российских и украинских СМИ и Интернете появилось много неправдивых новостей. «Вести» выбрали и опровергли главные из них.

Новость № 1. 1 марта спикер Совета Федерации РФ В. Матвиенко заявила, что при штурме ГУ МВД Украины в Крыму погибли россияне.

Опровержение. На следующий день убийства россиян опроверг генконсул РФ в Крыму В. Светличный: «Было несколько выстрелов в воздух с обеих сторон, но о жертвах или пострадавших данных нет», – заявил он. Чуть позже эту же информацию подтвердил глава ВС Крыма В. Константинов.

НОВОСТЬ № 2. 1 марта в СМИ появилась информация, что фрегат «Гетман Сагайдачный», возвращающийся из Аденского залива в Севастополь, отказался подчиняться новой власти и поднял Андреевский

флаг (знамя ВМС России – прим. авт.). Узнав об измене, Премьер-министр А. Яценюк обратился к турецкому коллеге с просьбой не пускать корабль в Черное море.

Опровержение. Минобороны заявило, что фрегат находится на военно-морской базе в Греции и в ближайшие дни вернется в Украину. «Военнослужащие верны присяге, а фрегат идет под флагом Украины», – заявил командир национального контингента, контр-адмирал А. Тарасов.

НОВОСТЬ № 3. 2 марта в сети разошлась новость о том, что 10 кораблей ВМС Украины покинули Севастополь, а большинство воинских частей в Крыму перешли на сторону властей автономии.

Опровержение. Министерство обороны сообщило, что ни один корабль не покинул Севастопольскую бухту. «Личный состав воинских частей ВСУ в Крыму сохраняет спокойствие и ведет переговоры с теми, кто их заблокировал», – отметили в пресс-службе Минобороны.

НОВОСТЬ № 4. 2 марта российские СМИ сообщили об очередях беженцев из Украины в Россию. По их данным, за последние две недели в РФ выехали 140 тыс. украинцев.

Опровержение. Активист В. Уманец, что материалы проиллюстрировали кадрами с украинско-польской границы – с пропускного пункта «Шегини-Медика». Госпогранслужба объявила, что массовых выездов наших граждан в Россию нет: «Показатели среднестатистические» ***(Главные фейковые новости о Крыме // ВЕСТИ (http://vesti.ua/krym/40761-glavnye-fejkovye-novosti-o-kryme). – 2014. – 4.03).***

***

Увечері, 3 березня, в офіційному Twitter-акаунті МЗС Росії з'явився запис: «Просьба на ФБ и Twitter сдержанно одобрить грамотный анализ [link] (+ упоминание @местнГазет и @властей в конце твита)», до якої було прикріплено посилання на статтю газети Der Spiegel.

За півгодини після появи твіт було видалено, але кілька десятків його ретвітів досі можна знайти в кеші Яндекса.

Зміст і наказова тональність твіта схожа на стандартні правила для ботів та людей, які за гроші поширюють повідомлення комерційних чи політичних структур ***(Російський МЗС випадково опублікував у Twitter інструкцію для своїх ботів? // UkrainianWatcher (http://watcher.com.ua/2014/03/04/rosiyskyy-mzs-vypadkovo-opublikuvav-u-tviteri-instruktsiyu-dlya-svoyih-botiv/). – 2014. – 4.03).***

***

Інформаційна війна як глобальний ІТ-бізнес

«ВІЙНА – ЦЕ МИР
СВОБОДА – ЦЕ РАБСТВО
НЕЗНАННЯ – СИЛА»

У цьому лозунгові із Орвелівської антиутопії можна знайти відображення аверсу інформаційної війни з боку Сходу. Інформаційна окупація України тривала роками, але сьогодні ми стали учасниками вибуху.

Пропаганда замість журналістики. Наразі на ефірних частотах найбільшої кримської приватної «Чорноморської телерадіокомпанії» розпочав мовлення російський державний інформаційний телеканал «Россия 24», на частотах 1+1 в АР (поки що) Крим транслюють канал «Росія».

Але кримлівські ляльководи не вдовольнилися тотальним контролем над ТБ, пресою та радіо. Сфера впливу неминуче зачепила Інтернет. З іншого боку є і реверс – вплив інформаційної політики Заходу.

Експерт у сфері зв'язків із громадськістю та соціології масової свідомості Л. Вежель розповідає:

«Протягом останніх двох з половиною років російські спецслужби стали виявляти особливу активність у соціальних мережах для збору розвідувальної інформації, негласного радіоконтролю та впливу на формування громадської думки українців. Як відомо, одним із новітніх атрибутів поширення інформації стало явище цифрової конвергенції, коли процес взаємопроникнення і злиття цифрової обчислюваної техніки і систем передачі даних відбувається на основі первинного оцифрування різнорідних інформаційних повідомлень (текстових, графічних, аудіовізуальних тощо). Одночасно знижуються витрати на обробку і доставку інформації та збільшуються, удосконалюються функціональні можливості усього комплексу інформаційно-комунікаційних систем. Це дає можливість розширення аудиторії, стимуляції її інтересу, провокування на відповідну реакцію. Активно створюються проросійські веб-ресурси, сторінки на Facebook, "ВКонтакте", "заливається" відео на YouTube. Головне, що назви інтернет-проектів не дотичні до подій, що відбуваються в Україні, тому пошуковими системами знайти їх неможливо. Наприклад, сторінка Sputnik & Pogrom на Facebook, що нараховує 16581 користувачів. Контент розміщується регулярно, переважно із зображенням та використанням сильних емоційних слів у заголовках. Ще один тренд діяльності "інформаційних окупантів" – створення "digital"-авторитетів, які делікатно та невимушено дають оцінку подіям, моделюють ситуації та пропонують свої прогнози, формуючи відповідну громадську думку. Вірусне відео стало ефективним інструментом проведення інформаційних кампаній. Після "публікації" роликів на відеохостингу відбувається їх посів у популярних контекстно-медійних мережах. Мова тут йде про соціальні платформи (Facebook, "Одноклассники", "ВКонтакте"), блоги та інші тематичні майданчики: форуми, сайти тощо. Сукупне використання всіх каналів посіву та розповсюдження робить значний вплив на підсумкове зростання трафіку. Так, відео про зраду контр-адмірала Березовського Д. В. за три дні переглянуло 20625 користувачів. Тому офіційні запити адміністрації В. Януковича про вилучення відео з YouTube тільки погіршили ситуацію, бо

однією з важливих тенденцій сучасного інформаційного простору є гіперпрозорість комунікацій.

Найбільш повне покриття в соціальних медіа отримав конфлікт у Криму з 25 лютого 2014 р. Пік – 28.02, 01.03, 02.03. Масове поширення фейкової інформації про події в Криму дезорієнтовувало українців, особливо жителів центральних, західних та східних регіонів. Люди інтенсивно завантажували відео зіткнень на YouTube і поширювали їх через Twitter, Facebook, "ВКонтакте". Ці процеси свідчать про те, що російські спеціалісти діють системно, регулярно, злагоджено і відпрацьовують єдину інформаційну політику. Протягом останніх двох днів йде фінансове вливання в соціальні мережі: проплачуються всі рекламні формати Facebook, Twitter, "ВКонтакте". Ситуація з Кримом буде загострюватися. Якщо я не помиляюсь, Апарат Ради національної безпеки і оборони України вже розробляє концепцію інформаційної політики. Крім того, Інститут журналістики Київського національного університету ім. Тараса Шевченка став ініціатором відновлення професії військового піарника, що була свідомо ліквідована екс-міністром оборони Д. А. Саламатіним».

Спецслужби РФ протягом трьох місяців здійснюють посилену політику виявлення й ліквідації небажаної реакції серед активних користувачів соціальних мереж. Інформація відстежується, обмежується або й повністю перекривається доступ до альтернативних джерел. Так було, зокрема, з пабліками «Української революції» та «Правого сектору» в соціальній мережі «ВКонтакте». 1 березня доступ до них заблокували. Згодом відновили, однак лише в Україні.

Український політолог, директор соціологічної служби «Український барометр» В. Небоженко повідомляє своє бачення ситуації: «Чисто пропаганда, знищується об'єктивна думка. Лякають тим, що бандерівці захоплюють всю Україну. Використовують політичні помилки, "фактор Фаріон". Тільки фотографія цієї жінки змусить затремтіти половину чоловічої частини населення Росії. І я не жартую, вони просто використовують наших нестриманих імпульсивних політиків, збільшують емоційний вплив в стократ, й виходить, що ми цілковито бандитська країна. Все тримається на емоції, на страхові, на відволіканні уваги від серйозних соціально-економічних проблем Росії. Усе контролюється з Кремля. Це і є початок маніпуляції. Населення не отримує альтернативних точок зору. "Образ ворога", який постійно робили зі США та Європи й навіть України, глибоко вкоренився в свідомість росіян. Насправді, президент РФ більше говорить як Д. Кисельов, ніж як президент В. Путін. Я собі не уявляю Б. Обаму, котрий починає говорити як редактор New-York Times.

В. Путін зробив страшну річ – він посіяв ворожнечу між двома близькими народами. Покоління, яке пережило Майдан, вже ніколи не повірить навіть найсолодшому політикові, який прийде після В. Путіна, і буде казати, що це все останній. Ми ж бачимо, що росіяни його підтримують. Західні ЗМІ після 1991 р. припинили це робити. У них теж було багато

методів маніпуляцій, промивання мізків, але вони вже відвикли їх застосовувати».

Знову ж таки, як не помітити паралелі з тезою Орвелла, у той час коли цілеспрямовано викривлюється реальність та встановлюється тотальний контроль впритул до історичного досвіду: «Кто управляет прошлым, гласит партийный лозунг, – тот управлет будущим; кто управляет настоящим, тот управляет прошлым». Маси доведені до такого стану, коли стало нормальним «зная, не знать; ...придерживаться одновремонно двух противоположных мнений, понимая, что одно исключает другое, и быть убежденным в обоих...».

Директор аналітичного центру «Політика», у минулому керівник Комітету виборців України, заступник голови Секретаріату Президента В. Ющенка, політолог І. Попов пояснює свою точку зору: «Навішування ярликів, підтасовка фактів, запуск дезінформації. Обидві сторони їх застосовують. Дзеркально. В чому виграє Захід – він веде, задає тон, а Росія дзеркально відповідає. В чому виграє Росія – Росія сильніша в інфраструктурі й дисципліні. Вона відразу захопила "Укртелеком" і відрубила канали Інтернету і змогли заблокувати доступ до багатьох сайтів, одразу захопили ТРК "Крим", "Чорноморку". З точки зору інфраструктури вони все роблять правильно. Організатори останньої революції в Києві це не розуміли, не могли зробити.

Що ж стосується обробки власних громадян у Росії – то там інфомашина запущена, працює професійно, і на своїй території вони звичайно перемагають. Але якщо говорити про нейтральні території, беручи до уваги всю Україну, східну її частину чи Крим – то тут інформаційна перемога однозначно за західними силами. Навіть такий приклад... Коли влада в Києві належала режимові В. Януковича, то підпільно, напівпідпільно й добровільно діяли опозиційні ЗМІ. А коли владу в Києві отримали опоненти В. Януковича, то протягом двох тижнів виїхали проросійські експерти, поховалися, хоча їх би ніхто не переслідував, бо вони всього лиш експерти, і позакривалися проросійські сайти. Це демонструє те, що в інформаційній війні на нейтральній території Росія програє. Тому що ідеологічна база набагато слабша».

Водночас серед океану відвертої брехні складно вхопитися за рятівне коло правди. В. Путін яскраво продемонстрував це тезами під час своєї прес-конференції. На сайті Посольства Штатів можна знайти спростування. У свою чергу маріонетки Кремля вже назвали українські війська окупантами, а Крим – Росією. Насправді ж, із цілковито абсурдної і неприйнятної думки цілком реально зробити прийнятну масам істину. Це детально описує політична теорія вікна Овертона.

Орвелл VS Хакслі

Читачі часто задаються популярним питанням: хто ж мав рацію – Д. Орвелл, котрий вважав, що суспільство загине від тотального контролю і відсутності інформації, чи О. Хакслі, який боявся, що її надлишок та

вседозволеність стане причиною нашої деградації до повної пасивності й інертності?

Якщо протягом трьох місяців розгортання подій Майданом і навколо Майдану українці починали відчувати на собі погляд Старшого Брата, якщо «мыслепреступники» зникали безслідно, то тепер реальність більше нагадує світ за О. Хакслі. Інформації настільки багато, що протистояти її впливу і бути спроможним відсіяти непотріб практично не можливо. У той же час президент РФ втілив в реальність побоювання О. Хакслі, котрий вважав, що найбільш абсурдним і жорстоким на війні є те, що людину, яка особисто не має нічого проти свого ближнього, змушують холоднокровно вбивати.

З іншого боку, Орвелівська концепція не втрачає актуальності. «Свобода, это возможность сказать, что дважды два – четыре». Але як тільки журналістика перестала бути журналістикою, два на два перестало бути четвіркою. Журналісти російських ЗМІ підтверджують цю думку мало чи не кожним матеріалом.

Та насправді, те коло читачів, що задається питанням, хто ж з письменників мав рацію, допускає хибу. Бо Д. Орвелл не боявся того, що нас позбавлять інформації. Він боявся, що ми не зможемо відшукати правду, яка буде приховуватися серед моря дезінформаційного сміття.

Сьогодні рядки з антиутопії «1984» практично нікому не здаються абсурдними чи ефемерними: «Раскол мира на три сверхдержавы явился событием, которое могло быть предсказано и было предсказано еще до середины XX века. После того, как Россия поглотила Европу, а Соединенные Штаты – Британскую империю, фактически сложились две из них. Третья, Остазия, оформилась как единое целое лишь спустя десятилетие, наполненное беспорядочными войнами...»

Тепер лишається консолідуватися, діяти розумно і плекати надію, що такий сценарій лишиться в обрамленні його книги, а не стане реальністю з похибкою в 30 років ***(Дачковська М. Інформаційна війна як глобальний IT-бізнес // InternetUA (http://internetua.com/nformac-ina-v-ina-yak-globalnii--t-b-znes). – 2014. – 7.03).). – 2014. – 7.03).***

Зарубіжні спецслужби і технології «соціального контролю»

Новая теория заговора: АНБ внедрило баг в iOS и OS X

Недавно в операционных системах iOS и OS X была обнаружена уязвимость, связанная с валидацией SSL-подключения, которая ставила под угрозу безопасность данных пользователя. Apple поспешила исправить ошибку, и уже выпустила обновление для iOS, но впечатлительные пользователи до сих пор обеспокоены произошедшим. Д. Грубер из Daring Fireball решил разобраться в причинах этой проблемы и, неожиданно для всех, разоблачил теорию заговора.

iOS 6 была выпущена осенью 2012 г., именно тогда, когда по информации Э. Сноудена, Apple присоединилась к программе Агентства

национальной безопасности по сбору информации PRISM. Д. Грубер находит это совпадение не случайным.

«Конечно, было интересно узнать, кто добавил эту сомнительную строку кода в файл. Конспирологически, можно предположить, что АНБ внедрило ошибку через агента, работающего под прикрытием. Безобидным объяснением является случайная ошибка со стороны инженера Apple», – поясняет Д. Грубер.

Согласно его теории, после внедрения ошибки в код, АНБ потребовались только автоматические тесты, использующие поддельные сертификаты безопасности, чтобы найти эту уязвимость в каждой новой версии операционной системы и получить доступ к конфиденциальной информации миллионов пользователей ***(Новая теория заговора: АНБ внедрило баг в iOS и OS X // InternetUA (http://internetua.com/novaya-teoriya-zagovora--anb-vnedrilo-bag-v-iOS-i-OS-X). – 2014. – 26.02).***

***

В социальной сети «ВКонтакте» по требованию Роскомнадзора заблокировано 13 сообществ, посвященных акциям протеста на майдане Незалежности в Киеве.

При попытке зайти на страницы групп 3 марта выдавалось сообщение о том, что данные материалы «заблокированы на территории Российской Федерации», передает Lenta.ru.

В частности, не открываются страницы таких сообществ, как «Украинская революция / Евромайдан» (более 500 тыс. подписчиков), «Правый сектор» (более 390 тыс. подписчиков) и «Революция / Евромайдан / Правый сектор» (около 352 тыс. подписчиков). В «заглушках», установленных по адресам этих групп, дается отсылка к решению Роскомнадзора номер 01КМ-7376 от 2 марта 2014 г.

Информацию о блокировке также подтверждает и официальный сайт надзорного ведомства. 3 марта на ресурсе появилось сообщение о том, что с требованием заблокировать сообщества в Роскомнадзор обратилась Генпрокуратура РФ. Представители прокуратуры усмотрели в группах «обращенные к российскому народу прямые призывы осуществлять террористическую деятельность и участвовать в несанкционированных массовых мероприятиях».

При этом, как отмечается в пресс-релизе Роскомнадзора, после удаления противоправной экстремистской информации некоторые сообщества были исключены из реестра запрещенной информации. Какие именно сообщества, не уточняется.

Впервые о блокировке украинских групп во «ВКонтакте» стало известно 1 марта. Тогда в сети появилась информация о том, что блокировке, в частности, подверглась страница организации «Правый сектор». Ограничение доступа произошло после публикации в сообществе обращения лидера националистического движения Д. Яроша к террористу Д. Умарову. В

тексте Д. Ярош призывал Д. Умарова организовать серию терактов на территории России.

Позже представители «Правого сектора» опровергли подлинность этого обращения, заявив, что его текст появился в группе в результате взлома. Пресс-секретарь «ВКонтакте» Г. Лобушкин в свою очередь отметил, что блокировка украинских общественно-политических групп продолжалась всего несколько минут и произошла «из-за ошибки модераторов».

Тем не менее, как позднее сообщили в Роскомнадзоре, ведомство не собирается отказываться от блокировки сообществ украинских группировок. В ведомстве подчеркнули, что по требованию Генпрокуратуры продолжат мониторинг информационного пространства и будут ограничивать доступ к другим интернет-адресам «в случае переноса на них экстремистского контента».

3 марта стало известно, что Следственный комитет РФ возбудил против лидера «Правого сектора» Д. Яроша уголовное дело. СК подозревает Д. Яроша в публичных призывах к осуществлению террористической и экстремистской деятельности с использованием СМИ ***(В России заблокировали «Евромайдан» во «ВКонтакте» // Левый берег (http://lb.ua/news/2014/03/03/257927_rossii_zablokirovali_evromaydan.html). – 2014. – 3.03).***

***

Британский центр правительственной связи (GCHQ) уличили в слежке за пользователями сервиса видеосвязи на сайте Yahoo!. Об этом 27 февраля сообщает газета The Guardian. Слежка осуществлялась ведомством в сотрудничестве с Агентством национальной безопасности США (АНБ).

Специалисты GCHQ собирали и хранили скриншоты с вебкамер Yahoo!, использовавшихся посетителями ресурса в так называемых видеочатах. Данные, полученные The Guardian, позволяют говорить о том, что программа слежки за видеосвязью активно применялась как минимум с 2008 по 2012 г.

За шесть месяцев 2008 г. сотрудники GCHQ, к примеру, получили доступ к более чем 1,8 млн конфиденциальных изображений, многие из которых носили сексуальный характер. В дальнейшем снимки предполагалось использовать для «идентификации ранее судимых и подозреваемых в терроризме» людей. Были ли снимки действительно использованы для этих целей, не уточняется.

Представители Yahoo! в ответ на просьбу журналистов прокомментировать опубликованные сведения заявили, что ничего не знали о слежке. Действия GCHQ в интернет-компании назвали беспрецедентным по масштабу нарушением пользовательских прав.

Документы о слежке GCHQ и АНБ за видеочатами Yahoo! передал The Guardian экс-сотрудник АНБ Э. Сноуден. Ранее в обнародованных Э. Сноуденом документах также сообщалось о слежке спецслужб за

электронной почтой Yahoo! и дата-центром компании, расположенном в США. Кроме того, активная слежка велась разведывательными ведомствами за пользователями таких компаний, как Google, Facebook, Microsoft, Linked-In и AOL ***(Британские спецслужбы уличили в слежке за видеочатами Yahoo! // InternetUA (http://internetua.com/britanskie-specslujbi-ulicsili-v-slejke-za-videocsatami-Yahoo). – 2014. – 27.02).***

***

Команда Yanukovychleaks.org опубликовала бумаги главы службы безопасности президента К. Кобзаря, который ежедневно получал обзор СМИ и текущей ситуации в стране.

Его подчиненные мониторили комментарии в социальных сетях и составляли ежедневный отчет об угрозах, особое внимание уделялось протестам в районе Межигорья, передают Подробности.

Мониторинг сообщений проводился в соцсетях «ВКонтакте» и Facebook, говорят активисты.

Напомним, команда Yanukovychleaks.org занимается систематизацией документов, найденных на территории резиденции беглого президента В. Януковича ***(Вот как команда Януковича следила за пользователями соцсетей // From-UA. Новости Украины (http://www.from-ua.com/news/be4be38563897.html). – 2014. – 4.03).***

***

Требования Роскомнадзора заблокировать ряд «экстремистских» сообществ из Украины вынудили администрацию «ВКонтакте» ввести так называемую «географическую сегрегацию» контента. Об этом «Ленте.ру» 3 марта сообщил анонимный источник в руководстве соцсети.

«Ранее такой сегрегации не было. Ввели буквально вчера, 2 марта», – рассказал источник, подчеркнув, что пойти на это в социальной сети решили, чтобы «не быть заблокированными вообще навсегда».

Внедрение новой системы отображения контента по географическому принципу подтверждают также и украинские пользователи «ВКонтакте». По словам некоторых из них, заблокированные на территории России сообщества националистической организации «Правый сектор» и группы Евромайдана в Украине по-прежнему открываются. (С введением «географической сегрегации» одни и те же материалы, страницы и группы могут быть недоступны для российских пользователей «ВКонтакте», но при этом открываться у всех остальных пользователей, находящихся в других странах) ***(Роскомнадзор вынудил «ВКонтакте» ввести «географическую сегрегацию» // InternetUA (http://internetua.com/roskomnadzor-vinudil--vkontakte--vvesti--geograficseskuua-segregaciua). – 2014. – 3.03).***

***

Похоже, Facebook перестал быть «простором украинской демократии». Сегодня, 5 марта, стало известно, что не только во «ВКонтакте» жителям России перестали показывать проукраинский контент. С ночи попытки российских пользователей зайти на страницу «Акция на Майдане «Правый сектор» остаются безуспешными. В Украине никаких проблем с доступом не наблюдается.

Если введение географической сегрегации во «ВКонтакте» было инициировано Генпрокуратурой РФ, то по чьему наитию блокируют контент в сети М. Цукерберга – пока неизвестно. В графе «причина блокировки» написано, что страница изъята для некоторых регионов по пространной причине: «Грабеж или вандализм». О каких именно регионах идет речь, не уточняется, сказано лишь, что для этих локаций публикация контента «Правого сектора» незаконна.

Какие еще украинские сообщества забанили для России, пока точно не известно ***(Сегрегация 2.0: В Facebook для россиян заблокировали страницу Правого сектора // Marketing Media Review (http://mmr.ua/news/id/segregacija-20-v-facebook-dlja-rossijan-zablokirovali-stranicu-pravogo-sektora-38644/). – 2014. – 5.03).***

***

Специалисты немецкой компании G Data обнаружили новую вредоносную программу, нацеленную на хищение конфиденциальной информации. По данным специалистов, разработкой вредоносной программы занимались представители спецслужб России. Руткит Uroburos получил свое название от имени мифического дракона, а также от последовательности символов внутри кода вредоносной программы: Ur0bUr()sGotyOu#.

Uroburos похищает файлы с зараженных компьютеров и перехватывает сетевой трафик. Вредоносная программа предназначена для работы в режиме P2P для установки связи между инфицированными системами. Эта функция позволяет получить удаленный доступ к одному компьютеру с интернет-подключением для того, чтобы управлять другими ПК в локальной сети.

Интересно, что для того, чтобы скрыть свою деятельность руткит использует две виртуальные файловые системы – NTFS и FAT, которые локально находятся на инфицированной машине. Эти файловые системы позволяют злоумышленникам хранить на компьютере жертвы инструменты сторонних производителей, инструменты для пост-эксплуатации, временные файлы и двоичные выходные данные. Доступ к виртуальным файловым системам можно получить через устройства: Device\RawDisk1 и Device\RawDisk2, а также диски \\.\Hd1 и \\.\Hd2.

Специалисты G Data отмечают: «Создание такой структуры, как Uroburos требует огромных инвестиций. Команда разработчиков этой вредоносной программы, очевидно, состоит из высококвалифицированных IT-специалистов. Такой вывод можно сделать, проанализировав структуру и

современный дизайн руткита. Мы считаем, что у разработчиков также имеются усовершенствованные версии Uroburos, которые появятся в будущем».

Обнаружив определенные технические характеристики (имя файла, ключи шифрования, поведение и др.), представители G Data предположили, что авторами Uroburos является группа злоумышленников, которая в 2008 г. осуществила атаку на компьютерные системы США при помощи вредоносной программы Agent.BTZ.

Эксперты заявляют, что перед установкой на систему жертвы Uroburos проверяет ее на наличие Agent.BTZ. Если последний присутствует, то новый руткит остается неактивным. Доказательством того, что за созданием Uroburos могут стоять русские является то, что в коде вредоносной программы присутствует кириллица.

Напомним, что после атаки Agent.BTZ на системы США американским военным запретили использовать USB-накопители и другие съемные носители. В то время предполагалось, что заражение системы Министерства обороны произошло через USB-накопитель.

По заявлениям G Data, целью авторов Uroburos являются крупные предприятия, государства, спецслужбы и прочие организации. Предположительно, руткит используется уже на протяжении трех лет, так как наиболее давние версии программы были написаны еще в 2011 г. ***(Немецкие IT-специалисты обнаружили разработанный россиянами руткит // InternetUA (http://internetua.com/nemeckie-IT-specialisti-obnarujili-razrabotannii-rossiyanami-rutkit). – 2014. – 4.03).***

***

Турецький уряд має намір ввести нові обмеження в Інтернеті, пише Корреспондент.net (http://ua.korrespondent.net/world/3316126-u-turechchyni-mozhut-zaboronyty-YouTube-i-Facebook).

Прем’єр-міністр Туреччини Р. Ердоган розповів, що після місцевих виборів, які намічені в Туреччині на 30 березня, уряд введе нові обмеження в Інтернеті, передає Agence France-Presse.

Зокрема, за словами глави турецького уряду, можуть бути заборонені відеосервіс YouTube і соціальна мережа Facebook. «Будуть нові кроки, які ми зробимо в цій сфері після 30 березня ... в тому числі заборона», – заявив Р. Ердоган.

Подальші обмеження Інтернету можуть бути пов’язані з корупційним скандалом, який виник у тому числі через витоки записів телефонних переговорів Р. Ердогана, що потрапили в мережу.

Так, були оприлюднені записи, на яких прем’єр-міністр та його син імовірно обговорюють способи приховування великої суми грошей. З матеріалів, що потрапили в ЗМІ, також випливає, що глава уряду міг втручатися в торгові угоди і правосуддя.

У Туреччині вже діє закон про блокування сайтів без рішення суду, який парламент схвалив на початку лютого. Обмежити доступ до інтернет-ресурсу влада зможе в разі виявлення на ньому будь-якого образливого контенту, який буде визначатися за так званим проблемним словами.

Нагадаємо, перший обмежувальний закон стосовно Інтернету був прийнятий у Туреччині ще в 2007 р., коли на території країни заблокували блогохостинг Wordpress і кілька місць для розміщення відеофайлів, зокрема, DailyMotion і Vimeo. YouTube в Туреччині блокували до 2010 р. З 2011 р. в країні також діє єдиний реєстр заборонених сайтів ***(У Туреччині можуть заборонити YouTube і Facebook // Корреспондент.net http://ua.korrespondent.net/world/3316126-u-turechchyni-mozhut-zaboronyty-YouTube-i-Facebook). – 2014. – 7.03).***

***

Бывший сотрудник Агентства национальной безопасности (АНБ) США Э. Сноуден подтвердил, что американское АНБ шпионило в телекоммуникациях стран ЕС, в частности, в сети бельгийского оператора «Бельгаком», и даже проникло в компьютерные сети Европейской комиссии.

Как сообщается в коммюнике Европарламента, эти данные, которые Э. Сноуден представил в письменном ответе европейским депутатам, пока не имеют других подтверждений.

«Я не хочу дублировать журналистов, но могу подтвердить, что все до сих пор раскрытые документы подлинны и не подвергались изменениям. Это означает, что действия, затронувшие “Бельгаком”, Swift (находящуюся в Брюсселе систему международных расчетов), учреждения ЕС, ООН, ЮНИСЕФ и другие, действительно имели место», – написал Э. Сноуден в ответе, обнародованном в Европарламенте.

Он отметил, что подразделение АНБ, занятое международными отношениями, имеет одну из главных задач – уговорить страны ЕС изменить законодательство, чтобы оно позволило проводить массовую слежку. Такие операции были проведены в Швеции, Нидерландах, Германии, в результате чего, по словам экс-сотрудника американских спецслужб, там созданы секретные системы массового наблюдения.

Э. Сноуден вменяет в вину АНБ, что оно присвоило себе право следить за гражданами стран-партнеров США, не информируя их об этом.

Он назвал «европейским базаром» состояние, при котором страны Союза, каждая в отдельности, уступают АНБ «ограниченные» права, которые, в конце концов, позволяют создавать «сеть массового наблюдения над простыми гражданами».

Но эта проблема, убежден Э. Сноуден, решается сама по себе: слабость системы массового наблюдения в том, что она скоро становится неподъемно дорогой из-за совершенствования техники, широкого распространения кодирования ***(Сноуден рассказал о слежке за гражданами Евросоюза //***

InternetUA (http://internetua.com/snouden-rasskazal-o-slejke-za-grajdanami-evrosouaza). – 2014. – 9.03).

***

Роскомнадзор внес в «черный список» запрещенных веб-сайтов страницу с видеохостинга YouTube. Основанием стало признание Генпрокуратурой соответствующего ролика экстремистским. Речь идет о ролике с обращением к жителям Украины, размещенном известными радикальными политиками В. Новодворской и К. Боровым. Он опубликован под заголовком «Воззвание к народу Украины “К оружию”».

Авторы ролика обвиняют российские власти во вторжении в Украину и призывают жителей этой страны к борьбе с армией России. В российском представительстве корпорации Google – владельце сервиса YouTube – заявили CNews, что изучают ситуацию.

Провайдеры обязаны заблокировать доступ к данному ролику, однако не все из них могут сделать это точечно. Многие провайдеры, например, «Ростелеком» и «Вымпелком», обычно блокируют по IP-адресу, что приводит к недоступности всего ресурса целиком. На момент публикации материала – 8 марта в 12 часов по Москве – абонентам «Вымпелкома» ролик с обращением к украинцам и весь YouTube был доступен (вероятно, провайдер еще не успел его заблокировать).

В пятницу, 7 марта, на недоступность YouTube жаловались абоненты «Акадо». Правда, «Акадо» имеет систему DPI для «тонкой» блокировки интернет-страниц по их адресу. В самой компании назвали произошедшее технической ошибкой.

Ранее Генпрокуратура признала экстремистским один из блогов на сервисе Blogspot.ru, также принадлежащем Google. Этот блог до сих пор не удален и не заблокирован, а потому он продолжает находиться в реестре запрещенных сайтов. При этом Роскомнадзор сменил в соответствующей строчке реестра IP-адрес: теперь он такой же, как и IP-адрес, с которым в реестр был внесен YouTube. Не исключено, что по данному IP-адресу могу работать и другие сервисы Google ***(Генпрокуратура России начала блокировать YouTube из-за обращения к украинцам // InternetUA (http://internetua.com/genprokuratura-rossii-nacsala-blokirovat-YouTube-iz-za-obrasxeniya-k-ukraincam). – 2014. – 8.03).***

***

Д. Ассанж, основавший сайт WikiLeaks, заявил, что в ближайшие несколько лет АНБ США (Агентство национальной безопасности) и британские спецслужбы смогут следить за каждым человеком на Земле.

По словам Д. Ассанжа, выступившего на международной конференции в Остине, уже сегодня разрабатывается так называемая «постмодернистская власть», то есть система власти, представители которой имеют полный контроль над наблюдательными структурами.

Кроме того, он отметил, что возможности в данной сфере удваиваются каждые 1,5 года, добавив, что мы «движемся к новому тоталитарному миру – но не в духе Пола Пота и Сталина, а тоталитарного режима в том смысле, что он будет охвачен тотальной слежкой» ***(Через несколько лет спецслужбы будут следить за каждым на планете // Информ Вест (http://informvest.com/2014/03/10/cherez-neskolko-let-specsluzhby-budut-sledit-za-kazhdym-na-planete/15388.html). – 2014. – 10.03).***

Проблема захисту даних. DDOS та вірусні атаки

В украинском Facebook началась очередная эпидемия. Хитроумные вирусописатели решили ловить пользователей на любопытство. Неизвестно, кто первым запостил картинку-ссылку с предложением узнать, кто удалил вас из друзей (who deleted me), но сейчас она довольно быстро распространяется по украинскому сегменту социальной сети.

Чтобы заразиться, достаточно перейти по ссылке. Иногда после перехода срабатывает антивирус. С зараженного аккаунта вирус начинает постить от имени пользователя, тегируя его друзей, и таким образом распространяется далее. Также от имени пользователя размещается коммент: see the people that deleted you on fb (посмотрите, кто удалил вас в Facebook).

Напомним, ровно год назад в украинском сегменте Facebook уже прошла «эпидемия»: вирус предлагал пользователю перейти по ссылке и установить расширение для браузеров Chrome и Firefox ***(Новый Facebook-вирус предлагает узнать, кто удалил вас из друзей // AIN (http://ain.ua/2014/02/24/513983). – 2014. – 24.02).***

***

За последние три месяца ряд американских ритейлеров признали, что стали жертвами хакерских атак, поразивших их системы через POS-терминалы. В США о крупных утечках данных сообщили ритейлеры Target и Neiman Marcus, потерявшие в общей сложности более 110 млн номеров банковских карт.

Как показали опубликованные новые данные, ритейлеры параллельно стали жертвами еще одной, правда не столь масштабной, атаки, в которой хакерами в качестве целей также выбиралось торговое оборудование.

21 февряля стало известно о том, что ритейлеры в 11 странах стали жертвами одной и той же вредоносной программы ChewBacca, заражавшей торгово-кассовое оборудование и перехватывавшей данные из оперативной памяти платежных терминалов. Такие данные озвучили в компании RSA Security, где проанализировали вредоносное ПО и его серверную инфраструктуру, пишет cybersecurity.ru.

В компании говорят, что большая часть заражений действительно пришлась на США, однако Штаты не стали единственным местом, что софт ChewBacca успел поработать. Согласно результатам анализа RSA, кроме

США этот вредонос также был выявлен на территории России, Канады и Австралии. В общей сложности следы присутствия отмечены в 11 странах. У. Флейдер, менеджер подразделения Cybercrime Research Lab в RSA, говорит, что в настоящее время присутствие вредоноса выявлено на 119 POS-терминалах у 45 разных ритейлеров, правда, две трети из них расположены в Северной Америке.

По его словам, банда, стоящая за ChewBacca, только лишь в США скомпрометировала не менее 50 тыс. банковских карт, причем компрометировались даже данные, зашифрованные на магнитных полосах карт. В RSA отказались называть ритейлеров, пострадавших от этой атаки, однако в компании говорят, что во всех случаях правоохранительные органы уже были поставлены в известность по фактам краж банковских данных.

Напомним, что впервые о вредоносе ChewBacca стало известно еще в декабре, когда этот код попал в поле зрения аналитиков из «Лаборатории Касперского». Одной из наиболее интересных функций ChewBacca (кроме возможности перехвата данных из RAM) является то, что этот код применяет Tor-соединения для конфиденциальности процесса общения вредоноса и контрольного сервера. После попадания на компьютер это ПО размещает на компьютере проксирующий Tor-клиент, который подключается к серверу через .onion-адрес. Напомним, что .onion – это псевдо-домен, который нужен только для общения в рамках Tor-сети ***(Вредоносный код ChewBacca через POS-терминалы поразил торговые сети 11 стран // Центр исследования компьютерной преступности (http://www.crime-research.ru/news/24.02.2014/7661/). – 2014. – 25.02).***

***

Специалисты по информационной безопасности говорят о выявлении уязвимости в iOS, позволяющей приложениям записывать все действия пользователя по сенсорному экрану, а также регистрировать нажатия кнопок. Особо стоит отметить, что данный трюк работает с невзломанными устройствами iOS, а также с приложениями, работающими в фоновом режиме.

В ИТ-компании FireEye говорят, что сенсорные функции являются основными средствами ввода в iOS-устройства, поэтому данный баг сродни возможности размещения в системе клавиатурного шпиона. Кроме того, атакующий может получать данные о координатах X и Y для определения того, какие именно символы были нажаты на планшете или смартфоне.

Сообщается, что указанная уязвимость присутствует в операционных системах iOS 7.x (включая текущую iOS 7.0.6), а также в iOS 6.1.x. В FireEye говорят, что уже уведомили Apple о проблеме в продукте и ожидают соответствующего патча.

Специалисты также говорят, что они обнаружили способ обхода процесса рассмотрения программ в Apple App Store. Сообщается, что он связан с багом регистрации нажатий по экрану. «Мы уже создали

концептуальное приложение по мониторингу невзломанных устройств iOS 7.0.x-устройств. Это мониторинговое приложение записывает все пользовательские манипуляции с сенсорным экраном и все нажатия клавиш, находясь в фоновом режиме. Приложение регистрирует в том числе нажатия по кнопке Home, по кнопкам громкости, а также по системе Touch ID. Приложение способно передавать эти данные на удаленный сервер, подконтрольный оператору атаки», – отмечают в FireEye.

В FireEye говорят, что атакующие могут использовать технику социальной инженерии для заражения планшета или смартфона вредоносным софтом. По словам специалистов, iOS 7 позволяет контролировать, какие приложения могут обновлять их данные, находясь в фоновом режиме, но и эти ограничения можно обойти, так как вредоносное приложение можно задекларировать как приложение потокового вещания, например музыкальный плеер ***(В iOS выявлен критически опасный баг – FireEye // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/02/26/ios-bug.html). – 2014. – 26.02).***

***

Исследователи из Ливерпульского университета обнаружили, что вирус может распространяться через Wi-Fi. Им удалось доказать это на примере вредоноса Chameleon, активность которого была зафиксирована в 2012 г. По словам ученых, вирус может не только быстро распространяться, но и выбирать наименее защищенные точки доступа Wi-Fi.

Исследователи провели демонстрацию атаки в Белфасте и Лондоне в лабораторных условиях. По итогам эксперимента оказалось, что Chameleon распространялся через точки доступа, которые предоставляли доступ к сети как обычным, так и корпоративным пользователям.

Как утверждают ученые, в городах с более высоким количеством населения точек доступа гораздо больше, и они находятся довольно близко друг к другу, что позволяет вирусу распространяться более быстро.

Профессор А. Маршалл утверждает, что при заражении точек доступа Chameleon не влиял на их работу. Он только собирал данные подключенных к ним пользователей. Затем вирус пытался обнаружить дополнительные точки доступа для дальнейшего заражения.

Стоит отметить, что Chameleon удалось избежать обнаружения антивирусными программами. Дело в том, что большинство решений настроены на поиск вредоносов в Интернете и на компьютере, а этот вирус распространяется через сеть Wi-Fi.

«Соединения Wi-Fi все чаще становятся целью злоумышленников из-за хорошо известных уязвимостей в их системе безопасности, что препятствует обнаружению и защите от вируса», – отметил А. Маршалл ***(Исследователи продемонстрировали распространение вируса через Wi-Fi // ООО «Центр информационной безопасности»***

(http://www.bezpeka.com/ru/news/2014/02/26/Wi-Fi-virus.html). – 2014. – 26.02).

***

Как следует из сообщения исследователей безопасности из Лаборатории Касперского, по итогам 2013 г. стало очевидным, что количество банковских троянов, ориентированных на пользователей операционной системы Android, начало стремительно возрастать. Так, за отчетный период компания зафиксировала появление порядка 100 тыс. подобных новых вирусов, что более чем в два раза больше по сравнению с показателями 2012 г.

Исследователи также подчеркивают, что свыше 98 % всех мобильных вредоносных программ, обнаруженных в течение 2013 г., были разработаны для инфицирования мобильных устройств на базе Android.

Не менее важной является тенденция по использованию мобильных приложений для распространения вирусов: за отчетный период было выявлено порядка 4 млн таких программ. В целом за 2012–2013 гг. было обнаружено более 10 млн таких программ.

Что касается наибольшего количества жертв злоумышленников, то 40 % уникальных нападений пришлось на пользователей из России. На втором и третьем местах – Индия (8 %) и Вьетнам (4 %). За ними следуют Украина (4 %) и Великобритании (3 %) ***(ЛК: Количество банковских Android-троянов стремительно растет // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/02/26/android-trns.html). – 2014. – 26.02).***

***

На сайт «СавикШустерСтудии» осуществляется DDoS-атака, передает корреспондент proIT со ссылкой на сообщение пресс-службы.

Так, 24 февраля на сайте 3s.tv начала выходить онлайн-трансляция программы «Шустер LIVE». 25 февраля, во время прямого эфира на сайт началась DDoS-атака.

«Наш сайт подвергался DDOS-атаке. Это могло вызвать перебои в трансляции. Мы делаем все возможное для возобновления его стабильной работы», – заявил П. Метальников, ИТ-директор «СавикШустерСтудии».

Напомним, на программе 24 февраля обсуждалось правительство народного правления и коалиция ***(Сайт студии Шустера подвергся DDoS-атаке // proIT (http://proit.com.ua/news/internet/2014/02/26/134959.html). – 2014. – 26.02).***

***

Злоумышленники использовали рекламную сеть YouTube для распространения банковского трояна Caphaw. Об этом сообщают эксперты компании Bromium Labs. По их словам, рекламные объявления YouTube In-

Stream перенаправляли пользователей на вредоносные веб-сайты, которые содержали набор эксплоитов Styx.

Эти страницы эксплуатировали уязвимости, существующие на системах жертв, посредством осуществления атак типа drive-by-download, что позволяло заражать компьютеры вирусом Caphaw. После установки на систему вредоносная программа идентифицировала версию Java, на основе которой запускала подходящий эксплоит.

Стоит отметить, что пока экспертам компании не удалось установить способ, который использовали злоумышленники для обхода внутренней проверки рекламы Google. По словам представителей последней, специалисты поискового гиганта изучают инцидент, а затем примут соответствующие меры.

По данным Bromium Labs, для соединения с C&C-сервером банковский троян использует алгоритмы создания доменных имен (Domain Generation Algorithm, DGA). Контрольный сервер троянского вируса находится на территории Европы. Важно также, что уже несколько антивирусных компаний отметили Caphaw как «вредоносный».

Количество пользователей, ставших жертвами данной вредоносной кампании, пока неизвестно. Следует также отметить, что уязвимость в Java, которую эксплуатируют злоумышленники, Oracle исправила еще в прошлом году. Поэтому SecurityLab настоятельно рекомендует вовремя обновлять продукцию Java, а также антивирусные решения и операционные системы ***(Банковский троян Caphaw использовал для распространения рекламу YouTube In-Stream // InternetUA (http://internetua.com/bankovskii-troyan-Caphaw-ispolzoval-dlya-rasprostraneniya-reklamu-YouTube-In-Stream). – 2014. – 26.02).***

***

Мобильное приложение WhatsApp, предназначенное для передачи сообщений и выкупаемое социальной сетью Facebook за 19 млрд дол., представляет собой крайне привлекательную для хакеров и государственных шпионов платформу. Об этом со ссылкой на исследователей безопасности из компании Praetorian сообщает издание Ars Technica.

По словам экспертов, проблема заключается в неэффективной реализации методов шифрования, позволяющей третьим лицам с относительной легкостью осуществлять перехват пользовательского трафика. Речь идет о протоколе secure sockets layer (SSL) версии 2, которая подвержена ряду «широко известных атак».

Более того, разработчики WhatsApp также не реализовали механизм защиты certificate pinning, предназначенный для блокирования атак с использованием поддельных сертификатов. Данная технология давно используется в Twitter, Facebook и Google.

Другими существенными недостатками, по мнению исследователей безопасности, являются использование SSL null cipher и SSL export ciphers:

«Это те вещи, которые хотели бы видеть в приложениях сотрудники АНБ» ***(Методы шифрования в WhatsApp – мечта АНБ // InternetUA (http://internetua.com/metodi-shifrovaniya-v-WhatsApp---mecsta-anb). – 2014. – 26.02).***

***

Неизвестные злоумышленники разработали собственный вариант трояна ZeuS, с помощью которого проводят масштабную атаку на клиентов одного из крупнейших разработчиков CRM-систем, компанию salesforce.com. При этом последняя предоставляет свои услуги исключительно под модели SaaS.

Вредоносная программа заражает системы пользователей из числа корпоративных работников и ожидает момента их авторизации на официальном веб-сайте организации (по уникальному адресу *.my.salesforce.com). После этого вирус извлекает конфиденциальную информацию атакуемой компании, сообщают исследователи из Adallom.

«Это не эксплоит для salesforce.com; эта разработанная на базе ZeuS угроза играет на доверительном отношении конечных пользователей к своему поставщику», – подчеркивает эксперт А. Луттвак.

По его словам, обнаружить вирус удалось благодаря системе автоматического оповещения о подозрительных действиях. Тревога была поднята после того, как один из клиентов Adallom «выполнил сотни операций по просмотру salesforce.com в течение короткого периода времени».

В результате расследования выяснилось, что во время этого просмотра вирус в режиме реального времени провел индексацию всей обнаруженной информации ***(Троян ZeuS атаковал клиентов одного из крупнейших разработчиков CRM-систем // InternetUA (http://internetua.com/troyan-ZeuS-atakoval-klientov-odnogo-iz-krupneishih-razrabotcsikov-CRM-sistem). – 2014. – 27.02).***

***

Число украденных учетных записей в социальных сетях за последние 12 месяцев составило 500 млн. Такие данные приводят аналитики корпорации Symantec в отчете Intelligence Report за январь 2014 г., в котором представлен общий обзор актуальных угроз в Интернете.

Число направленных атак, по наблюдениям аналитиков, в январе находится на самой высокой отметке с августа 2013 г., когда после всплеска показатель на протяжении следующих четырех месяцев находился на средне-низком уровне. Количество обнаруженных уязвимостей также возросло после низких показателей в ноябре-декабре. Однако 555 уязвимостей в январе – это все же меньше, чем 663 уязвимости, найденные в октябре.

Из всех атак на социальные сети 82 % составили фальшивые предложения. Второе место заняли атаки типа likejacking («угон лайков»), доля которых составила 8 % всех атак.

«Основным видом “угона” учетных записей является таргетированная рассылка спама, якобы от самих учетных сетей (с подменой ссылок). Так же не стоит забывать о том, что часто пользователи сами оставляют всю исчерпывающую информацию о себе в социальных сетях, которая достаточна для ответов на контрольные вопросы при изменении e-mail или пароля. Так же не снижается процент людей, использующих одни и те же пароли для многих сервисов либо использующих пароли типа qwerty или “12345”, – объяснил менеджер по работе с финансовым сектором, Check Point Software Technologies Д. Титков. – Сейчас все действия злоумышленников направлены на извлечение экономической выгоды. Данные учетных записей могут быть проданы сторонним людям, которые заинтересованы в компрометировании владельца, могут быть использованы для создания паники на фондовом рынке (как это уже было с Twitter-аккаунтом информационного агентства Associated Press) или же для дальнейшей таргетированной атаки на френд-листы жертв».

«Взламывая персональную страницу человека, злоумышленники получают доступ ко всей информации пользователя, включая личную переписку, контакты друзей. Таким образом, можно найти пароли и снять деньги с банковской карты, узнать конфиденциальные данные, отправлять рассылки по списку контактов. При этом довольно часто взламывают аккаунты известных людей, которых читают тысячи подписчиков. Периодически на странице того или иного популярного блоггера неожиданно появляется ссылка на нелегальный контент», – добавила директор по маркетинговым коммуникациям Orange Business Services в России и странах СНГ Д. Абрамова.

При этом способы безопасности не меняются – длинные сложные пароли, регулярная их смена, блокировка ботов. «Но пользователи, по-прежнему, исходят из соображений удобства, игнорируя вопросы безопасности. Это и создает новые прецеденты, и приносит новые выгоды мошенникам», – отметила Д. Абрамова.

«Ваш пароль – это ключ, открывающий мошенникам доступ к вашим учетным записям в сети. И хотя очень удобно и привычно использовать имя любимого питомца для всех сервисов, взломав этот пароль, злоумышленник сможет очень легко получить доступ к другим вашим учетным записям. Поэтому убедитесь, что вы используете сложные пароли и не повторяете их дважды, – рекомендует Д. Титков. – Во-вторых, нужно быть более внимательным к почтовым сообщениям, которые к вам приходят, и тем более к ссылкам, по которым вы переходите. В-третьих, тщательно фильтруйте указываемую о себе информацию на страницах в социальных сетях – будьте более разборчивы и тщательно следите за тем, что вы публикуете, и кто может получить доступ к этой информации. Большая часть информации,

которую вы оставляете в Интернете, сегодня может быть использована кем угодно – даже если вы не знаете этих людей. И, конечно, не стоит пренебрегать средствами антивирусной защиты и их своевременными обновлениями. 85 % атак в Интернете осуществляются за счет перенаправления пользователей с легитимных сайтов, поэтому эти меры будут хорошей страховкой» ***(За год в мире украдено 500 млн аккаунтов в соцсетях // InternetUA (http://internetua.com/za-god-v-mire-ukradeno-500-mln-akkauntov-v-socsetyah). – 2014. – 28.02).***

***

Бразильские хакеры угрожают сорвать чемпионат мира по футболу, осуществляя разнообразные атаки – от вывода из строя сайтов до похищения конфиденциальных данных. Поскольку киберпреступность в латиноамериканской стране процветает, в настоящее время власти пытаются всеми силами защитить правительственные ресурсы и сайты FIFA. Об этом 26 февраля сообщило агентство Reuters.

Напомним, что в июне прошлого года в Бразилии проходили массовые акции протеста в связи с тем, что правительство страны выделило из госбюджета на приготовления к чемпионату мира по футболу 14 млрд дол. Теперь же к протестующим присоединились хакеры.

«Мы уже составляем планы. Я не думаю, что они смогут как-то нас остановить», – заявила Э. Диоратто, утверждающая, что является членом Anonymous.

Корреспонденты Reuters связались online с Э. Диоратто, а также с другими самопровозглашенными членами Anonymous. Они не смогли с уверенностью определить, что хакеры являются именно теми, за кого себя выдают, однако попытались разобраться в масштабе угроз, которые те представляют.

По словам Anonymous, чемпионат привлечет беспрецедентное количество зрителей, поэтому сайты FIFA являются идеальной мишенью. Они сообщили, что атаки будут осуществляться на официальные ресурсы FIFA и спонсоров мероприятия, однако рядовые бразильские пользователи не пострадают.

«Вопрос не в том, будут ли совершены атаки, а в том, когда именно. Поэтому очень важно обеспечить устойчивость и своевременное отражение», – отметил эксперт по безопасности У. Бир. Тем не менее, власти Бразилии заявили, что страна готова, насколько это вообще возможно. Что касается представителей FIFA, то они отказались комментировать ситуацию ***(Бразильские хакеры угрожают сорвать Чемпионат мира по футболу // InternetUA (http://internetua.com/brazilskie-hakeri-ugrojauat-sorvat-cempionat-mira-po-futbolu). – 2014. – 28.02).***

***

Tilon был активным семейством вредоносных программ, специально разработанным для хищения средств с банковских счетов. Впервые он был обнаружен в 2012 г. Исследователи компании Delft Fox-IT установили, что новая версия вируса под названием Silon является банковским трояном SpyEye2. Последний – более сложная версия трояна SpyEye.

Большая часть функций вредоносной программы осталась прежней. Так, вирус напоминает банковский троян SpyEye, разработанный 24-летним российским хакером, известным под ником Gribodemon, который был арестован в июле 2013 г.

SpyEye инфицировала более 1,4 млн компьютеров по всему миру начиная с 2009 г. Программа предназначена для кражи данных пользователей и финансовой информации, в том числе и через систему онлайн-банкинга. Кибермошенники могли получать данные кредитной карты клиента, имена пользователей, пароли и PIN-коды. SpyEye тайно заражает компьютер жертвы и предоставляет злоумышленнику право удаленного доступа. Благодаря этому киберпреступники, используя C&C-сервер, могут осуществлять веб-инъекции, устанавливать кейлоггеры и пр.

Исследователи подтвердили, что команда, разработавшая SpyEye, также создала Tilon, получивший название SpyEye2. Управление SpyEye2 осуществляется через единый, унифицированный интерфейс, который был полностью переработан, но все еще содержит несколько уникальных особенностей своего предшественника.

Судя по всему, SpyEye после ареста автора начал терять активность ***(Tilon/SpyEye2 стал менее активным после ареста создателя программы // InternetUA (http://internetua.com/Tilon-SpyEye2-stal-menee-aktivnim-posle-aresta-sozdatelya-programmi). – 2014. – 1.03).***

***

УНІАН, «Тиждень.ua», «Українська правда» та інші інтернет-видання зазнають потужних DDoS-атак

Від 2 березня ведеться потужна DDoS-атака на низку українських інтернет-видань, що висвітлюють суспільно-політичні події, зокрема вторгнення російських військ у Крим. Про атаки на свої сайти заявили УНІАН, «Тиждень.ua», «Українська правда», «События Крыма», Чорноморська ТРК.

Сайт Тиждень.ua зазнає DDoS-атаки з 12-00 2 березня. «Загрозу вдалося локалізувати півгодини тому (2 березня 22.30. – Ред.). На якомусь етапі атака сягнула сотень тисяч запитів до сайту щохвилини. Стандартні заходи безпеки не допомогли розв’язати цю проблему. Тож ми зважилися на надзвичайні кроки і вимушені були на кілька годин припинити роботу сайту. Спроби перешкодити роботі сайту тривають і зараз. Перепрошуємо за тимчасові незручності. Залишайтеся з нами!» – повідомила редакція ввечері 2 березня.

На сайт УНІАН масштабна атака розпочалася близько першої години ночі 3 березня. «Найпотужніша безперервна DDoS-атака триває досі. У зв'язку з цим можливо періодичне повне "падіння" сайту, некоректне відображення контенту та повільна робота ресурсу. Ми приносимо свої вибачення нашим читачам за проблеми з доступом на сайт, і докладаємо всіх зусиль для якнайшвидшого відновлення нормальної працездатності сайту», – повідомила редакція.

Атака на «Українську правду» розпочалася вдень 3 березня. Перед цим редакція отримала лист, який процитувала у Facebook: «Ваш продажный, прозападный сайт. Будет Здыхать от ддоса вместе с остальными. Unian.net уже понял что мы не шутим. http://lenta.ru/news/2014/03/03/unian/ Вам небудет места в сети. Продажные западные низкопробные б***оты. Меня зовут Себастьян Перейро. Чао буратино! Слава Росии Путину и ФСБ!».

Інтернет-портал «События Крыма» періодично стає недоступним через потужні DDoS-атаки, що тривають уже більше тижня. «Велика частина комп'ютерів, з яких вона йде, розташована в Москві», – пише видання. Такі дії редакція пов'язує з тим, що сайт пише правдиві новини про події в Криму і не підтримує введення російських військ до Криму. Страждають від DDoS-атаки й інші кримські інтернет-ресурси, зокрема «Кафа» і «Свіжа газета».

Сайт «Чорноморської телерадіокомпанії» також зазнає потужних DDoS-атак. Про це в коментарі Інституту масової інформації повідомила головний редактор телерадіокомпанії О. Квітко. «Як вдалося з'ясувати, велика частина з них здійснюється з Дніпропетровська. Онлайн-трансляція нашого каналу на даний момент призупинена. Ми робимо все можливе, щоб відновити роботу сайту», – повідомила вона.

Як писала «Телекритика», 3 березня «Чорноморська ТРК» була вимкнена з ефіру. Мовлення було припинено на всій території Кримського півострова за рішенням республіканського телерадіопередавального центру ***(УНІАН, «Тиждень.ua», «Українська правда» та інші інтернет-видання зазнають потужних DDoS-атак // «Телекритика» (http://www.telekritika.ua/rinok/2014-03-03/91057). – 2014. – 3.03).***

***

Эксперты зафиксировали новую волну фишинг-атак, направленных на пользователей учетных записей Apple ID. В письмах, предназначенных для владельцев iPhone, iPad и Mac, злоумышленники пытаются убедить людей в том, что их аккаунт заблокирован и предлагают обновить пользовательские данные, пройдя по специальной ссылке.

В письмах говорится, что это якобы автоматическое сообщение, сформированное системой безопасности Apple. Злоумышленники дают 48 часов на то, чтобы подтвердить информацию. «Ваш Apple ID был заблокирован, так как мы не смогли проверить достоверность сведений, которые содержатся на вашей учетной записи. После того, как вы обновите данные, мы снова повторим проверку и снимем блокировку. Это поможет

защитить вашу информацию в будущем. Процедура не займет больше трех минут. Чтобы продолжить, подтвердите сведения на вашей учетной записи, пройдя по ссылке далее и следуя нашей инструкции», – говорится в фишинговой рассылке.

Письма отправляются с разных адресов (включая appleid@id.appleidupdates.com) и содержат логотип Apple, поэтому невнимательный пользователь может поверить рассылке. Перейдя по прилагаемому линку Click to Validate Your Account, человек увидит стилизованный под apple.com веб-сайт, предлагающий ввести параметры учетной записи Apple ID.

Если пользователь не поймет подвоха и введет свой идентификатор Apple ID и пароль, он будет переадресован на подлинную страницу сервиса. Таким образом, человек может подумать, что ошибся при вводе учетных данных и успешно авторизоваться со второй попытки. Большинство пользователей будут уверены, что прошли процесс восстановления и от них больше ничего не требуется.

Будьте бдительны! Получив в распоряжение пароли от учетных записей Apple ID, хакеры могут использовать их по своему усмотрению. Пострадавшим следует обратиться в службу поддержки Apple, которая поможет восстановить доступ и сменить пароль аккаунта ***(Как уводят пароли от Apple ID // InternetUA (http://internetua.com/kak-uvodyat-paroli-ot-Apple-ID). – 2014. – 4.03).***

***

Специалисты по информационной безопасности говорят об обнаружении сети из взломанных домашних роутеров. Сеть включает в себя более 300 тыс. роутеров в домах и малых офисах, захватить роутеры удалось благодаря наличию уязвимостей в программном обеспечении сетевых устройств.

В ИТ-компании Team Cymru говорят, что обнаруженная ими бот-сеть из роутеров является крупнейшей в своем роде. При этом Cymru отмечает, что пока не слишком понятно, как именно операторы сети собираются использовать сеть из скомпрометированных роутеров. В описании на сайте Team Cymru сказано, что впервые они зафиксировали факты компрометации отдельных роутеров разных производителей в январе этого года. Первые жертвы были расположены в Восточной Европе, но в настоящее время подавляющее большинство жертв расположено на территории Вьетнама, а небольшая часть – в Европе и ряде других стран.

«После того как роутер взломан, атакующие могут подменять внутренние инструкции, перенаправляя пользователей на поддельные веб-сайты без изменения доменного имени», – говорится в заметке компании. «Потенциально, атакующий может получить полный контроль над интернет-трафиком пользователя, а также заражать его компьютер передаваемым вредоносным программным обеспечением».

С. Санторелли, ИТ-специалист компании Team Cymru, говорит, что наличие сети из зараженных роутеров было установлено как раз на фоне наличия большого количества поддельных DNS-запросов со стороны конечных пользователей. Специалистов заинтересовал тот факт, что пользовательские устройства в массовом порядке работают не с провайдерскими DNS, а со сторонними серверами.

По словам С. Санторелли, эта атака похожа на недавний ИТ-инцидент в Польше, когда взломанные роутеры одного из провайдеров массово перенаправлялись на вредоносные сайты, где хакеры предпринимали усилия по краже логинов и паролей пользователей от банковских систем ***(Обнаружена бот-сеть из 300 000 взломанных домашних роутеров // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/04/router-botnet.html). – 2014. – 4.03).***

***

Вредоносные программы, заражающие электронную «начинку» банкоматов, – явление не слишком распространенное, поэтому появление новых образцов подобного ПО неизменно вызывает интерес специалистов. В распоряжении вирусных аналитиков компании «Доктор Веб» появился образец троянца Trojan.Skimer.19, способного инфицировать банкоматы одного из зарубежных производителей, используемые многочисленными банками на территории России и Украины.

Это уже третий тип банкоматов, на которые ориентированы троянцы семейства Trojan.Skimer. Согласно имеющейся у «Доктор Веб» информации, организованные злоумышленниками атаки на банковские системы с применением Trojan.Skimer.19 продолжаются и по сей день.

Основной вредоносный функционал этого троянца, как и его предыдущих модификаций, реализован в виде динамической библиотеки, которая хранится в NTFS-потоке другого вредоносного файла, детектируемого антивирусным ПО Dr.Web как Trojan.Starter.2971. Если в инфицированной системе используется файловая система NTFS, Trojan.Skimer.19 также хранит свои файлы журналов в потоках – в эти журналы троянец записывает треки банковских карт, а также ключи, используемые для расшифровки информации.

Заразив операционную систему банкомата, Trojan.Skimer.19 перехватывает нажатия клавиш EPP (Encrypted Pin Pad) в ожидании специальной комбинации, с использованием которой троянец активируется и может выполнить введенную злоумышленником на клавиатуре команду. Среди выполняемых команд можно перечислить следующие: сохранить лог-файлы на чип карты, расшифровать PIN-коды; удалить троянскую библиотеку, файлы журналов, «вылечить» файл-носитель, перезагрузить систему (злоумышленники дважды отдают команду инфицированному банкомату, второй раз – не позднее 10 секунд после первого); вывести на

дисплей банкомата окно со сводной статистикой: количество выполненных транзакций, уникальных карт, перехваченных ключей и т. д.; уничтожить все файлы журналов; перезагрузить систему; обновить файл троянца, считав исполняемый файл с чипа карты.

Последние версии Trojan.Skimer.19 могут активироваться не только с помощью набранного на клавиатуре банкомата кода, но и с использованием специальных карт, как и в более ранних вариантах троянских программ данного семейства. Для расшифровки данных Trojan.Skimer.19 применяет либо встроенное ПО банкомата, либо собственную реализацию симметричного алгоритма шифрования DES (Data Encryption Standard), используя ранее перехваченные и сохраненные в журнале ключи ***(Новый троян-скиммер угрожает банкам // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/04/skimming-trn.html). – 2014. – 4.03).***

***

Используя изображения и популярные в сети фотографии котов и заката, хакеры передавали команды компьютерным системам, инфицированным вредоносным приложением Zbot. Об этом сообщают исследователи безопасности из Trend Micro.

Как следует из сообщения эксперта Д. Губмана, атака злоумышленников ориентирована на клиентов нескольких европейских банков.

«Мы обнаружили только фотографии заката, но другие исследователи безопасности сообщили об аналогичных файлах с изображениями кота, – следует из отчета. – С помощью стеганографии в них был скрыт перечень финансовых организаций, мониторинг которых должен проводить вирус. Этот список включает в себя компании со всего мира, однако в большинстве своем это банки Европы и Ближнего Востока».

По словам другого исследователя Trend Micro Р. Фергюсона, подобный дилетантский метод сокрытия файлов конфигурации позволяет обойти многие традиционные методы обеспечения безопасности.

При этом необычность подобной вредоносной кампании заключается в том, что фотографии используются для передачи команд довольно сложному, многофункциональному и дорогому в разработке финансовому вирусу Zbot ***(Хакеры распространяли вирус Zbot с помощью фотографий заката и котов // InternetUA (http://internetua.com/hakeri-rasprostranyali-virus-Zbot-s-pomosxua-fotografii-zakata-i-kotov). – 2014. – 5.03).***

***

Как следует из сообщения в блоге египетского исследователя безопасности И. Раафата, ему удалось обнаружить опасную уязвимость на одном из поддоменов компании Yahoo! suggestions.yahoo.com.

Брешь позволяла потенциальному злоумышленнику удалить с сайта, а точнее из службы Yahoo’s Suggestion Board, произвольные нити обсуждений, а также и комментарии к ним.

Эксплуатация уязвимости позволяет атакующему повысить свои привилегии и получить таким образом возможность удалить более 365 тыс. сообщений и 1,1 млн комментариев из базы данных компании.

Пример удаления комментария на suggestions.yahoo.com выглядит так:

prop=addressbook&fid=367443&crumb=Q4.PSLBfBe.&cid=1236547890&cmd=delete_comment ***(Уязвимость в Yahoo! позволяла хакерам удалить 1,5 миллиона записей из базы данных компании // InternetUA (http://internetua.com/uyazvimost-v-Yahoo--pozvolyala-hakeram-udalit-1-5-milliona-zapisei-iz-bazi-dannih-kompanii). – 2014. – 4.03).***

***

Специалисты «Лаборатории Касперского» обнаружили почти 900 скрытых онлайн-сервисов, постоянно работающих в анонимной сети Tor. Анализ этой сети, функционирующей в рамках так называемого «подпольного Интернета», позволил прийти к заключению, что подобная анонимность в общении и создании различных веб-сервисов все больше привлекает киберпреступников.

Сеть Tor представляет собой свободное программное обеспечение, работающее через Интернет. Равно как и в любом другом веб-пространстве ее пользователи посещают сайты, обмениваются сообщениями на форумах и в чатах, пользуются различными сервисами. Принципиальное отличие от «обычного» Интернета заключается в том, что Tor обеспечивает полную анонимность своих пользователей при помощи так называемой «луковой маршрутизации» – многослойной системы прокси-серверов, шифрующих каждую передачу данных.

Таким образом, если в традиционном сегменте Интернета у каждого веб-сайта и сервиса есть доменное имя, позволяющее узнать, кто является владельцем ресурса и где он находится физически, то Tor, используя «псевдодомены», делает любые попытки получить персональную информацию о владельце бессмысленными.

Все эти особенности сети Tor привлекают, конечно, не только законопослушных пользователей, желающих сохранить конфиденциальность своих контактов и данных. Киберпреступники начинают все активнее использовать эту анонимную сеть для создания своей вредоносной инфраструктуры. К настоящему времени «Лаборатория Касперского» обнаружила ряд зловредов, так или иначе использующих возможности Tor. Среди них 64-битный троянец ZeuS с центром управления через сеть Tor, вредоносная программа ChewBacca с функционалом обмена данными через Tor, а также первый Tor троянец для Android.

Помимо анонимности, которая, безусловно, играет на руку киберпреступникам, эта сеть располагает также множеством ресурсов,

облегчающих задачу создания и распространения вредоносного ПО: командно-контрольные серверы, панели администратором и т. п.

«Размещение командно-контрольных серверов в сети Tor затрудняет их идентификацию, блокирование или полный вывод из строя. И хотя от киберпреступников требуется больше усилий для создания в Tor центра коммуникации со своими зловредами, мы считаем, что количество вредоносного ПО, использующего возможности этой анонимной сети, будет расти», – отметил С. Ложкин, антивирусный эксперт «Лаборатории Касперского» ***(Киберпреступники уходят в Tor-сети // InternetUA (http://internetua.com/kiberprestupniki-uhodyat-v-Tor-seti). – 2014. – 6.03).***

***

Исследовательская компания Blue Coat Security Labs, изучающая вопросы безопасности в Интернете, назвала главным источником вредоносного программного обеспечения мобильную рекламу.

Уровень угрозы, исходящий от мобильной рекламы, превысил даже традиционного лидера – сайты с материалами «для взрослых».

Согласно исследованию, в феврале 2014 г. каждое пятое мобильное устройство заразилось вирусом, содержащимся в интернет-рекламе – данный показатель втрое больше, чем статистика за 2012 г.

При этом характер вредоносных программ не изменился: в первую очередь, с помощью рекламы распространяются вирусы, выдающие себя за популярные приложения.

Всё чаще в рекламе появляются приложения-шпионы, которые ищут уязвимости, выясняя тип операционной системы и браузера, а также, их модификации. Активизировались программы, анализирующие интернет-трафик чтобы узнавать привычки пользователя, его интересы и поисковые запросы ***(Мобильная реклама признана главным рассадником вирусов в сети // Блог Imena.UA (http://www.imena.ua/blog/mobile-ad-virus-place). – 2014. – 6.03).***

***

Специалисты компании «Доктор Веб» исследовали вредоносную программу Trojan.Rbrute, предназначенную для взлома паролей Wi-Fi-роутеров методом перебора (brute force), а также подмены адресов DNS-серверов, указанных в настройках этих устройств. Злоумышленники используют данную вредоносную программу для распространения другого троянца, известного под именем Win32.Sector.

Запустившись на инфицированном компьютере, работающем под управлением Windows, Trojan.Rbrute устанавливает соединение с удаленным сервером и ожидает от него соответствующих команд. В качестве одной из них троянец получает диапазон IP-адресов для выполнения сканирования. Вредоносная программа обладает функционалом по подбору паролей к следующим моделям Wi-Fi-роутеров: D-Link DSL-2520U, DSL-2600U, TP-

Link TD-W8901G, TD-W8901G 3.0, TD-W8901GB, TD-W8951ND, TD-W8961ND, TD-8840T, TD-8840T 2.0, TD-W8961ND, TD-8816, TD-8817 2.0, TD-8817, TD-W8151N, TD-W8101G, ZTE ZXV10 W300, ZXDSL 831CII и некоторым другим. Фактически, троянец способен выполнять две команды: сканирование сети по заданному диапазону IP-адресов; перебор паролей по словарю.

При этом перечисленные команды не взаимосвязаны и могут выполняться троянцем по отдельности. Если по одному из опрошенных IP-адресов обнаруживается работающий роутер, Trojan.Rbrute получает оттуда веб-страницу, определяет модель устройства с использованием тега realm=\», и рапортует об этом событии на управляющий сервер.

Также троянец может получить команду на подбор пароля к обнаруженному роутеру по словарю – такое задание содержит все необходимые исходные данные: IP-адрес цели, DNS для подмены и словарь паролей. В качестве логина Trojan.Rbrute использует значения admin или support.

Если аутентификация с подобранным сочетанием логина и пароля прошла успешно, троянец рапортует на удаленный сервер об успешном факте взлома и посылает роутеру запрос на изменение адресов зарегистрированных в его настройках DNS-серверов. В результате при попытке открытия в окне браузера различных веб-сайтов пользователь может быть перенаправлен на другие ресурсы, специально созданные злоумышленниками. Эта схема в настоящее время используется киберпреступниками для расширения численности бот-сети, созданной с использованием вредоносной программы Win32.Sector.

В целом используемая злоумышленниками схема выглядит следующим образом:

1. На компьютер, уже инфицированный троянцем Win32.Sector, с использованием этой вредоносной программы загружается Trojan.Rbrute.

2. Trojan.Rbrute получает с управляющего сервера задания на поиск Wi-Fi-маршрутизаторов и данные для подбора паролей к ним.

3. В случае успеха Trojan.Rbrute подменяет в настройках роутера адреса DNS-серверов.

4. При попытке подключения к Интернету пользователь незараженного компьютера, использующий подключение через скомпрометированный маршрутизатор, перенаправляется на специально созданную злоумышленниками веб-страницу. С этой страницы на компьютер жертвы загружается троянец Win32.Sector и инфицирует его. Впоследствии Win32.Sector может загрузить на вновь инфицированный ПК копию троянца Trojan.Rbrute. Цикл повторяется ***(Троянец Rbrute атакует роутеры D-Link и TP-Link // InternetUA (http://internetua.com/troyanec-Rbrute-atakuet-routeri-D-Link-i-TP-Link). – 2014. – 6.03).***

***

«Русское Кибер Коммандование» заявило о начале кибервойны против российских военных предприятий.

В ночь на четверг, 6 марта, группа хакеров, назвавшая себя «Русским Кибер Коммандованием», сообщила об осуществлении атаки на серверы ОАО «Рособоронэкспорт». В своем сообщении они заявили, что намерены «объявить кибервойну российским военным предприятиям».

По словам хакеров, они взломали системы Посольства Индии в Москве и отправили главе «Рособоронэкспорта» вредоносное электронное письмо с текстом «Привет Жене Касперскому – его ПО не работает». Кроме того, они инфицировали системы компаний «Сухой», «Оборонпром», «Газфлот», «РУСАЛ» и многих других.

«Русское Кибер Коммандование» опубликовало архивные файлы объемом 448 МБ, содержащие тысячу документов различной степени секретности, которые, по их словам, им удалось похитить. Хакеры также пообещали, что вскоре опубликуют документы, принадлежащие вышеуказанным компаниям. Активисты указали ссылки для скачивания на сайте Cyberguerrilla, а также упомянули о своей поддержке движений Anonymous и LulzSec ***(Хакеры из «Русского Кибер Коммандования» атаковали российские военные предприятия // InternetUA (http://internetua.com/hakeri-iz--russkogo-kiber-kommandovaniya--atakovali-rossiiskie-voennie-predpriyatiya). – 2014. – 6.03).***

***

Сайт «Российской газеты» ранним утром в пятницу, 7 марта, подвергся атаке хакеров. По состоянию на момент написания новости при попытке захода на сайт выдавалось сообщение о внутренней ошибке сервера. Уход сайта в офлайн подтверждает и сервис downforeveryoneorjustme.

Однако ранее, как свидетельствуют скриншоты, разошедшиеся в сети, на сайте «РГ» появлялись сообщения, что кибератаку провела некая группировка украинских хакеров «Кіберсотня». Кроме логотипа «Кіберсотні» на взломанном сайте «Российской газеты» появились изображения, критикующие политику властей РФ по отношению к Украине.

Представители «Российской газеты» пока хакерскую атаку на свой сайт никак не прокомментировали.

В начале марта хакеры взломали сайт телеканала Russia Today и добавили слово «Nazi» (нацист, нацистский) к заголовкам всех англоязычных материалов. Нападение на сайт RT тогда косвенно связали с событиями вокруг Крыма, в первую очередь с тем, что Совет Федерации РФ разрешил ввести войска на территорию Украины для защиты российских граждан. Это решение вызвало крайне негативную реакцию как у ряда интернет-пользователей, так и у лидеров многих стран мира ***(«Украинские хакеры» взломали сайт «Российской газеты» // InternetUA***

(http://internetua.com/ukrainskie-hakeri--vzlomali-sait--rossiiskoi-gazeti). – 2014. – 7.03).

***

Исследователи из General Dynamics Fidelis обнаружили кибератаки на несколько нефтегазовых и правительственных организаций Среднего Востока, осуществленных хакерской группировкой STTEAM. Злоумышленники получили контроль над серверами их веб-сайтов и инфицировали системы организаций трояном с функцией бэкдора.

На взломанных сайтах хакеры опубликовали сообщение «Взломано STTEAM» («Hacked by STTEAM»), продублированное на арабском языке и сопровождающееся эмблемой активистов Anonymous. Кроме того, они оставили несколько угроз нефтегазовым компаниям.

По словам экспертов, этот дефейс был осуществлен с целью отвлечь внимание от более серьезного проникновения в сети организаций и заражения двумя видами троянов с функциями бэкдоров. Исследователи заявили, что злоумышленники, скорее всего, не преследовали политические цели, а искали информацию, которую можно было бы продать.

Код одного из бэкдоров, содержащий буквы турецкого алфавита, способен похищать системную информацию, подключаться к базам данных SQL, перемещать и удалять файлы и т. д. Второй бэкдор имеет те же функции, но помимо этого, может добавлять пользователей в систему, в группу администраторов, отключать межсетевой экран Windows, активировать RDP, запускать Netcat и т. п. ***(Нефтегазовые компании Среднего Востока стали жертвами хакеров // InternetUA (http://internetua.com/neftegazovie-kompanii-srednego-vostoka-stali-jertvami-hakerov). – 2014. – 7.03).***

***

Как сообщают исследователи из Lookout, им удалось обнаружить вредоносное приложение Dendroid, ориентированное на пользователей Android. Вирус представляет собой руткит (Remote Access Toolkit), предоставляющий злоумышленникам удаленный доступ к скомпрометированным устройствам.

В настоящее время создатели Dendroid продают свою разработку всем, кто желает автоматизировать процесс распространения вредоносного ПО, по цене в 300 дол. Авторы вируса заверяют, что инструмент способен скрытно осуществлять видеосъемку, записывать аудио и звонки пользователя, отправлять текстовые сообщения и многое другое.

Более того, руткит содержит несколько функций, предназначенных для того, чтобы скрыть свою активность от антивирусных решений, в том числе от Bouncer на Google Play.

По мнению исследователей, Dendroid является результатом объединения нескольких вредоносных проектов. Об этом свидетельствует

невероятно обширный список возможностей вируса, а также заметно варьирующийся уровень сложности отдельных компонентов – некоторые из них довольно сложно эксплуатировать, не имея соответствующих навыков ***(Вирус Dendroid способен захватить контроль над смартфоном // InternetUA (http://internetua.com/virus-Dendroid-sposoben-zahvatit-kontrol-nad-smartfonom). – 2014. – 8.03).***

***

Компания Qrator Labs, специализирующаяся на защите сайтов от DDoS-атак, подготовила отчет по активности киберпреступников в этой сфере в 2013 г. За прошлый год Qrator Labs с помощью собственного одноименного сервиса нейтрализовала 6644 DDoS-атак. Годом ранее эта цифра составила 3 749. Рост обусловлен как увеличением числа клиентов Qrator Labs, так и ростом активности киберпреступников в целом.

По словам А. Лямина, основателя и генерального директора Qrator Labs, показатели компании отражают тенденцию отрасли. «По нашим оценкам, общее количество атак на российские сайты возросло за прошлый год примерно на четверть. Также возросло среднее число атак, приходящихся на один сайт. Одна из причин происходящего – в том, что осуществить DDoS-атаку в последние годы не становится сложнее. Например, для организации атаки типа DNS Amplification полосой 150 Гб/сек и больше достаточно 5–10 серверов средней мощности».

По сравнению с предыдущим 2012 г., в 2013 г. максимальное число атак в день, нейтрализованных сетью фильтрации трафика Qrator, возросло с 73 до 151. Максимальный размер ботнета, задействованного в атаке, возрос с 207 401 до 243 247 машин. Увеличилась также доля Spoofing-атак – с 43,05 % до 57,97 %. Это атаки, в которых вместо IP-адреса реального пользователя подставляется фальшивый.

Максимальная длительность атаки сократилась с 83 дней в 2012 г. до 22 дней в 2013 г., а уровень средней доступности веб-ресурсов компаний, пользующихся услугами сети Qrator, возрос с 99,71 % до 99,83 %.

«Хакеры стали более гибкими в отношении выбора метода атаки. Мы наблюдаем четкую тенденцию уменьшения длительности атак на наших клиентов – если раньше исполнители атак могли долго пытаться преодолеть защиту, то сейчас речь идет в основном о кратковременных «пробах прочности», за которыми следует отказ от намерений либо смена методики или технологии атаки», – говорит А. Лямин.

На фоне заметного роста «интеллектуализации» ботнетов, имитирующих поведение рядового пользователя, также существенно возросло количество высокоскоростных атак типа SYN-flood. Число атак в 2013 г. увеличилось также в среднем на одного клиента сети Qrator. Такая тенденция уже наблюдалась в 2012 г. по сравнению с 2011 г., однако в 2013 г. темпы роста увеличились в два раза – с 17 % до 34 %.

С марта по октябрь 2013 г. подавляющее число атак производилось с использованием DNS Amplification. Это атаки, когда злоумышленник посылает запрос (обычно короткий в несколько байт) уязвимым DNS-серверам, которые отвечают на запрос уже в разы большими по размеру пакетами. Если при отправке запросов использовать в качестве исходного IP-адреса адрес компьютера жертвы (ip spoofing), то уязвимые DNS-серверы будут посылать ненужные пакеты этому компьютеру, пока полностью не парализуют его работу. Часто объектом такой атаки оказывается инфраструктура провайдера, которым пользуется жертва. Нападения такого типа совершались в прошлом году как на клиентов крупных операторов, так и небольших провайдеров хостинговых услуг.

С октября по декабрь проявила активность крупная бот-сеть, объединяющая более 700 тыс. компьютеров-зомби, которая использовалась для нападения преимущественно на российские банки среднего размера. Эта активность совпала с действиями ЦБ РФ по отзыву лицензий у ряда банков.

В декабре 2013 г. стало расти число атак с использованием технологии NTP Amplification. Такие атаки по принципу организации похожи на DNS Amplification, но вместо DNS-серверов злоумышленники используют серверы синхронизации времени – NTP. Увеличение количества подобных инцидентов продолжается и в первые два месяца 2014 г.

С учетом приведенной статистики можно сказать, что в 2013 г. наблюдался ряд тенденций, которые в 2014 г. продолжат свое развитие:

– Рост числа высокоскоростных атак с использованием Amplification публичных UDP-сервисов;

– совершенствование атак уровня приложений с использованием ботнетов. Такие атаки часто низкоскоростные и алгоритмы их автоматического обнаружения довольно сложны;

– цель 2013 г. у киберпреступников – DNS-серверы; технология DDoS года – DNS Aplification.

«В 2014 г. ситуация с DDoS в Рунете будет зависеть от того, как отреагирует сообщество операторов на вызовы киберпреступников. Два года назад ожидалось, что атаки сетевого уровня будут постепенно уступать место прикладным атакам, но летом 2013 г. преступники смогли организовать атаку 150 Гб/сек, и это не повлекло никакой реакции в индустрии. Следовательно, если не будут предприниматься согласованные меры всех участников межоператорского взаимодействия по противодействию угрозе, с высокой вероятностью можно ожидать устойчивого роста и скоростей, и количества атак», – продолжает А. Лямин.

Другим важным трендом на ближайшие годы могут стать атаки с использованием протокола BGP, отвечающего за глобальную доступность сетей в Интернете (так называемые атаки BGP Hijacking). Суть проблемы заключается в отсутствии механизмов проверки источника маршрутной информации, что в результате делает возможным неавторизованное перенаправление трафика (перехват) на свою AS и его последующий анализ

или сброс. Обнаружить такой перехват со стороны атакуемой AS теоретически невозможно. До 2013 г. было несколько подобных инцидентов, самый известный из них привел к практически глобальной недоступности сервиса YouTube в 2008 г. Однако, начиная с 2013 г., использование данной конструктивной уязвимости BGP встало на поток, а задачи, решаемые атакующими, стали шире. Теперь это не только атаки на отказ в обслуживании, но и перехват трафика (man-in-the-middle), а также использование чужого адресного пространства для других видов хакерской деятельности: рассылка спама, обычные DoS атаки и т. д.

При отсутствии методов непосредственной борьбы с BGP Hijacking единственным решением остается внешний мониторинг, который может позволить оперативно реагировать на возникающие проблемы в глобальной маршрутизации. Для реализации данной амбициозной задачи компания Qrator Labs запустила проект radar.qrator.net, который предоставляет разнообразную аналитику на междоменном сетевом уровне, в том числе, данные по циклам маршрутизации и обнаруженным ботнетам. В ближайшее время Qrator Labs также сможет предоставлять информацию об аномальных маршрутах в сообщениях протокола BGP, что позволит анализировать и пресекать инциденты с неавторизованным перенаправлением трафика ***(За последний год количество DDoS-атак примерно удвоилось // InternetUA (http://internetua.com/za-poslednii-god-kolicsestvo-DDoS-atak-primerno-udvoilos). – 2014. – 8.03).***

***

Компания Marble Security сообщила об обнаружении партии смартфонов от ведущих производителей с предустановленным шпионским ПО. Согласно данным компании, во время расследования инцидента безопасности они обнаружили у одного из своих клиентов вредоносное ПО, замаскированное под приложения Netflix. В ходе расследования удалось выяснить, что многие новые телефоны, которые были приобретены компанией, содержали шпионское ПО.

Среди скомпрометированных устройств были смартфоны и планшеты от Samsung, Motorola, Asus и LG Electronics. После исследования троянского приложения выяснилось, что вредонос собирал пароли и финансовую информацию, а затем отправлял их на сервер, расположенный в России.

По словам технического директора Marble Security Д. Джеванса, устройства были куплены у поставщика уже с установленным вредоносным ПО. С такой же проблемой немного позже в компанию обратился другой клиент.

В настоящее время известно, что вредоносное ПО было установлено до покупки смартфона клиентом. В список скомпрометированных устройств попало семейство Samsung Galaxy Note, телефоны Galaxy 3 и 4 phones, планшеты Asus, смартфон LG’s Nexus S, а также телефоны Motorola Droid ***(Обнаружена партия новых смартфонов на Android с***

предустановленным троянским приложением // InternetUA (http://internetua.com/obnarujena-partiya-novih-smartfonov-na-Android-s-predustanovlennim-troyanskim-prilojeniem). – 2014. – 8.03).

***

Агрессивный вирус Snake («Змея») атакует десятки телекоммуникационных систем Украины, и число таких атак резко возросло с января 2013 г., сообщают эксперты в области кибербезопасности.

Международная компания BAE Systems, работающая в сфере безопасности, сообщила в докладе, выпущенном в пятницу, о выявлении 56 случаев атак Snake по всему миру с 2010 г., причем 32 из них были направлены против Украины.

Двадцать две атаки произошли, начиная с прошлого года; часть из них была направлена против сетей украинского правительства.

По мнению экспертов, вирус, также известный под названием «Уроборос» – по имени мифической змеи, поедающей собственный хвост – позволяет получить беспрепятственный доступ к сетям, в том числе для скрытного ведения слежки или получения контроля над самими системами.

Разработчик вируса Snake неизвестен, но эксперты утверждают, что операторы вируса, по-видимому, находятся в часовом поясе Москвы, а также что в коде обнаружен текст на русском языке.

По мнению аналитиков, Snake напоминает Stuxnet – вирус, атаковавший объекты иранской ядерной программы в 2010 г. ***(Компьютерный вирус Snake атакует десятки телекоммуникационных систем Украины // InternetUA (http://internetua.com/kompuaternii-virus-Snake-atakuet-desyatki-telekommunikacionnih-sistem-ukraini). – 2014. – 10.03).***

***

Компания Microsoft представила отчёт за вторую половину прошлого года, рассказывающий о числе полученных со стороны правоохранительных органов запросов относительно пользовательских данных. Впервые такую статистику Microsoft стала делать публичной в 2012 г., отчитываясь отдельно за первое и второе полугодие.

Доклад под названием Law Enforcement Requests Report сообщает нам о том, что в прошлом году число запросов слегка уменьшилось. Если в 2012 г. Microsoft получила их 75378, то в прошлом лишь 72279. Из них на первое полугодие пришлись 37196 запросов, затрагивающих 66539 аккаунтов пользователей в сервисах Microsoft; на второе – 35083 запроса относительно 58676 аккаунтов.

Из запросов за последнее полугодие 17,85 % не привели к нахождению данных, наличие которых подозревалось, то есть запросы оказались «неоправданными». Ещё 3,4 % запросов Microsoft отказалась удовлетворять. 76 % требований были выполнены, приведя к раскрытию таких данных

пользователей, как имя адрес электронной почты, место проживания и IP-адрес. Наконец, 2,32 % запросов, разрешение на которые дал суд, открыли непосредственно данные, такие как переписка, фото и файлы, в таких сервисах, как Microsoft OneDrive.

Microsoft сообщает, что серия январских хакерских атак привела к решению убрать связанные с подобными запросами документы с серверов компании ***(Во второй половине 2013 года Microsoft получила 72 тысячи запросов на данные пользователей // InternetUA (http://internetua.com/vo-vtoroi-polovine-2013-goda-Microsoft-polucsila-72-tisyacsi-zaprosov-na-dannie-polzovatelei). – 2014. – 10.03).***

***

Pinterest обнародовал первый доклад в порядке транспарентности, документ, содержащий подробную информацию о количестве запросов к базе данных Pinterest государственными и федеральными органами власти, полученных за последние шесть месяцев.

Pinterest за прозрачность отчетности

В отличие от других социальных сетей, таких как Facebook и Twitter, доклад подтверждает, что правительство не часто обращается к Pinterest при сборе информации о пользователях.

В течение шести месяцев: с июля по декабрь 2013 г., было только 12 государственных запросов и ни одного от органов, находящихся за пределами Соединенных Штатов. Только один из запросов был из федерального агентства. Pinterest предоставил информацию для 11 из 12 заявок.

«Каждая компания, которая хранит информацию – от банков до телефонных компаний – должны отвечать на запросы об информации от правоохранительных органов, судов и т. д., – пишет А. Бартон, менеджер проектов в Pinterest, в своем блоге. – Мы считаем важным информировать Вас об этих запросах».

Приведенные цифры намного меньше, чем те, которые были выявлены в отчетах других социальных сетей. Twitter, который публикует доклады «прозрачности» с 2012 г., получил 1410 запросов за последние шесть месяцев 2013 г. На Facebook поступило около 38 тыс. запросов в течение первых шести месяцев 2013 г.

Прозрачность отчетов стала ходовым товаром после того, как прошлым летом в СМИ всплыла информация о том, что известные компании, такие как Facebook, Apple и Yahoo, делятся пользовательскими данными с Агентством национальной безопасности США. Тогда все три компании впервые опубликовали отчеты «прозрачности» ***(Pinterest за прозрачность отчетности // Uinny (http://uinny.ru/index.php?id=1256). – 2014. – 10.03).***