СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(28.12.2015–17.01.2016)

2016 № 1

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(28.12.2015–17.01.2016)
№ 1

Засновники:
Національна бібліотека України імені В. І. Вернадського
Служба інформаційно-аналітичного забезпечення
органів державної влади (СІАЗ)

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

© Національна бібліотека України
імені В. І. Вернадського, 2016

Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Пользователи Facebook заметили изменение в мобильном приложении соцсети: ленту новостей разделили по темам, позволив, например, читать материалы о моде или развлечениях отдельно от спорта или политики. Об этом сообщает tjournal.ru

То, как основная лента разделена по темам, напоминает приложение Paper от Facebook, выпущенное в 2014 г. Paper задумывался как новостной ридер, дробящий поступающий в ленту пользователя контент на тематические материалы и отображающий их в виде журнала.

В Paper можно было читать не только статьи от изданий, но и записи от друзей, однако приложение позиционировалось как отдельный от Facebook сервис. Тогда М. Цукерберг заявлял, что новостная лента Paper будет служить отдельным местом для потребления контента, подчиняясь тренду на дробление функциональности соцсети по нескольким приложениям.

Помимо тематической новостной ленты, компания Facebook также стала тестировать «маркетплейс»: раздел для покупки товаров от различных магазинов и отдельных пользователей. Он появился у небольшого количества американских пользователей ещё в октябре.

В ответ на запрос The Verge представители Facebook заявили, что действительно тестируют интерфейс магазина, но пока он далёк от полноценного запуска. Что касается новостной ленты, то пока не известно, появится ли она у всех пользователей: это нововведение компания не комментировала ***(Фейсбук начал тестировать разделение новостной ленты на темы // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45778/118/lang,ru/). – 2015. – 30.12).***

***

Японская корпорация Panasonic в сотрудничестве с Facebook разработала новую систему хранения больших массивов данных на оптических дисках. Она пригодится дата-центрам, чтобы освободить драгоценное место на серверах от так называемых «холодных» – то есть востребованных редко или вообще никогда – данных.

Технология под названием freeze-ray позволит центрам обработки данным по всему миру сэкономить на эксплуатационных расходах и энергопотреблении, при этом не рискуя сохранностью хранимой в архивах информации. Особые характеристики оптических дисков – их долговечность, совместимость с предыдущими версиями, низкое энергопотребление и устойчивость к изменениям внешней среды – делают их оптимальным решением для «холодного» хранения.

При разработке freeze-ray использовались такие технологии Panasonic как оптические диски высокой плотности, а также программное обеспечение для ЦОДов, облегчающее контроль над библиотеками данных. Со стороны Facebook оказался востребован опыт в проектировании, развертывании, управлении и обслуживании систем хранения в дата-центрах.

В настоящее время Facebook внедряет в своих ЦОДах системы хранения первого поколения на 100 гигабайтных Blu-Ray дисках и рассматривает возможность установки систем второго поколения на базе 300-гигабайтных дисков Archival Disc позже в 2016 г. В перспективе же компании не исключают создания аналогичной системы на 500-гигабайтных и даже терабайтных оптических носителях ***(Panasonic разработала для Facebook систему «холодного» хранения данных // InternetUA (http://internetua.com/Panasonic-razrabotala-dlya-Facebook-sistemu--holodnogo--hraneniya-dannih). – 2016. – 9.01).***

***

По данным Information, Facebook ищет способы установки собственных приложений в обход магазина приложений Play Store для системы Android.

Меры предосторожности приняты на случай возможного конфликта с поисковым гигантом. Помимо Play Store, Google отвечает за другие важные функции Android, вроде пуш-уведомлений, приём платежей и обновление программ.

Источники The Information сообщают, что ранее представители Facebook вели переговоры с производителями Android-смартфонов без сервисов Google. Предмет беседы очевиден: предустановка приложений крупнейшей социальной сети на подобные гаджеты. Также Facebook предлагали свои API по работе с деньгами и защитой от взлома сторонним разработчикам ***(Facebook хочет меньше зависеть от Android и Google // InternetUA (http://internetua.com/Facebook-hocset-menshe-zaviset-ot-Android-i-Google). – 2016. – 9.01).***

***

Соцсеть Facebook считает, что пользователям пора забыть про телефонные номера. Предлагает общаться через Facebook Messenger, аудитория которого уже превышает 800 млн пользователей.

Глава сервиса Д. Маркус напоминает, что Facebook Messenger позволяет писать сообщения, звонить, отправлять смайлики, делиться фотографиями и видео и даже переводить деньги. Все пользователи соцсети идентифицированы и персонализированы, запоминать их номера телефонов больше не нужно.

Свой же телефонный номер придется запомнить в любом случае. Компания рекомендует привязать его к учетной записи, чтобы включить функции «Подтверждения входа» и «Уведомления о входе», которые гарантируют защиту от несанкционированного доступа ***(Facebook предлагает***

забыть про телефонные номера // InternetUA (http://internetua.com/Facebook-predlagaet-zabit-pro-telefonnie-nomera). – 2016. – 9.01).

***

В Facebook никогда не уделяли должного внимания приложениям для настольных платформ. Однажды начав тестирование Facebook Messenger для Windows, компания свернула проект и более к нему не возвращалась. Напротив, мобильный мессенджер весьма популярен, а сравнительно недавно была запущена веб-версия сервиса.

И на днях TechCrunch опубликовал снимок, на котором якобы изображён официальный мессенджер Facebook для Mac. Ресурс отмечает, что MacBook на фото принадлежит одному из сотрудников компании. Снимок получился совсем нечётким, однако даже на нём можно разглядеть некоторые особенности возможного приложения.

В основном внешний вид программы напоминает Facebook Messenger для iOS и содержит аналогичные элементы интерфейса. Вполне возможно, что приложение на снимке является неофициальным клиентом популярного мессенджера.

Однако некоторая особенность программы всё же может служить подтверждением того, что это именно разработка компании Facebook: ни в одном из известных клиентов нет навигационной панели в левом нижнем углу окна. А представленное на фото приложение её содержит.

Впрочем, Facebook частенько тестирует ПО лишь внутри компании, так что даже, если на снимке изображён официальный мессенджер, будет ли он выпущен – неизвестно. Представитель компании отказался «комментировать слухи и спекуляции на эту тему», однако Д. Констин, один из авторов TechCrunch, отметил, что на вопросы об уже вышедших продуктах, в Facebook отвечали точно так же ***(Facebook разрабатывает мессенджер для Mac // InternetUA (http://internetua.com/Facebook-razrabativaet-messendjer-dlya-Mac). – 2016. – 11.01).***

***

Социальная сеть Facebook запустила приложение Mentions для пользователей Android, сообщает издание TechChurch.

Отмечается, что данное приложение доступно только для владельцев верифицированных аккаунтов. Оно предназначено для управления официальными страницами публичных персон. В частности, такие пользователи увидят специальную ленту с постами, в которых они упоминаются, и получат возможность оперативно отвечать своим читателям. Кроме того, с помощью приложения знаменитости смогут проводить онлайн-видеотрансляции ***(Facebook выпустил приложение для знаменитостей на Android // InternetUA (http://internetua.com/Facebook-vipustil-prilojenie-dlya-znamenitostei-na-Android). – 2016. – 13.01).***

***

Twitter планирует предоставить пользователям возможность создавать посты длиной до 10 тыс. символов. Об этом сообщает lenta.ru со ссылкой на портал Re/code.

По их словам, в соцсети рассчитывают реализовать идею до конца I квартала 2016 г. Не исключено, что на первых этапах максимальная длина сообщения будет больше нынешних 140, но меньше 10 тыс. символов – в Twitter эту концепцию на переходный период называют Beyond 140.

Официальных комментариев соцсети порталу получить пока не удалось.

Информация о том, что Twitter собирается изменить ограничения по максимальной длине твитов, появлялась в сентябре прошлого года, однако официального подтверждения так и не нашла ***(Re/code узнал о планах Twitter увеличить размер постов до 10 тысяч символов // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45821/118/lang,ru/). – 2016. – 6.01).***

***

«ВКонтакте» выпустила новую версию приложения для пользователей iPhone. Компания обновила раздел новостей, игр и запустила рекомендации друзей.

В новой версии появился ряд функций. Например, новости теперь появляются автоматически (раньше для этого требовалось обновить ленту). В ленте отображаются рекомендованные друзья – пользователи, с которыми человек может быть знаком. Также появилась возможность перехода по ссылкам и голосования в опросах без необходимости открывать публикацию (дополнительно кликать по ней).

При размещении записи автоматически появляется фрагмент закрепленного в ссылке изображения, а после добавления фотографий к публикации, сообщению или комментарию сервис сохраняет последовательность выбранных изображений.

В игровом разделе каталог приложений теперь разделен по жанрам на категории.

Кроме этого, компания добавила поддержку промопубликаций и рекомендованных приложений ***(«ВКонтакте» масштабно обновила приложение для iPhone // InternetUA (http://internetua.com/vkontakte--masshtabno-obnovila-prilojenie-dlya-iPhone). – 2016. – 8.01).***

***

Twitter обновил официальный клиент для OS X до версии 4.0.0. Этого события владельцы Mac ждали в течение нескольких лет. Новая версия клиента визуально напоминает мобильное приложение.

Среди основных нововведений:

• Поддержка GIF.

• Возможность отправки групповых сообщений (одновременно до 50 пользователей).

• Просмотр видео в потоковом режиме прямо в ленте.

• Возможность исключения отдельных твитов пользователя из своей ленты без отмены подписки на его аккаунт.

• Индивидуализированные темы интерфейса (с выбором более светлого или темного тона).

• Возможность цитирования твитов.

Новую версию клиента уже можно загрузить в Mac App Store ***(Twitter выкатил долгожданное обновление для OS X // InternetUA (http://internetua.com/Twitter-vikatil-dolgojdannoe-obnovlenie-dlya-OS-X). – 2016. – 1.01).***

***

Трансляции из сервиса Periscope наконец стали доступны для просмотра прямо через Twitter. Трансляции теперь встраиваются напрямую в ленту социальной сети, что позволяет просматривать видео без необходимости проходить по каким-либо ссылкам – касается это как прямых трансляций, так и их записей. При этом видеоролики даже можно просматривать в полноэкранном режиме, а загрузка их начинается сразу же после того, как пользователь находит видео в ленте – примерно как в Instagram.

Новая возможность пока доступна только на устройствах на базе iOS, но в конечном итоге встроенные в ленту Twitter трансляции Periscope станут доступны и на Android, а также в веб-версии сервиса. Благодаря такому ходу база пользователей Periscope должна сильно увеличиться. Сервис был приобретен компанией из Сан-Франциско около года назад и с момента своего официального запуска, который состоялся в марте прошлого года, собрал уже более 10 млн пользователей.

Пользователи Periscope записали уже более 100 млн трансляций, заявила компания.

В целом же пользователи Periscope за день просматривают примерно 40 лет видео – напомним, что после завершения прямой трансляции видео остаётся доступно всем желающим ещё 24 часа. В прошлом месяце Apple назвала Periscope лучшим приложением 2015 г. ***(Лента Twitter начала поддержку трансляций Periscope // IGate (http://igate.com.ua/lenta/12632-lenta-twitter-nachala-podderzhku-translyatsij-periscope). – 2016. – 14.01).***

***

Щоб об’єднати всіх україномовних відеоблогерів, у мережі створили організацію YouthTube. Авторами ідеї є закарпатський відеоблогер Д. Яким та тернополянин В. Стрільчук, відомий під псевдонімом Арчі. Про це повідомляє hromadske.lviv.ua

До групи вже приєдналися виконавиця відомих світових хітів, блогер Jerry Heil з Києва та Ю. Кіндрацька з Тернополя.

Молоді учасники розповідають, що метою YouthTube є консолідувати зусилля, щоб створювати якісний розважальний контент українською мовою, який у майбутньому зможе конкурувати з російськомовним YouTube та українськими блогерами, які розмовляють російською.

Кількість учасників спільноти помітно зростає. До групи можна приєднатися усім, хто пов'язує свою діяльність з YouTube і має ентузіазм творити цікаві матеріали українською мовою ***(Україномовні відеоблогери створили платформу YouthTube // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45896/118/lang,ru/). – 2016. – 15.01).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

15 самых популярных аккаунтов политиков в Twitter, The Kiev Times (http://thekievtimes.ua/lifestyle/435330-15-samyx-populyarnyx-akkauntov-politikov-v-twitter.html).

1. Барак Обама, президент США

Аккаунт: @POTUS / @BarackObama

Количество подписчиков: 2,37 млн / 59,4 млн

В Twitter: с мая 2015 г. / с марта 2007 г.

У президента США – целых два аккаунта в Twitter. Официальный появился в 2007 г. 18 мая 2015 г. Б. Обама завел личный аккаунт в Twitter, который получил название @POTUS (President Of the United States – президент Соединенных штатов).

2. Н. Моди, премьер-министр Индии

Аккаунт: @narendramodi

Количество подписчиков: Более 12 млн

В Twitter: с января 2009 г.

Н. Моди – главный популяризатор в Индии социальных сетей в целом и Twitter в частности. Он активно использовал сервис в своей предвыборной кампании и заставил высших индийских чиновников завести собственные аккаунты. Под его влиянием недавно даже президент Индии П. Мукерджи присоединился к Twitter. Н. Моди пишет в свой микроблог, минимум, несколько раз в день.

3. С. Юдойоно, президент Индонезии

Аккаунт: @SBYudhoyono

Количество подписчиков: Более 7 милн

В Twitter: с марта 2013 г.

Отставной генерал С. Юдойоно – первый президент Индонезии, избранный прямым голосованием избирателей. Twitter и социальные сети для политика – эффективный способ поддерживать популярность в народе. Правда, сотрудники аппарата президента ведут его аккаунт на индонезийском языке в крайне официальной манере, но иногда С. Юдойно пишет в Twitter самостоятельно и делится воспоминаниями из своего прошлого.

4. А. Гюль, бывший президент Турции

Аккаунт: @cbabdullahgul

Количество подписчиков: Более 6 млн

В Twitter: с декабря 2009 г.

А. Гюль – активный пользователь Twitter – год назад выступил в роли защитника соцсети в Турции. После того, как премьер-министр страны Р. Эрдоган объявил запрет на Twitter в Турции, А. Гюль, который был тогда президентом, тут же выступил с заявлением, что данный шаг недопустим. Вскоре турецкий суд отменил запрет на Twitter в Турции.

5. Р. Эрдоган, президент Турции

Аккаунт: @RT_Erdogan

Количество подписчиков: Более 6 млн

В Twitter: с августа 2009 г.

Р. Эрдоган недолюбливает социальные сети, и Twitter, в частности, еще со времен волнений на площади Таксим в 2013 г.

Время от времени турецкий политик предпринимает новые атаки на Twitter, сравнивая его со «скальпелем в руках хирурга» и «ножом в руке убийцы». Но вся эта воинствующая риторика не мешает президенту Турции активно вести собственный аккаунт – один их самых популярных в мире.

6. М. Рашид аль-Мактум, премьер-министр и вице-президент ОАЭ

Аккаунт: @HHShkMohd

Количество подписчиков: Более 4 млн

В Twitter: с июня 2009 г.

Один из богатейших монархов мира, шейх М. Рашид аль-Мактум – большой поклонник социальных сетей, образования и технологий.

7. Э. Ньето, президент Мексики

Аккаунт: @EPN

Количество подписчиков: 3,95 млн

В Twitter: с марта 2007 г.

Президент Мексики пишет в Twitter про политику, футбол, театр, культуру и общается с лидерами других стран. Записи в его микроблоге появляются практически ежедневно.

8. Х. Сантос, президент Колумбии

Аккаунт: @JuanManSantos

Количество подписчиков: Более 3,8 млн

В Twitter: с августа 2009 г.

Аккаунт в Twitter бывший министр обороны Колумбии Х. Сантос завел за год до того, как стал президентом страны.

В своем блоге Х. Сантос пишет по несколько раз в день, а также пользуется Periscope – новым приложением Twitter для видеотрансляций.

9. Р. аль-Абдулла, королева Иордании

Аккаунт: @QueenRania

Количество подписчиков: Более 3,7 млн

В Twitter: с апреля 2009 г.

В Twitter королева, как обычная женщина, публикует фотографии семьи, детей, одежды, нарядов и интересных мест из официальных поездок. Иногда в ее микроблоге появляются даже записи про футбол и матчи европейской Лиги Чемпионов.

10. К. Киршнер, президент Аргентины

Аккаунт: @CFKArgentina

Количество подписчиков: Более 3,7 млн

В Twitter: с апреля 2010 г.

К. Киршнер крайне активно ведет свой Twitter. Официальные и эмоциональные записи, фоторепортажи, видеообращения публикуются в ее аккаунте по несколько раз в день.

11. Д. Медведев, премьер-министр России

Аккаунт: @MedvedevRussia

Количество подписчиков: Более 3,7 млн

В Twitter: с июня 2010 г.

Главный популяризатор Twitter в России, который ввел моду на эту социальную сеть среди российских чиновников.

12. Д. Русеф, президент Бразилии

Аккаунт: @dilmabr

Количество подписчиков: Более 3,5 млн

В Twitter: с апреля 2010 г.

Д. Русеф ведет свой блог не так ярко и эмоционально, ее стиль – крайне официальный и лаконичный.

13. Х. Клинтон, госсекретарь США

Аккаунт: @HillaryClinton

Количество подписчиков: Более 3,5 млн

В Twitter: с апреля 2013 г.

Аккаунт Х. Клинтон в Twitter ведут ее сотрудники, но иногда Госсекретарь пишет в него сама. В этом случае ее записи сопровождаются в конце буквой Н.

14. Б. Клинтон, бывший президент США

Аккаунт: @billclinton

Количество подписчиков: Около 3,5 млн

В Twitter: с апреля 2013 г.

15. А. Шварценеггер, бывший губернатор Калифорнии

Аккаунт: @Schwarzenegger

Количество подписчиков: Более 3,3 млн

В Twitter: с января 2008 г.

Свой микроблог А. Шварценеггер ведет в яркой и непосредственной манере. Недавно бывший губернатор Калифорнии объявил в Twitter о своем возвращении в кинематограф, и теперь публикует в микроблоге видео и фото со своих съемок в кино. В настоящее время политических записей в его аккаунте практически нет ***(15 самых популярных аккаунтов политиков в Twitter // The Kiev Times (http://thekievtimes.ua/lifestyle/435330-15-samyx-populyarnyx-akkauntov-politikov-v-twitter.html). – 2016. – 2.01).***

***

Белый дом присоединился к Snapchat, чтобы общаться с миллениалами.

Как отметил директор по управлению продукцией для Белого дома Д. Миллер, платформа поможет сотрудникам взаимодействовать с широкой группой населения новыми и креативными способами» и делиться ежедневными историями с американцами. Канал, который запустил свою первую историю 11 января, показал Овальный кабинет, предложит закулисные снимки и ракурсы, которые больше нигде нельзя будет увидеть. Более 60 % американцев-владельцев смартфонов в возрасте от 13 до 34 лет пользуются Snapchat. Поэтому неудивительно, что Белый дом хочет найти общий язык с некоторыми из 100-миллионной базы платформы ***(Белый дом присоединился к Snapchat, чтобы общаться с миллениалами // Marketing Media Review (http://mmr.ua/show/belyy_dom_prisoedinilsya_k_snapchat__chtoby_obshtatysya_s_millenialami_). – 2016. – 12.01).***

***

Офіційне представництво Головного управління Національної поліції у Волинській області відтепер доступне в соціальних мережах Twitter, Facebook та Instagram.

На сторінках будуть розміщувати останні офіційні новини, фото, відеозвернення та інші тематичні посилання.

Також прес-служба повідомляє, що нині працюють над можливістю подання через Інтернет електронних заяв, повідомлень, запитів. Власне, ідеться про запровадження комплексу сервісних послуг в онлайн, які стосуються компетенції поліції.

У соціальній мережі Facebook є також акаунт керівника волинської поліції П. Шпиги.

Відеоматеріали щодо роботи поліції можна переглянути, підписавшись на офіційний канал YouTube.

Адміністратором публічних сторінок Головного управління Національної поліції у Волинській області є сектор комунікації ***(Відтепер за роботою Нацполіції на Волині можна слідкувати у Twitter, Facebook та Instagram // ВолиньPost (http://www.volynpost.com/news/63470-vidteper-za-robotoyu-nacpolicii-na-volyni-mozhna-slidkuvaty-u-twitter-facebook-ta-instagram). – 2016. – 13.01).***

***

Глава полиции Одесской области Г. Лорткипанидзе объявил о приеме обращений в Facebook. При этом можно обращаться к нему в личных сообщениях – они тоже будут рассмотрены.

На странице главы ГУНП в Одесской области была опубликована информация о том, что полицейские начали бескомпромиссную борьбу с игорными заведениями; уже изъято оборудование нескольких, что подтверждается прикрепленным видео. В связи с этим Г. Лорткипанидзе обратился к своим подписчикам. «Если вы владеете какой-либо информацией о местах незаконного игорного бизнеса, сообщайте пожалуйста в территориальные отделы полиции, а также мне в личные сообщения на Facebook», – говорится в сообщении.

В комментариях к данной записи один из пользователей сообщает, что на сообщения реагируют.

Ранее глава ГУНП писал, что полиция рассматривает все обращения, поступающие из любых источников, однако не акцентировал внимания на соцсетях, тем более на информации, поступающей в «личку» ***(Глава полиции Одесской области Лорткипанидзе объявил о приеме обращений в Facebook // Маяк (http://mayak.org.ua/news/the-chief-of-police-of-odessa-region-lortkipanidze-announced-the-acceptance-of-applications-in-facebook/). – 2016. – 14.01).***

***

Мэр Кременчуга В. Малецкий обсудил с руководителем Службы помощи мэра Ю. Войтенко основные направления работы структурного подразделения с обращениями граждан.

Как известно, недавно в Службу помощи мэра кременчужанам граждане могут обращаться с помощью страницы в Facebook.

По словам Ю. Войтенко, с момента создания страницы в социальной сети в Службу помощи мэра кременчужанам поступило около 30 сообщений. Все заявители получили промежуточный ответ о том, что их обращение взято на контроль.

Примечательно, что на сообщения, которые не требуют дополнительного изучения (отсутствие горячего или холодного водоснабжения, ремонт электрических сетей и т. д.), специалисты Службы помощи мэра кременчужанам отвечают сразу.

В. Малецкий отметил, что работу в этом направлении необходимо продолжать, а также «расширяться» благодаря другим соцсетям.

Также В. Малецкий поставил перед Ю. Войтенко задачу регистрировать обращения и по возможности информировать кременчужан о проделанной работе путем фотофиксации факта. Он уверен, что через несколько недель службе удастся перейти на оперативное реагирование с использованием всех возможностей, которые есть в социальных сетях для обмена информацией.

Отметим, что на странице службы можно сообщать об аварийных отключениях, проблемах ЖКХ, благоустройства и транспорта. Сообщения граждан будут зарегистрированы, как обращения, оперативно отработаны и приняты соответствующие меры по их решению.

В сообщении необходимо указать:

– фамилию, имя, отчество;

– адрес, по которому вы проживаете;

– номер телефона;

– информацию о жалобе ***(Больше 30-ти человек уже обратились в Службу помощи мэра кременчужанам 15-63 через Фейсбук // Кременчуг Today (http://kremen.today/2016/01/05/v-sluzhbu-pomoshhi-mera-cherez-facebook-obratilos-okolo-30-kremenchuzhan/). – 2016. – 5.01).***

***

КП «Харьковский метрополитен» зарегистрировало официальный аккаунт в приложении Instagram.

«В нашем аккаунте будут публиковаться интересные фотографии, снятые с необычных ракурсов, с деталями, которые пассажиры обычно не замечают. Также будем показывать места, куда доступа, как правило, нет, и работу метро изнутри», – сообщили на предприятии.

Напомним, что КП «Харьковский метрополитен» помимо официального сайта также имеет верифицированную страницу «ВКонтакте» ***(У Харьковского метрополитена появился аккаунт в «Instagram» // Сайт Харьковского городского совета (http://www.city.kharkov.ua/ru/news/-30492.html). – 2016. – 6.01).***

***

Нова патрульна поліція Закарпаття зареєструвала власний акаунт у популярному сервісі для розміщення фотографій та коротких відеороликів Instagram.

На офіційній сторінці патрульної служби Закарпаття в Instagram, крім фотографій з присяги, можна знайти знімки з місця роботи, є навіть селфі вартових правопорядку. Наразі сторінка в Instagram має кількох підписників.

Наостанок залишається відзначити, що всі публікації позначено відповідним хештегом #transcarpathianpolice #новаполіція #Ужгород #Мукачево ***(У закарпатської поліції з'явився аккаунт в Instagram // Transkarpathian news (http://transkarpathianews.net/social/21171-u-zakarpatskoyi-polcyi-zyavivsya-akkaunt-v-instagram-foto.html). – 2016. – 5.01).***

***

Facebook-література в Україні: чому й навіщо

Відомі блогери Б. Логвиненко («Перехожі»), С. Іванов, М. Воскало («Кокс Квасневського») та поетеса й літредактор К. Хаддад-Розкладай

обговорили один з феноменів українського Facebook – публікацію там літературних творів, які нерідко таким чином знаходять свого видавця.

Учасники розмови зібралися обговорити цікаве й поширене в українському інтернет-сегменті явище: присутність у Facebook літературних творів, частина з яких потім виходить друком. Популярність такого формату зумовлена тим, що українські користувачі цієї соцмережі, зокрема громадські активісти, журналісти, письменники, використовують її не лише для приватного спілкування й інформування про своє життя, а і як інтелектуальний майданчик.

Як результат – українські видавництва запропонували читачам уже кілька книг, в основу яких лягли пости з Facebook. Це збірки двох українських журналісток: З. Казанжі («Якби я була») та Х. Бердинських («Є люди»), декілька книг-хронік про події Революції гідності, книгу блогерки О. Степової про Донбас. І це лише кілька прикладів.

Що таке Facebook-література

Новим явищам в інтернет-сфері не завжди легко дати визначення. Філолог за освітою, К. Хаддад-Розкладай пропонує говорити про літературу у Facebook у контексті трьох складових:

– тексти, які вперше були опубліковані в соціальній мережі, а потім вийшли друком;

– публікацію у Facebook раніше виданих творів із метою промотування;

– тексти, що існують тільки в Інтернеті.

«Все це має право на існування й існує в Україні. Але публікація на папері переводить будь-який текст в інший вимір», – зазначила поетеса.

І якщо під час дискусії йшлося насамперед про першу з названих категорій, слід зазначити, що піар-менеджери сучасних великих українських видавництв активно використовують соціальні мережі (як Facebook, так і «ВКонтакте») для реклами власних видань, а молоді поети й прозаїки публікують свої твори як на особистих сторінках, так і в спеціалізованих спільнотах соцмереж чи на сайтах, прагнучи, вочевидь, знайти якщо не видавця, то читача.

…Б. Логвиненко звернув увагу й на те, що величезна кількість розгорнутих текстів у Facebook – це особливість саме України. «Для громадян більшості інших країн Facebook – це як “Одноклассники”. Списалися, познайомилися, пішли в кіно. В Україні це щось більше, це інтелектуальна платформа. Тому те, що в нас відбувається, – це справді феномен», – зазначив блогер, який кілька років працював журналістом.

Однією з причин, на його думку, є засміченість медіа-простору. «Більшість ЗМІ в нас є політичними, а не інформаційними проектами. Медіа не виконують освітньої функції. З багатьох видань позникала тематика культури, історії, подорожей, а людям час від часу це все ще потрібно. Мало й глибокої аналітики. Тому все це з’являється у відкритому просторі, спочатку це сталося в LiveJornal, тепер у Facebook», – вважає Б. Логвиненко.

Крім того, на його думку, поява масиву інтелектуального контенту в соціальній мережі обумовлена й тим, що впродовж десятиліть радянського часу в Україні були доступні тільки засоби пропаганди. «Тому й були самвидави, якісь альтернативні платформи, щоб дізнаватися інформацію. Роль самвидавів зараз відіграють соцмережі. Також у нас немає культури платити за тексти. За книги ще платять, а за друковані ЗМІ – ні», – додав він ***(Толокольнікова К. Facebook-література в Україні: чому й навіщо // MediaSapiens (http://osvita.mediasapiens.ua/web/social/facebookliteratura_v_ukraini_chomu_y_navischo/). – 2016. – 15.01).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Юристи, бухгалтери, аналітики, експерти з телекомунікацій і цифрових технологій виділили 10 технотрендів, які підприємцям не варто випускати з уваги в цьому році.

1. Несподівані аспекти у сфері кібершахрайства, наприклад, використання підроблених документів.
2. Поширення Інтернету і розвиток Інтернету речей.
3. Аналіз великих обсягів даних в режимі реального часу замінить інтуїцію у прийнятті складних рішень.
4. З'являться нові закони про захист персональних даних.
5. Однотипні завдання будуть виконувати роботи і штучний інтелект.
6. Смартфони стануть основним інструментом для виконання безлічі завдань.
7. З'являться бізнес-додатки для віртуальної реальності.
8. Реклама стане більш персоналізованою і заснованою на місцезнаходженні клієнта.
9. Дрони зможуть доставляти товари і брати участь у соціально значущих проектах.
10. Традиційний бізнес буде відчувати тиск з боку стартапів ***(10 техно-трендів, які впливають на бізнес в 2016 // Finance.ua (http://news.finance.ua/ua/news/-/367093/10-tehno-trendiv-yaki-vplyvayut-na-biznes-v-2016). – 2016. – 16.01).***

***

В Twitter появился новый формат объявлений – Conversational Ads, совмещающий опросы и пользовательские хештеги. Задача СА повысить вовлеченность пользователей в контент и простимулировать их делиться твитами с друзьями. Об этом пишет likeni.ru.

С помощью Conversational Ads бренды смогут создавать опросы с двумя ответами на выбор, включающими пользовательские хештеги и картинки или видео.

После клика по объявлению пользователи получают благодарственное сообщение от бренда на месте CTA-кнопок. По задумке разрботчиков, это должно замотивировать пользователя расшарить персонализированный твит у себя в ленте.

В ближайшие несколько месяцев формат будет тестироваться на западных рынках ***(Twitter запустил новый формат объявлений Conversational Ads // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45827/118/lang,ru/). – 2016. – 6.01).***

***

Twitter позволит использовать твиты пользователей в рекламе. Бренды смогут собирать сообщения, связанные с их продукцией, и затем интегрировать данный контент в свои промокампании, сообщает adindex.ru.

Новый сервис был представлен на Международной выставке потребительской электроники в Лав-Вегасе. Новинка построена на том, что Twitter называет «галерея брендированных твитов», в которой будут собираться твиты, связанные с компаниями, из нее уже рекламодатели смогут выбрать нужные для себя. Затем Twitter будет спрашивать разрешение от имени бренда на использование сообщения, пишет Digiday.

Многие бренды используют звезд для промотирования своих продуктов. Идея же данного сервиса в том, что мнение обычных «неоплаченных» пользователей может быть гораздо полезнее для бренда. Им охотнее будут доверять, считает источник издания.

Также на выставке Twitter представил видеосервис, который позволит превратить любую длинную рекламу в короткое видео, больше подходящее для сервиса ***(Twitter позволит использовать твиты пользователей в рекламе // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45850/118/lang,ru/). – 2016. – 12.01).***

***

Компания Nanigans, которая работает в области автоматизации рекламы, опубликовала отчёт о мировых трендах рекламы в Facebook за IV квартал 2015 г. Об этом пишет searchengines.ru.

В отчётном периоде расходы на рекламу в Facebook возросли на 11 % по сравнению с предыдущим кварталом. В Q3 2015 эта цифра составляла 16 %.

По данным компании, маркетологи продолжают увеличивать бюджеты на Facebook. Причём это справедливо для всех категорий бизнеса. Большинство клиентов рекламной платформы Nanigans в течение последних двух месяцев увеличило свои расходы на этот канал.

В сравнении квартал к кварталу, в Q4 2015 онлайн-ритейлеры наблюдали значительный рост ключевых метрик дохода по Facebook: покупок – на 68 %; средней цены заказа – на 49 %; ROI – 87 %.

Расходы на видеорекламу в Facebook возросли на 41 % по сравнению с Q3 2015; на мобильное видео – на 44 %. Среди зарубежных рекламодателей (за пределами США) – на 86 % и 94 % соответственно.

Расходы на динамические товарные объявления возросли на 210 % по сравнению с предыдущим кварталом, на объявления в формате карусели – на 34 % ***(Расходы на видеорекламу в Facebook выросли на 41 % в Q4 2015 // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45893/118/lang,ru/). – 2016. – 15.01).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

На основе данных соцсетей Facebook и Twitter можно получить точный портрет личности человека. К такому выводу пришла журналистка издания NPR А. Шахани, передает ain.ua.

А. Шахани использовала в эксперименте суперкомпьютер IBM Watson, которому дала доступ в свои аккаунты в соцсетях.

Характер А. Шахани искусственный интеллект анализировал по словам, которые она использует в своих текстах, общему тону сообщений и прочим данным из соцсетей.

В итоге получилась диаграмма с указанием основных особенностей характера журналистки. Оказалось, что больше всего у А. Шахани проявляется вызов общепризнанным авторитетам, и она скорее интроверт, чем экстраверт.

А. Шахани не ожидала столь точной оценки ее личности на основании данных из ее Facebook и Twitter. Ее поведение в разных соцсетях сильно отличатся. «В Facebook я – это я, а в Twitter я превращаюсь в придирчивую всезнайку. Я думала, система даст разные оценки моей личности по разным аккаунтам, но оценка практически одинакова. Удивительно», – заявила А. Шахани.

Технология, которая использовалась в эксперименте, была разработана для использования в сфере маркетинга. Отмечается также, что сервис анализа личности не доступен для обычных пользователей ***(Касьяненко С. По Facebook и Twitter программа может составить психологический портрет //***

Podrobnosti.ua (http://podrobnosti.ua/2083456-po-facebook-i-twitter-programma-mozhet-sostavit-psihologicheskij-portret.html). – 2016. – 12.01).

***

Интерфейс чата Facebook принципиально влияет на восприятие ваших сообщений

Ш. Жандар, дизайнер и фронтенд-разработчик с опытом психолога, обнаружила, что ее подруга очень резко отреагировала на безобидное сообщение в Facebook. Удивившись такому поведению, Ш. Жандар поняла, что дело может быть в интерфейсе чата Facebook и решила провести небольшое исследование на эту тему. Результат показал, что интерфейс, который вы выбираете при переписке, может принципиально отразиться на восприятии ваших сообщений, пишет AIN.UA (http://ain.ua/2016/01/14/626629).

Учитывая то, что интерфейс может влиять на отображение сообщения, Ш. Жандар задалась вопросом: «А будут ли люди по-разному реагировать на одного и то же сообщение, показанное в разных интерфейсах?».

Ш. Жандар написала одинаковые сообщения и поместила в три формы, каждая из которых отображалась в разных интерфейсах. Напечатано оно было одинаково. Использовались окно чата в Facebook (Chat), полноформатное окно диалогов в Facebook (Full Conversation) и простой текст без ничего (Control) («контрольное» исследование).

В каждой форме был обозначен ряд характеристик, по которым можно было оценить сообщение: отчаяние, уверенность, смелость, неловкость, мужественность и женственность.

При сравнении ответов по характеристикам получились интересные результаты: если сообщение появлялось во всплывающем окне чата Facebook, люди находили автора текста более безрассудным, неловким и менее уверенным в себе, чем при использовании полноформатного окна диалогов. Причем значительно.

В реальной жизни мы больше полагаемся на физические и вербальные атрибуты, вроде языка тела, которые демонстрируют социальные навыки и дополняют смысл сказанного. В Интернете мы пользуемся другими индикаторами, вроде количества сообщений или их длины. Слишком много сообщений или их избыточная длина могут изменить порядок сил и сделать беседу неловкой и не сбалансированной.

Давайте взглянем на интерфейс всплывающего чата Facebook, учитывая вышесказанное. Каждое сообщение имеет свои границы, подчеркивающие их количество. Из-за небольшой ширины окна чата, сообщения занимают несколько строчек в высоту, перекрывая собой почти все окно.

Каков визуальный результат? В окне чата, сообщения выглядят больше и массивнее, нежели в других интерфейсах. А поскольку у читателя нет никакой связи с тем, кто пишет, кроме этих сообщений, он будет судить его, основываясь исключительно на этой переписке.

Несмотря на то что автор ни в чем не виноват, он будет выглядеть более дискредитированным, менее уверенным в себе, более неловким и отчаянным, чем в другой ситуации. Это не говорит о том, что использование чата Facebook – социальный суицид для автора, однако это значительно трансформирует реакцию адресата.

Идем дальше. Мы уже знаем, что шрифты и расположение текста влияют на его восприятие: «средство передачи является сообщением», шрифту Baskerville доверяют больше, чем Comic Sans, печатные эссе получают другие оценки, чем написанные вручную и т. д. Но в данном контексте происходит нечто особенно интересное.

Данный интерфейс играет специальную роль: он выступает социальным медиатором. Это касается и адресата и того, что кто пишет. Интерфейс становится частью цифрового языка тела. А это большой пласт возможностей и ответственности. И, как показывает это исследование, социальные сети могут нас объединять, а интерфейсы – отдалять друг от друга ***(Интерфейс чата Facebook принципиально влияет на восприятие ваших сообщений, и вот почему // AIN.UA (http://ain.ua/2016/01/14/626629). – 2016. – 14.01).***

Маніпулятивні технології

У зоні АТО фіксуються масові спроби терористів поширювати серед місцевого населення дезінформацію про завдання й наміри командування бойовиків, окремих підрозділів і формувань

Про це на своїй сторінці у Facebook повідомив координатор групи «Інформаційний спротив», народний депутат Д. Тимчук, передає Еспресо.TV.

«Розпускаються чутки про прибуття на ту чи іншу ділянку фронту відомих ватажків бойовиків. Серед бойовиків і представників місцевого населення ведеться робота щодо користування соцмережами, обмеження користування засобами зв'язку», – зазначив Д. Тимчук.

За даними групи «Інформаційний спротив», незаконні збройні формування поширюють дезінформацію серед мешканців населених пунктів у районі Маріуполя про підготовку «зачисток» серед мирного населення з боку бійців «Азову» ***(Бойовики забороняють мешканцям Донбасу користуватися соцмережами і телефоном // Espreso.tv (http://espreso.tv/news/2015/12/30/boyovyky_zaboronyayut_miscevym_zhytelyam_korystuvatysya_socmerezhamy_i_telefonom). – 2015. – 30.12).***

***

Топові українські акаунти в соцмережі Twitter піддалися масовим блокуванням.

Під санкції потрапили, зокрема, @Dbnmjr (Новости Украины) з 500 тисячами підписчиків, @TukvaSociopat, @xyevii_kharkov, @banderenko, @ReggaeMortis1, @SPaWN_ua (Капітан Прайс), @canabina (Євгеній

Коноплянка), @UKROPSTEEL, @psb4ukr (центр «Миротворець»), @olegnovikovkh, @CatDemokrat, @bloodypastor (Кровавий пастор), @forest_brothert (Лісовий брат), @PV_Petrychenko (Паша Петриченко), @kozakmamai (Ukrainian Forces), @persident_ukr (Перзидент України) і багато інших.

Хвиля блокування почалася після того, як Twitter посилив правила безпеки, за якими можна припиняти дію акаунта за найменші порушення. Після цього проросійські боти прийнялися вишукувати в постах українських користувачів некоректні цитати і скаржитися на них. Причому в хід часто йдуть старі твіти – річної давності і більше.

На ситуацію вже відреагував навіть посол України у Фінляндії А. Олефіров, який є активним користувачем Twitter. Він оприлюднив звернення до техпідтримки компанії з проханням звернути увагу на блокування українських акаунтів. Посол також пропонує робити скріншоти, які дають змогу довести зловмисний характер банів від російських тролів.

«Це надасть доказову базу для посольства України в США для звернення до керівників офісу [Twitter]. Ми перемогли колу і пепсі, бо там був очевидний доказ», – зазначив А. Олефір ***(Twitter масово банить топові українські акаунти // LB.ua (http://ukr.lb.ua/news/2016/01/08/325148_twitter_masovo_banit_topovi.html). – 2016. – 8.01).***

***

Группа «Информационное сопротивление – юг» зафиксировала появление в Интернете нового «информационного вируса», связанного с Одессой.

Об этом сообщил координатор «ИС» С. Братчук. По его словам, «в социальных сетях читателям украинского сегмента предлагают активно включиться в обсуждение темы «что делал Одесский десант» (сохранена стилистика авторов) на территории Молдовы в начале 90-х годов прошлого века, в ходе вооруженного конфликта, завершившегося созданием – с помощью России – квазигосударства Приднестровская Молдавская Республика». Аналитики «ИС» предполагают, что таким образом нагнетается истерия в связи с укреплением совместного украинско-молдавского противодействия агрессии Кремля.

«Приднестровью отводилась отдельная роль в проекте «Русская весна». Проект «Новороссия» должен был обеспечить сухопутный мост между Крымом, Донбассом и Приднестровьем, устанавливая тотальный контроль Москвы над северным побережьем Черного моря и делая Украину нежизнеспособной без морских портов. Именно российский контингент в Приднестровье должен был открыть второй фронт при наступлении на Одессу», – подчеркнул С. Братчук. Он отметил: «О каком “одесском десанте” начала 90-х может идти речь, сложно догадаться даже самому сведущему в военно-политических делах эксперту».

В «ИС» уверены, что приднестровская тема будет играть не последнюю роль в информационном давлении Кремля на южные регионы Украины ***(«Одесский десант»: новый «информационный вирус» // ВІКНА-ОДЕСА (http://viknaodessa.od.ua/news/?news=127627). – 2016. – 11.01).***

***

Боевики так называемого «Исламского государства» массово возвращаются в мессенджер Telegram, шифрующий сообщения пользователей. Его разработчик – П. Дуров – подвергся резкой критике со стороны представителей служб безопасности после терактов в Париже, унесших жизни 130 человек. По информации правоохранительных органов, джихадисты пользуются защищенным сервисом Telegram в планировании своих нападений.

П. Дуров неоднократно отказывался блокировать пользователей-членов ИГИЛ и других джихадистских группировок. Однако после нападений в Париже он нехотя заблокировал 78 аккаунтов, связанных с исламистами, пишет Inosmi.

Сервис обмена сообщениями Telegram, запущенный в сентябре 2014 г., позволяет рассылать сообщения неограниченному числу подписчиков и предоставляет защищенное киберпространство для частной и групповой переписки. За последние несколько недель боевики «ИГ» и другие джихадисты вернулись в Telegram еще в большем количестве, чем ранее, чтобы вербовать новых участников джихада и распространять пропаганду. Специалисты разведывательных служб опасаются, что джихадисты могут организовывать и планировать нападения в чатах, которые остаются невидимыми, и расшифровать которые почти невозможно.

По словам С. Сталински – главы вашингтонской мониторинговой группы MEMRI, исследующей деятельность джихадистов в сети, Telegram потенциально может превзойти Twitter по популярности среди боевиков «Аль-Кайды» и «Исламского государства».

«Также за последние несколько дней Талибан впервые создал несколько аккаунтов в Telegram», – отмечает он.

Американские и европейские специалисты по вопросам безопасности сообщают, что несмотря на тот факт, что у них нет окончательных доказательств того, что террористы, организовавшие атаки в Париже, пользовались технологиями шифрования, в условиях, когда их главари находятся в Сирии, группе было необходимо создать защищенный канал для передачи информации.

Как отмечает глава MEMRI, популярность и трафик Telegram «просто огромны». «С октября прошлого года мы сосредоточили внимание на использовании Telegram джихадистами, и до парижских терактов мы увидели беспрецедентный рост числа пользователей приложения, – говорит С. Сталински. – Это было самое большое развитие в кибер-джихада с момента, когда исламисты начали активно обмениваться информацией в Twitter два года назад. На П. Дурова было оказано давление, и он нехотя забанил несколько

аккаунтов, однако сейчас все эти люди вернулись – и еще в большем числе. Они прибывают. Каждый день. Это сумасшествие – прошлой ночью мы видели, как в одном “канале” за ночь появились более десяти тысяч чатов».

Пользователям так называемых «каналов» Telegram, позволяющих посылать сообщения большой аудитории, предоставляется возможность сохранять относительную анонимность. Канал показывает только общее число подписчиков его другим пользователям – без разглашения настоящих имен. Списки подписчиков и тех, на кого они подписаны, доступны всем, как в Twitter, что делает возможной перекрестную проверку «про-игиловских» аккаунтов и тех, кто подписан на них.

Пользователи Telegram также могут перенаправлять контент одного канала другим пользователям сервиса, облегчая распространение джихадистского контента, включающего, в частности, инструкции по изготовлению бомб и призывы к осуществлению атак «террористов-одиночек».

Связь с каналом в Telegram – односторонняя: подписчики не могут отсылать свой контент тому, кто ведет канал. Это блокирует возможность – в отличие от Twitter – перекрестной беседы, которой пользуются западные власти для борьбы с пропагандой экстремизма.

Помимо каналов, пользователи Telegram могут создавать частные и групповые чаты с численностью до тысячи человек. Telegram также предлагает Secret Chats – возможность зашифрованного обмена информацией с обеих сторон, не оставляющей следа на серверах Telegram благодаря встроенному коду самоуничтожения подобных сообщений.

Американские и европейские чиновники неоднократно озвучивали недовольство тем, что разработчики таких технологий де-факто помогают террористам и подстрекают к подобной преступной деятельности.

Ведущие специалисты «Силиконовой долины» заявляют, что они обеспокоены возможными нарушениями приватности – комплекса прав на тайну переписки, защиту личной информации и других гражданских свобод, – а приоритетом для них остается защита интересов их пользователей, а не национальной безопасности. Эти настроения только усилились после того, как экс-сотрудник Агентства национальной безопасности Э. Сноуден разгласил подробности программ электронной слежки в США.

Тем временем, ИГИЛ и другие джихадисты все реже сталкиваются с трудностями в вопросах коммуникации, вербовки и планирования атак. В сервисе Telegram исламисты «ИГ» ведут сразу несколько каналов, распространяющих контент таких медиа-групп, как Nashir, Fursan Al-Raf и Al-Battar. Группа, именующая себя «Союзниками «Исламского государства», на аватаре которой помещено изображение лидера «ИГ» Абу Бакра аль-Багдади, появилась 17 декабря, и уже через 48 часов насчитывала 500 подписчиков ***(Боевики ИГ массово переходят на Telegram // InternetUA (http://internetua.com/boeviki-ig-massovo-perehodyat-na-Telegram). – 2016. – 11.01).***

***

В ИГИЛ разработали собственный секретный мессенджер для Android, сообщает The Next Web. Приложение называется The Alwari, именно его террористы используют для общения друг с другом. В СМИ информация поступила от хакеров из Ghost Security Group, которые занимаются борьбой с терроризмом.

После того как другая хакерская группа – Anonymous – объявила ИГИЛ войну, террористам пришлось отказаться от использования Telegram, Facebook, WhatsApp и других ранее популярных среди них площадок для общения.

По данным издания, система безопасности The Alwari не дотягивает до Telegram, но позволяет преступникам общаться, не рискуя быть рассекреченными. Приложение не размещено в Google Play, чтобы его найти, пользователю придется «рыться в темных участках сети» ***(В ИГИЛ создали собственный мессенджер // InternetUA (http://internetua.com/v-iqil-sozdali-sobstvennii-messendjer). – 2016. – 15.01).***

***

Роберт ван Ворен: Чому я не видаляю пропутінських тролів у Facebook

«Серед п’яти тисяч моїх друзів у Facebook багато росіян. Деякі з них дотримуються пропутінських поглядів, і це, звісно, додає нового специфічного присмаку слову “друг”. Деякі з них порядні люди, просто наші погляди кардинально відрізняються. Зрештою, у цьому світі є безліч тих, чиї погляди, скажімо, “шкідливі для мого здоров’я”.

Серед згаданих прихильників Путіна є і сотні тролів, що належать до інтернет-армії кремлівської пропаганди. Чому я не видаляю їх зі списку друзів? Тому що для мене вони є ідеальним індикатором того, що можна чекати від Путіна далі.

Найчастіше діям передує пропагандистська кампанія в соціальних медіа або, навпаки, пропагандистська кампанія проводиться після того, як якісь задуми Кремля провалилися, щоб пояснити нам, чому ми повинні розцінювати невдачу, як успіх. Завдяки цьому я можу “відчути”, коли в Східній Україні плануються якісь військові дії, або коли нова затія Кремля не призвела до бажаних результатів (тоді вони починають “пояснювати” це російськомовній аудиторії).

Для мене Facebook став соціально-політичним барометром і з плином часу він лише підтвердив свою ефективність.

Ще з новорічної ночі, я помітив, що росіяни взялись активно поширювати певні відео – відео з іммігрантами (“біженцями”), які ходять групами десь вулицями Західної Європи і влаштовують там пекло. Супроводжуючі коментарі, зазвичай, варіюються від “чого не показують у ЗМІ” до “тварини, яких ми самі впустили”. Використовується принизлива лексика, націлена на розпалювання ненависті та створення відчуття фрустрації.

Я ще можу зрозуміти стурбованих німців, голландців, бельгійців, які публікують такі пости через свої страхи та побоювання. Але чому відео про іммігрантів у Європі публікують росіяни?

…Я можу повірити, що троє або четверо опублікували це просто тому, що відео привернуло їхню увагу, і вони не замислювалися над його змістом. Я навіть можу повірити, що деякі росіяни автоматично не люблять людей, які мають іншим колір шкіри або належать до “іншої” культури, особливо з урахуванням того факту, що Росія – зовсім не найтолерантніша країна у світі.

Але чому подібні пости поширюють сотні росіян і, зазвичай, супроводжують їх однаковими коментарями?

Я намагаюся не вірити в казки і не піддаватися параноїдальним теоріям змови, проте в цьому разі дійсно вважаю, що ми маємо справу з новою конструкцією кремлівської пропаганди. Після масивного потоку антиукраїнської пропаганди (коли цілу країну перетворюють на жидобандерівських фашистів) ми стаємо свідками антиіммігрантської пропагандистської кампанії, спрямованої на підрив європейської єдності та розпалювання напруженості, особливо в тих країнах, які впродовж останніх двох років активно підтримували Україну, де люди бачили справжнє обличчя Путіна.

Я не кажу, що вся іммігрантська криза є витівками російської пропаганди, і не заперечую, що європейська ідентичність переживає важкі часи. До нинішньої ситуації призвело безліч факторів – надто складних і великих, щоб обговорювати їх тут. Я лише кажу, що хтось активно, цілеспрямовано і в організованому порядку підкидає хмизу в огонь для розпалювання напруженості.

Сьогодні ми дійсно переживаємо найбільший виклик світу і безпеці в Європі з часів закінчення Другої світової війни. І у нас є не один Гаврило Принцип, який убив у 1914 році ерцгерцога Франца Фердинанда і, тим самим, розв’язав найбільш руйнівну війну в історії людства, яка, за фактом, тривала 31 рік і закінчилася лише в 1945-му. Ні, зараз у нас є ціла армія “Гаврил Принципів”, які всі разом убивають Європейський Дім. І хтось у цей момент сидить і насолоджується видовищем, як його Facebook та інші Принципи роблять свою руйнівну справу» ***(Роберт ван Ворен: Чому я не видаляю пропутінських тролів в Facebook // InfoKava.com (http://infokava.com/lang-uk/34656-pochemu-ya-ne-udalyayu-proputinskih-trolley-v-facebook-robert-van-voren.html). – 2016. – 6.01).***

***

Израильская неправительственная организация «Шурат а-Дин» поставила своеобразный эксперимент, призванный продемонстрировать тенденциозную политику, проводимую администрацией социальной сети Facebook.

В один и тот же день члены этой организации создали и опубликовали две страницы, антипалестинскую и антиизраильскую, и выложили их в

Facebook, после чего обратились к администраторам сети с требованием убрать обе – как провоцирующие этническую ненависть и разжигающую насилие.

В результате этой жалобы страница, содержащая негативную информацию в отношении палестинцев, была немедленно закрыта, в то время как антисемитская, по утверждению авторов эксперимента, продолжает открываться и набирать просмотры.

Вечером во вторник, 5 января, радиостанция «Решет Бет» сообщила о том, что «Шурат а-Дин» подала в нью-йоркский суд иск, в котором обвиняет руководство Facebook в необъективности, антиизраильской направленности и потакательстве исламским радикалистам, беспрепятственно вербующих сторонников с помощью этой сети ***(«Шурат а-Дин» подала иск в суд Нью-Йорка: эксперимент доказал антисемитизм Facebook // NEWSru.co.il (http://www.newsru.co.il/world/05jan2016/shurat456.html). – 2016. – 5.01).***

***

В наличии фальшивых профилей в социальных сетях нет ничего нового. Их есть десятки миллионов, потому что это отличный бизнес, позволяющий зарабатывать немалые деньги на продаже фанатов. В последнее время такими фальшивыми профилями кишит Instagram, и большинство из них касается услуг для взрослых.

Специалисты с Symanteca зарегистрировали истинное нашествие поддельных профилей в Instagram, одной из самых популярных социальных сетей, которая имеет уже более 400 млн пользователей и используется в основном для размещения фотографий. В последнее время там появились, кажется, что сотни, если не тысячи фальшивых профилей, которые спамьят пользователей, пытаясь побудить их подписаться на сайтах знакомств, а также посетить сайты для взрослых. Таким образом, продвигают также ювелирные услуги, техническую поддержку для различных продуктов и многое другое, в том числе страницы, содержащие вредоносные программы.

Это похоже на скоординированную акцию, а ее вдохновители зарабатывают деньги на аффилиационных программах, а также заражая пользователей вредоносными программами.

С. Наранг, один из специалистов Symanteca, утверждает, что поддельные профили сосредоточены вокруг трех основных моделей. Первый тип включает в себя только список фотографий, краткое описание и ссылку на внешнюю страницу. Второй тип профиля – это много фотографий, всегда украденных с других профилей или веб-страниц, в то время как третий тип ориентирован исключительно на рекламу и содержит одно большое изображение. Поддельные профили не только рекламируют различные услуги, но также используются для рассылки спама.

Symantec предупреждает пользователей Instagram не кликать ни на какие ссылки размещены на фальшивых профилях и не входить во взаимодействие с такими «владельцами», поскольку их компьютеры могут быть заражены вредоносными программами ***(Толубяк И. Instagram наводнен фальшивыми***

профилями // Prostotech (http://prostotech.com/internet/2414-instagram-navodnen-falshivymi-profilyami.html). – 2016. – 12.01).

Зарубіжні спецслужби і технології «соціального контролю»

Правительство Китая одобрило новый антитеррористический закон, который ранее называли спорным и противоречивым. Пока в сенате США идут жаркие дебаты о том, стоит ли заставлять производителей и поставщиков услуг устанавливать бекдоры в свои продукты, в КНР решили проблему прослушки немного иначе.

Постоянный комитет Всекитайского собрания народных представителей – высшего законодательного органа КНР, окончательно одобрил документ, направленный на борьбу с терроризмом. Китай, разумеется, тревожится не из-за недавних терактов в Европе. Дело в том, что внутри страны растет угроза со стороны сепаратистов и силовиков, а в районе Синьцзян за последние годы погибли сотни людей.

Так как защищенные средства связи в наши дни стали считаться опасной штукой, новый антитеррористический закон обязывает все компании, работающие на территории КНР, по первому требованию передавать ключи шифрования от своих продуктов представителям китайских правоохранительных органов. При этом власти Китая уверяют, что данная мера – совсем не аналог установки бекдоров в продукты компаний, и страна не делает ничего такого, что не было бы уже применено в западных странах.

С этим заявлением, однако, не согласны в Вашингтоне. Американцы убеждены, что новый закон, в сочетании с нововведениями в банковском и страховом секторах Китая, это ни что иначе, как способ избирательного давления на зарубежные компании. На Западе вообще полагают, что новый закон может нарушить право на свободу слова и права человека.

Впрочем, с некоторыми компаниями у КНР явно возникнут проблемы. К примеру, компания Apple никак не сможет предоставить правоохранительным органам Китая ключи шифрования от iMessage. Ведь приложение было специально создано таким образом, что даже сама Apple не имеет ключей в своем распоряжении и не может «вскрыть» собственный мессенджер ***(Китай обяжет компании предоставлять ключи шифрования властям // InternetUA (http://internetua.com/kitai-obyajet-kompanii-predostavlyat-kluacsi-shifrovaniya-vlastyam). – 2015. – 29.12).***

***

Служба безопасности Украины (СБУ) задержала работника одной из райгосадминистраций Донецкой области, который создал сепаратистское сообщество в одной из социальных сетей.

Как сообщает пресс-служба СБУ, участники группы распространяли материалы, которые дискредитировали украинскую власть и призывали к вхождению освобожденных от сепаратистов территорий Донецкой области в состав т. н. ДНР.

«Также сеть использовалась для передачи террористам информации о дислокации и перемещении украинских подразделений», – говорится в сообщении.

В настоящее время продолжаются неотложные оперативно-следственные действия ***(СБУ задержала администратора сепаратистского сообщества // InternetUA (http://internetua.com/sbu-zaderjala-administratora-separatistskogo-soobsxestva). – 2016. – 9.01).***

***

Иностранные соцсети должны выполнять определённые условия для того, чтобы продолжать работать на территории России, сообщил в эфире «Русской службы новостей» (РСН) советник президента РФ по Интернету Г. Клименко. Об этом пишет rusnovosti.ru.

«Если они [соцсети. – РСН] будут сотрудничать с правоохранительными органами. Если они будут вести себя так же, как и отечественные, если у них будут те же права и обязанности. Не просто права, но и обязанности», – сказал Г. Клименко.

11 января стало известно, что Роскомнадзор пообещал проверить «ВКонтакте». Также ведомство разберется, как выполняют требования о хранении персональных данных «Microsoft Россия», «Озон», Samsung и Hewlett-Packard ***(Иностранные соцсети в России обяжут сотрудничать с правоохранительными органами // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45855/118/lang,ru/). – 2016. – 12.01).***

***

Государственная дума России окончательно одобрила законопроект, согласно которому вводятся тюремные сроки за публичные призывы к экстремизму с помощью Интернета, а также за финансирование экстремистской деятельности. За экстремизм в сети теперь можно угодить в тюрьму на пять лет, за финансовую помощь экстремистам суд имеет право наказывать шестью годами заключения, передает ИТАР-ТАСС. Поводом для уголовной статьи может стать репост или лайк провокационных записей в Интернете.

Депутаты Госдумы одобрили поправки в третьем, окончательном чтении. Отныне в Уголовный кодекс вводится новая статья, устанавливающая наказание за «предоставление или сбор средств либо оказание финансовых услуг, заведомо предназначенных для финансирования организации, подготовки и совершения хотя бы одного из преступлений экстремистской направленности либо для обеспечения деятельности экстремистского сообщества или экстремистской организации».

За финансирование группировок экстремистской направленности предполагаются: штрафы от 300 тыс. до 500 тыс. р.; лишение права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет; обязательные работы на срок до 200 часов; исправительные работы на срок от одного года до двух лет; лишение свободы на срок до трех лет. Если преступление будет совершено с использованием служебного положения, максимальное наказание составит шесть лет тюрьмы.

Что касается Интернета, то меры по контролю за пользовательским контентом снова ужесточились. Отныне распространение в сети экстремистской информации – уголовно-наказуемая деятельность, при этом, судя по последним событиям, достаточно поставить лайк или сделать репост какого-либо подобного материала.

Так, наказание за публичные призывы к экстремизму в Интернете – принудительные работы или лишение свободы до пяти лет. Аналогичным образом дополняется и известная статья 282 («Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства») – под нее теперь также будут подпадать соответствующие преступления, совершенные в информационном пространстве, например, в сети.

Также в МВД РФ разработали стратегию противодействия экстремизму в России до 2025 г. Ее цель – на фоне сохранения силовой составляющей борьбы с экстремистскими проявлениями «кардинально повысить эффективность противодействия радикальной идеологии, поставить надежные барьеры на путях ее проникновения в общественное сознание». Основной акцент в документе сделан на информационном подавлении «экстремистов». Для этого предложено вести мониторинг СМИ и Интернета и разработать новые способы «ограничения доступа» к вредной информации.

Стоит подчеркнуть, что принятый Госдумой закон, скорее всего, облегчит правоохранителям доказательство вины в таких случаях, как с оппозиционером Д. Бычковым, которого обвинили в призывах к терроризму за перепост картинки с пулями и комментарий в социальной сети «ВКонтакте». В Барнауле в настоящее время начинается процесс по этому делу, сообщает портал «ОВД-Инфо» ***(Госдума России одобрила закон о тюремных сроках за лайки и репосты в интернете // InternetUA (http://internetua.com/gosduma-rossii-odobrila-zakon-o-tuaremnih-srokah-za-laiki-i-reposti-v-internete). – 2016. – 14.01).***

***

Около 40 % приемных комиссий, которые занимаются зачислением в американские колледжи, проверяют профили Instagram или Facebook абитуриентов. Об этом пишет gazeta.ru.

Отмечается, что по сравнению с исследованиями, которые были проведены в 2008 г., эта цифра увеличилась в четыре раза. Тем не менее, большинство респондентов (89 %), которые непосредственно занимаются

отбором кандидатов на зачисление, утверждают, что прибегают к проверке соцсетей очень редко и на индивидуальной основе.

Чаще всего профили абитуриентов в соцсетях интересуют приемную комиссию в том случае, если необходимо получить более полную информацию об интересах или о творческой составляющей. Кроме того, с помощью профиля в Instagram или Facebook можно узнать как о необычных и заслуживающих внимания наградах подростка, так и его поведении или причастности к нелегальным занятиям.

При этом треть участников опроса добавили, что чаще всего такие проверки выявляют неутешительные результаты – большинство информации на личных страницах носит скорее негативный характер и плохо отражается на решении о зачислении подростка в колледж ***(40 % колледжей США мониторят Facebook и Instagram своих абитуриентов // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45878/118/lang,ru). – 2016. – 14.01).***

***

Исследователи Пенсильванского университета, США, разработали алгоритмическую платформу для целевой слежки за пользователями сети. Об этом сообщается в журнале Proceedings of the National Academy of Sciences. По словам ученых, алгоритм позволит с высокой точностью обнаруживать деятельность террористов в Интернете, в то же время защищая конфиденциальность обычных пользователей.

Поводом для создания технологии стали сведения о массовом слежении американских спецслужб за всеми пользователями сети Интернет. Исследователи надеются создать инструмент, позволяющий сохранить баланс между обеспечением национальной безопасности и защитой прав человека.

Исследователи предлагают ввести четкую классификацию пользователей Интернета и поделить их на группы. К примеру, в контексте борьбы с терроризмом предлагается создать три группы пользователей: подозреваемые в террористической деятельности, информаторы и лица, не связанные с терроризмом. «Алгоритмы позволят сформировать список из подтвержденных целей, обнаруженных в сети, принятие мер в отношении которых не повлияет на защиту конфиденциальности прочих пользователей», – сообщается в публикации.

Алгоритмы ученых основаны на теории графов – раздела дискретной математики, изучающего свойства непустого множества вершин и связей между таковыми. Каждый пользователь представлен в виде отдельного графа, связанного вершинами с определенными группами. Поиск потенциальных террористов и оптимизация результатов выдачи будет осуществляться с помощью так называемой статистики близости – определения соотношения графов с конкретными группами.

В ходе пробного сканирования социальных сетей с созданием случайно сгенерированных искусственных целевых групп ученым удалось создать сеть,

состоящую из подтвержденных целей. При этом конфиденциальность пользователей из других групп была сохранена в полном объеме ***(Разработан механизм целевого слежения за пользователями сети // InternetUA (http://internetua.com/razrabotan-mehanizm-celevogo-slejeniya-za-polzovatelyami-seti). – 2016. – 15.01).***

***

Египетская полиция арестовала двух человек, в совокупности управлявших 47 сообществами в Facebook. Об этом сообщает Reuters.

Согласно заявлению властей, они задержали двоих: 26-летнего мужчину, в чьем ведении находилось 41 сообщество, и 22-летнюю администратора шести сообществ. В вину обоим вменяется пропаганда идей происламской организации «Братья-мусульмане» и подстрекательство против власти.

Аресты произвели в преддверии пятой годовщины революции в стране.

2 января стало известно об аресте в Египте администраторов 22 оппозиционных сообществ ***(Египетские власти арестовали администраторов 47 Facebook-сообществ // InternetUA (http://internetua.com/egipetskie-vlasti-arestovali-administratorov-47-Facebook-soobsxestv). – 2016. – 14.01).***

***

Глава подразделения Twitter в Европе Б. Дэйсли рассказал, что сервис предоставляет своим 320 млн пользователей новые инструменты для защиты от интернет-троллей. В частности, сервис призывает делиться списками заблокированных онлайн-хулиганов с другими пользователями.

«Над обеспечением безопасности наших пользователей мы работаем больше, чем над чем-либо другим», – заявил Б. Дэйсли Independent.

Также, по его словам, в число мер входит телефонная верификация аккаунтов, на которые поступило много жалоб, и их владельцам затем напоминают, что то, чем они занимаются, происходит в реальном, а не виртуальном мире, поэтому последствия этого тоже реальны.

Б. Дэйсли заверил, что эти меры уже дали хороший результат: в уходящем году количество троллинга в Twitter заметно уменьшилось, и пользователи стали чувствовать себя намного безопаснее ***(Twitter отчитался об успехах борьбы с пользователями-троллями // InternetUA (http://internetua.com/Twitter-otcsitalsya-ob-uspehah-borbi-s-polzovatelyami-trollyami). – 2015. – 30.12).***

***

Власти Индонезии заблокировали не менее 11 экстремистских веб-сайтов, а также несколько аккаунтов в социальных сетях после терактов, происшедших 14 января в столице страны Джакарте, передает Reuters.

По их данным, были обнаружены несколько аккаунтов в социальной сети Facebook, выражающих поддержку проведенных атак.

«Мы следим за многими веб-сайтами и жалобами населения относительно них», – сказал представитель министерства связи Индонезии И. Кавиду.

По его словам, правительство также направило письма в Facebook, Twitter и Telegram с просьбой немедленно блокировать или удалять все экстремистские материалы ***(Более 10 экстремистских сайтов заблокировали в Индонезии после атак в столице страны // InternetUA (http://internetua.com/bolee-10-ekstremistskih-saitov-zablokirovali-v-indonezii-posle-atak-v-stolice-strani). – 2016. – 16.01).***

Проблема захисту даних. DDOS та вірусні атаки

Итальянская компания VoidSec, работающая в сфере информационной безопасности, опубликовала материал о недавно обнаруженном ботнете из маршрутизаторов Aethra. Как выяснилось, злоумышленники использовали данный ботнет для осуществления брутфорс-атак на сайты под управлением WordPress.

Одна из атак была обнаружена специалистом VoidSec во время проверки личного веб-сайта WordPress в феврале нынешнего (2015. – Ред.) года. Как показал анализ, атака осуществлялась с IP-адресов, относящихся к шести интернет-провайдерам: Fastweb, Albacom (BT-Italia), Clouditalia, Qcom, WIND, BSI Assurance UK. Большая часть данных компаний устанавливает клиентам маршрутизаторы Aethra (BG1242W, BG8542W и пр.).

В данном случае значительная часть маршрутизаторов использовала установленные по умолчанию логин/пароль, благодаря чему злоумышленники смогли взломать девайсы и внедрить вредоносное ПО. Как отметили эксперты, некоторые устройства также подвержены XSS- и CSRF-уязвимостям, позволяющим преступнику получить доступ к устройству даже в случае использования различных логинов.

При помощи поисковой системы Shodan экспертам VoidSec удалось обнаружить более 12 тыс. маршрутизаторов Aethra по всему миру. Большая часть устройств расположена в Италии – 10 866 девайсов. В брутфорс-атаках было задействовано 8 тыс. маршрутизаторов. В настоящее время порядка 70 % устройств работают с настройками по умолчанию. По оценкам специалистов, каждый инфицированный маршрутизатор способен осуществлять DDoS-атаки в диапазоне от 1,7 до 17 Гб/с.

Специалисты связались с Fastweb и BT-Italia – крупнейшими итальянскими провайдерами, чьи маршрутизаторы были задействованы в брутфорс-атаках. Fastweb отреагировала оперативно, всего за неделю выпустив корректирующее обновление прошивки. Провайдер BT-Italia признал наличие проблемы, однако за 11 месяцев так и не устранил уязвимость ***(Ботнет из 12 тыс. маршрутизаторов Aethra использовался для атак на Wordpress-сайты***

// InternetUA (http://internetua.com/botnet-iz-12-tis--marshrutizatorov-Aethra-ispolzovalsya-dlya-atak-na-Wordpress-saiti). – 2015. – 29.12).

***

Независимый эксперт в области компьютерной безопасности К. Викери из города Остин в штате Техас выявил базу данных на 191 млн избирателей из США, передает Daily Mail.

По его словам, данный источник информации был обнаружен случайно и ее владелец остается неизвестным. В настоящее время он вместе с властями США работает над установлением его личности.

По словам К. Викери, основное беспокойство у него вызвал тот факт, что «информация носит такой концентрированный характер» ***(В сети обнаружили базу данных на 191 млн американских избирателей // InternetUA (http://internetua.com/v-seti-obnarujili-bazu-dannih-na-191-mln-amerikanskih-izbiratelei). – 2015. – 28.12).***

***

Активисты выразили свой протест против введения цензуры в Интернете, взломав сайт Телекоммуникационного сообщества стран Азиатско-Тихоокеанского региона.

Группировка Anonymous получила доступ к административному интерфейсу сайта под управлением Drupal и осуществили дефейс главной страницы. Дефейс – тип хакерской атаки, при которой страница веб-сайта заменяется другой, чаще всего содержащей рекламу, угрозы или вызывающие предупреждения, страницей. Взломщики также похитили и опубликовали в Интернете хранящуюся на ресурсе конфиденциальную информацию.

Как заявил один из взломщиков в эксклюзивном интервью HackRead, причиной атаки стал протест против введения цензуры Интернета в странах Азии. При осуществлении атаки активистам Anonymous помогали хакеры из других группировок ***(Anonymous взломали сайт Телекоммуникационного сообщества стран Азиатско-Тихоокеанского региона // IGate (http://iqate.com.ua/lenta/12340-anonymous-vzlomali-sajt-telekommunikatsionnogo-soobshhestva-stran-aziatsko-tihookeanskogo-regiona). – 2015. – 29.12).***

***

В турецких СМИ появились сообщения о массированных атаках группы интернет-активистов, которым подверглись порядка 40 тыс. сайтов по всей стране. Несколько банков, включая Isbank, Garanti и государственный Ziraat Bank, подтвердили, что подверглись кибератакам, ставшим причиной временных сбоев в операциях с кредитными картами.

«Атаки серьезные, – говорит представитель интернет-провайдера Turk Telekom O. Оз. – Но их мишень не Turk Telekom. Крупной атаке подверглись банки и государственные институты». «Эти атаки начались две недели назад,

но участились в последние два дня», – сообщил Б. Атакани, специалист по компьютерным сетям в Стамбульском техническом университете. А. Аджар, ректор Ближневосточного технического университета ÜÇIDT Турции, управляющего доменами с расширением tr, назвал кибератаки на зарегистрированные в Турции веб-сайты одними из самых массированных в истории.

«Мы получили информацию о том, что против некоторых банков были совершены кибератаки. На сайт нашего министерства систематических атак не было, но мы приняли необходимые меры. Турция не останется беспомощной перед лицом таких атак. Проводится расследование, ответ будет дан», – заявил глава министерства торговли и таможни Турции Б. Тюфенкчи журналистам в пятницу.

Отметим, что группа хакеров Anonymous объявила о запуске крупномасштабной кампании по кибервойне против турецкого правительства, предупредив, что если Турция не прекратит поддерживать террористическую группировку «Исламское государство», ее участники продолжат атаки на турецкие интернет-ресурсы, серверы, банки, аэропорты и военные объекты ***(Хакеры нанесли удар по турецким интернет-ресурсам и банковским системам // IGate (http://igate.com.ua/lenta/12326-hakery-nanesli-udar-po-turetskim-internet-resursam-i-bankovskim-sistemam). – 2015. – 28.12).***

***

Группа хакеров Ayyıldız из Турции сообщила о взломе сайта хакеров Anonymous и о подготовке кибератак на российские сайты, передает Aksam.

По данным издания, на сайте Anonymous накануне появилась надпись «Вы атакованы киберармией Ayyıldız », турецкий флаг и изображение основателя Турецкой Республики М. Ататюрка.

Лидер группы хакеров Д. Яфес заявил, что тем самым они «преподали урок тем, кто хочет оскорбить турецкое государство», и пообещал, что следующей целью атак станет Россия ***(Турецкие хакеры взломали сайт Anonymous и готовят атаки на российские сайты // InternetUA (http://internetua.com/tureckie-hakeri-vzlomali-sait-Anonymous-i-gotovyat-ataki-na-rossiiskie-saiti). – 2015. – 29.12).***

***

Турецкие хакеры из группы Börteçine Siber Tim взломали сайт Посольства России в Израиле. Об этом они сообщили в своем Twitter.

На сохранившейся в кэше Google версии страницы видно, что хакеры разместили там флаг Турции и надписи на турецком языке. ***(Турецкие хакеры взломали сайт посольства России в Израиле // InternetUA (http://internetua.com/tureckie-hakeri-vzlomali-sait-posolstva-rossii-v-izraile). – 2016. – 17.01).***

***

Немецкие ИБ-специалисты К. Нол и Ф. Браунлейн обнаружили новую уязвимость в расположенных в Германии платежных терминалах, позволяющую злоумышленникам похитить PIN-код и информацию магнитных полос кредитных и дебетовых карт.

Эксперты протестировали платежные терминалы от пяти крупных операторов платежных систем. Устройства использовали две сети с одинаковым программным обеспечением.

В рамках доклада на Всемирном конгрессе хакеров К. Нол и Ф. Браунлейн намерены продемонстрировать примеры нескольких атак с эксплуатацией ошибок в платежных протоколах ZVT и Poseidon, используемых терминалами. По словам К. Нола, протокол ZVT используют порядка 90 % устройств, поэтому уязвимость затрагивает подавляющее большинство терминалов.

Проэксплуатировав ошибки в протоколе ZVT атакующий может получить PIN-код кредитной карты жертвы, а также всю информацию, содержащуюся на магнитной ленте. Как оказалось, любой платежный терминал, предоставленный операторами, использует для подписи сообщений один и тот же ключ.

Атака происходит следующим образом: злоумышленник отправляет на терминал имитирующее легитимное сообщение с просьбой ввести PIN-код, ждет, пока жертва не начнет транзакцию, а затем отправляет вредоносные команды. В результате, атакующий становится обладателем PIN-кода и данных магнитной полосы кредитной карты.

«Раньше мошенники использовали уязвимости в программном обеспечении. Для устранения проблем требовалось просто загрузить обновление. Мы взламываем сам протокол, то есть устройство работает в нормальном режиме, но при этом остается уязвимым. В результате данную проблему нельзя решить с помощью патча – придется перенастраивать всю систему», – пояснил К. Нол в интервью изданию Motherboard.

«Те, кто несет ответственность за пробелы в безопасности, в том числе банки, признают существование проблемы, однако принимать меры для ее решения не спешат. Они говорят, что подобных случаев мошенничества пока не зафиксировано – но ведь это лишь вопрос времени! Своим бездействием они только усугубляют ситуацию», – подчеркнул специалист ***(Уязвимость в протоколах PoS-терминалов приводит к хищению данных кредитных карт // InternetUA (http://internetua.com/uyazvimost-v-protokolah-PoS-terminalov-privodit-k-hisxeniua-dannih-kreditnih-kart). – 2015. – 29.12).***

***

В середине декабря SecurityLab писал о критической уязвимости в одной из самых распространенных систем управления контентом Joomla!. Проэксплуатировав проблему, удаленный пользователь может выполнить произвольный PHP-код на целевой системе с привилегиями веб-сервера.

Уязвимость распространяется на версии Joomla! с 1.5 по 3.4.5 включительно. Производитель уже успел выпустить исправление безопасности. Тем не менее, злоумышленники продолжают активно атаковать сайты, использующие неисправленные версии Joomla!. По данным экспертов ИБ-компании Symantec, ежедневно на уязвимые ресурсы осуществляется более 16 тыс. атак.

Эксплуатация ошибки в Joomla! позволяет преступникам скомпрометировать серверы и использовать их для хостинга вредоносного ПО или осуществления иной деятельности, в том числе перенаправления жертв на сайты, содержащие наборы эксплоитов. Помимо прочего, преступники могут продавать доступ к серверам на подпольных рынках.

По словам специалистов Symantec, злоумышленники пытаются определить уязвимые серверы путем отправки специально сформированного HTTP-запроса. Обнаружив подходящий сервер, хакеры устанавливают бэкдор, позволяющий выполнять команды, загружать файлы и модифицировать веб-сайты, расположенные на сервере ***(Злоумышленники активно атакуют уязвимые серверы Joomla! // InternetUA (http://internetua.com/zloumishlenniki-aktivno-atakuuat-uyazvimie-serveri-Joomla). – 2015. – 30.12).***

***

Пользователи телекоммуникационного приложения Skype на платформе Windows недавно обнаружили в нём неисправность, которая мешает вести переписку, меняя правильный порядок отображения сообщений. Обсуждения на форуме техподдержки Microsoft говорят, что пользователи последней версии программы видят самое свежее сообщение выше отправленных ранее пользователями из их списков контактов. Такое поведение приложения наблюдается у некоторых пользователей на протяжении уже нескольких недель.

В Microsoft сообщают, что знают о существовании проблемы, и до её решения рекомендуют установить предыдущую версию Skype. Неисправной является версия 7.17.0.105, хотя проблема наблюдается далеко не у всех её обладателей. Пока Microsoft не говорит, когда будет представлена обновлённая версия Skype.

В версиях Skype для других платформ, таких как Mac OS X, Linux, Android и iOS, никаких проблем не наблюдается. Также можно использовать веб-версию Skype, Skype в Outlook.com и плагин Skype Click to Call ***(В Skype на Windows обнаружен баг // InternetUA (http://internetua.com/v-Skype-na-Windows-obnarujen-bag). – 2015. – 30.12).***

***

Член команды Google Project Zero Т. Орманди обнаружил опасный баг в расширении AVG Web TuneUp для браузера Chrome. Компания AVG называет пользователям установку AVG Web TuneUp во время инсталляции собственного антивируса. Воспользовавшись уязвимостью, найденной

Т. Орманди, злоумышленники могут получить доступ к истории браузера, файлам cookie и так далее.

В своем баг-репорте Т. Орманди пишет, что расширение AVG Web TuneUp установлено на компьютерах 9 млн пользователей Chrome. При этом продукт AVG уязвим перед XSS (cross-site scripting) атаками.

«Данное расширение добавляет в Chrome несколько JavaScript API, видимо, чтобы иметь возможность «подправить» настройки поиска и новой вкладки, – объясняет Т. Орманди. – Процесс инсталляции запутанный, так как AVG приходится обходить защиту официального Chrome Web Store от вредоносного ПО, которая как раз должна предотвращать попытки нецелевого использования API расширений».

В ходе своих изысканий Т. Орманди выявил, что многие добавленные в браузер JavaScript API написаны из рук вон плохо, содержат баги и могут использоваться хакерами для получения доступа к личным данным пользователей.

Теоретически, XSS-уязвимость в расширении AVG может применяться злоумышленниками для получения данных с аккаунтов таких сервисов как Gmail, Yahoo, а также банковских сайтов.

Т. Орманди пишет, что HTTPS в данном случае не спасает, так как расширение «отключает SSL».

Разработчики AVG уже устранили проблему, выпустив AVG Web TuneUp 4.2.5.169. Однако из-за данного инцидента компания Google заблокировала возможность потоковой инсталляции этого расширения. То есть пользователям, которые захотят установить AVG Web TuneUp, придется зайти в Chrome Web Store и установить расширение вручную.

В отношении компании AVG проводится расследование, так как в Google подозревают, что производитель антивирусных решений умышленно нарушил правила Chrome Web Store ***(AVG навязывает пользователям небезопасное расширение для Chrome // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/12/29/avg-web-tuneup-xss.html). – 2015. – 29.12).***

***

«Исламское государство» расширяет свое влияние в Интернете и уже предпринимает попытки совершить кибератаки на американские компьютеры, отвечающие за регулирование электросетей, пишет газета Politico со ссылкой на заявления официальных лиц США.

Чиновники утверждают, что пока попытки ИГ не увенчались успехом. Тем не менее, на своих форумах сторонники террористической группировки выкладывают фотографии и видеоролики из кабин самолетов и обсуждают, как при помощи взлома бортовой электроники можно вызвать крушение воздушного судна.

«У них мало возможностей, потому мы и наблюдаем эти атаки, которые происходят на низких уровнях. Но это совершенно не значит, что таким

образом они не будут продвигаться вперед. Несомненно, они работают над развитием этих навыков», – сказал аналитик А. Кассайрер, занимающийся мониторингом террористических сайтов.

Издание подчеркивает, что США ежегодно тратят 5 млрд дол. на обеспечение кибербезопасности, однако их системы по-прежнему уязвимы. По мнению автора статьи, в последнее время боевики ИГ начинают осознавать, что проще ударить по США при помощи «цифрового оружия», чем добраться до границ страны ***(Хакеры ИГ готовят кибератаки на США // InternetUA (http://internetua.com/hakeri-ig-gotovyat-kiberataki-na-ssha). – 2015. – 30.12).***

***

Відключення електроенергії в Україні в грудні 2015 р. було викликано кібератакою.

Такого висновку дійшли фахівці дослідницького центру SANS ICS, передає Deutsche Welle.

Згідно з аналізом SANS ICS, атака хакерів на електростанцію Прикарпаттяобленерго була ретельно спланована і складалася з кількох рівнів. Зокрема, зловмисникам вдалося встановити шкідливу програму в систему управління компанії, а потім віддалено вимкнути подачу електроживлення.

Повідомляється, що хакери позбавили українських диспетчерів доступу до систем управління і блокували телефонні дзвінки споживачів, які пробували повідомити про неполадки.

Відключення електрики було результатом «прямого вторгнення противника, а не тільки роботи шкідливих програм», підкреслюється в опублікованому звіті.

За даними SANS ICS, це перший підтверджений випадок кібератаки на електростанцію, який призвів до перебоїв у її роботі.

Раніше НВ повідомляло, що в грудні 2015 р. проти українських компаній – постачальників електроенергії була скоєна низка кібератак, які були спрямовані на виведення підприємств з ладу.

Прикарпаттяобленерго була єдиною компанією, яка заявила про збої в роботі, однак подібні шкідливі програми були виявлені в мережах ще як мінімум двох інших підприємств.

Спецслужби США підозрюють російських хакерів в атаці на українську енергомережу ***(Збій в енергосистемі України був викликаний кібератакою – SANS ICS // InternetUA (http://internetua.com/zb-i-v-energosistem--ukra-ni-buv-viklikanii-k-beratakoua---SANS-ICS). – 2016. – 10.01).***

***

Джерела «Інформаційного Спротиву» повідомили, що 9 січня відбулася потужна атака на український сегмент в Інтернеті, після чого багато Facebook-сторінок заблокували. Користувачі скаржились на зависання сторінок і повільне оновлення даних, повідомляє «Інформаційний Спротив».

Користувачі розповіли, що зловмисники розсилали повідомлення з їхніх сторінок. Крім того, у мережі створювалися клони зламаних сторінок з ідентичними даними, з яких також розсилаються фейкові повідомлення і запити на додавання друзів. Після відновлення сторінок продовжували з'являтися нові повідомлення.

Після новорічних канікул Facebook очікувала атак на сторінки своїх користувачів. Про джерела загроз не повідомлялось, але адміністрація соцмережі повідомила, що додала у своє меню кнопку повідомлення про злам або підозрілу активність акаунту ***(«Інформаційний Спротив» : Хакери масово зламують українські акаунти у Facebook // Телекритика (http://www.telekritika.ua/internet/2016-01-11/112923). – 2016. – 11.01).***

***

Twitter-акаунт постійного представника України в ООН Ю. Сергєєва зламали хакери. Про це повідомляє Український тиждень з посиланням на департамент політики і комунікацій МЗС України.

«Акаунт постійного представника України про ООН Ю. Сергєєва @Yuriy_Sergeyev зламано», – ідеться в повідомленні.

Раніше офіційну сторінку Адміністрації Президента України у Twitter зламали невідомі ***(Хакери зламали Twitter постійного представника України в ООН // Телекритика (http://www.telekritika.ua/internet/2016-01-11/112922). – 2016. – 11.01).***

***

Специалисты Emsisoft обнаружили новый вид вымогательского ПО, работающего на основе JavaScript. Об этом сообщается в блоге компании. Вредонос Ransom32 позволяет заблокировать работу системы и зашифровать персональные данные пользователей. Для восстановления доступа к информации жертва должна выплатить вымогателям выкуп через Bitcoin.

На первый взгляд Ransom32 практически не отличается от другого вымогательского ПО. Использовать вредонос для вымогательства может любой злоумышленник, имеющий Bitcoin-кошелек. Для обработки данных о регистрациях используется скрытый сервер в анонимной сети Tor.

Введя адрес Bitcoin-кошелька, злоумышленник получит доступ к административному интерфейсу. На специальной странице преступник может настроить параметры вымогательского ПО – например, отображаемые вредоносом сообщения, тип шифруемых файлов и сумму выкупа.

Вредонос поставляется в качестве самораспаковывающегося архива WinRAR размером в 22 Мб. При запуске содержимое архива копируется в папку с временными файлами пользователя и происходит открытие вредоноса.

Вымогательское ПО использует для запуска фреймворк NW.js, позволяющий создавать десктопные приложения с помощью JavaScript и HTML. Вредонос пытается имитировать браузер Chrome – исполняемый файл выглядит как почти идеальная копия интернет-обозревателя.

При запуске вымогательское ПО прописывается в автозагрузке и запускает встроенный клиент Tor. Впоследствии Ransom32 соединяется с C&C-сервером по порту 85, шифрует файлы пользователя и отображает сообщение о необходимости выплаты выкупа. …В качестве алгоритма шифрования используется AES с 128-битным ключом в режиме CTR. Для каждого файла используется отдельный ключ ***(Обнаружено первое в мире вымогательское ПО на JavaScript // InternetUA (http://internetua.com/obnarujeno-pervoe-v-mire-vimogatelskoe-po-na-JavaScript). – 2016. – 10.01).***

***

Уязвимость в телевизорах Panasonic, Philips, Sharp и других марок позволяет злоумышленникам устанавливать вредоносные приложения без ведома пользователя.

Уязвимость в телевизорах

Умные телевизоры Panasonic, Philips, Sharp и нескольких других менее известных марок, работающих под управлением Android, содержат уязвимость, которая позволяет злоумышленникам получать полный контроль над устройством без ведома пользователя. Об этом сообщили исследователи из компании Trend Micro.

Уязвимости присвоен номер CVE-2014-7911. Она содержится в Android начиная с версии Cupcake 1.5 и заканчивая Kitkat 4.4W.2. Операционная система Android используется для организации функции «умный телевизор», позволяющей подключаться к интернету и запускать приложения.

Производители телевизоров не уделяют обновлению прошивок такого внимания, как производители смартфонов. Поэтому в большинстве телеприемников стоят устаревшие версии Android, содержащие уязвимость, подчеркнули исследователи.

Помимо телевизоров, проблема касается некоторых телеприставок, в которых тоже присутствует Android.

Заражение и повышение привилегий

Для того чтобы взломать телевизор, злоумышленники направляют пользователей на сайты с вредоносными приложениями, предназначенными якобы для просмотра телеканалов, транслируемых в других странах.

Вот некоторые из адресов с такими приложениями – htvmarket.com, wak2p.com, waks2.com. Все они ведут на серверы, размещенные в США и Канаде.

Загружаемые приложения заражены троянами, которые поселяются в системе и позволяют злоумышленникам поднять при получить корневой доступ к системе. Исследователи обнаружили как минимум один из таких троянов – AndroidOS_RootsTV.A ***(Найден троян, поражающий телевизоры Panasonic, Philips и Sharp // InternetUA (http://internetua.com/naiden-troyan--porajauasxii-televizori-Panasonic--Philips-i-Sharp). – 2016. – 12.01).***

***

Как хакеры взламывают Smart TV

Check Point Software, специализирующаяся исключительно на информационной безопасности, опубликовала отчет о найденных уязвимостях в безопасности сети при использовании EZCast.

EZCast – это ТВ-стример в виде флеш-устройства с разъемом HDMI, который превращает обычные телевизоры в Smart TV. Согласно результатам исследования, хакеры могут получать полный несанкционированный доступ к домашней сети пользователя EZCast, что ставит под угрозу конфиденциальность личной информации и управление домашними устройствами.

Устройство EZCast, которым пользуются порядка 5 млн человек, работает с собственной WiFi-сетью и управляется со смартфона или ПК. Это решение является представителем поколения устройств, подключенных к сети и объединенных в концепцию «Интернета вещей» (Internet of Things, IoT). «Интернет вещей» создает уникальные вызовы безопасности как для потребителей, так и для компаний. Последнее исследование Check Point позволило выделить следующие риски использования EZCast:

· Злоумышленники получают доступ к системе WiFi и могут взломать не только EZCast, но и домашние сети.

· Проникнув внутрь, хакеры способны незаметно перемещаться по сети, получая возможность просматривать конфиденциальную информацию и заражать домашние устройства.

· Атаки можно инициированы удаленно; хакер может активировать вредоносный код, находясь где угодно.

«Наше исследование дает представление о том, что станет нормой в 2016 г. и далее – киберпреступники будут использовать новые творческие способы использования уязвимостей в подключенном к интернету мире, – говорит О. Вануну, менеджер группы исследований по безопасности Check Point. – “Интернет вещей” продолжит развиваться, поэтому и потребителям, и предприятиям важно задуматься над тем, как защитить свои “умные” устройства и приготовиться к более глубокому распространению технологий IoT».

«Интернет вещей» включает широкий спектр самых разнообразных устройств: от простых потребительских гаджетов до автомобилей и сложных промышленных систем. Флеш-носитель EZCast – пример IoT-устройства, так как он позволяет передавать данные по сети без необходимости взаимодействия на уровне «человек-человек» и «человек-компьютер». Рынок устройств IoT растет в геометрической прогрессии, он изменит не только способ взаимодействия всех предприятий, правительственных учреждений и потребителей с окружающим миром, но также способы обеспечения их безопасности ***(Как хакеры взламывают Smart TV // ITnews (http://itnews.com.ua/news/79590-kak-khakery-vzlamyvayut-smart-tv). – 2016. – 13.01).***

***

Исследователи из Arbor Networks обнаружили вредоносную кампанию, направленную против азиатских правительственных и общественных организаций. Согласно экспертам, хакерская группировка Group 27 из Восточной Азии получает удаленный доступ к системам жертв с помощью нового, пока еще редко встречающегося трояна Trochilus (произносится «трокилас»).

В прошлом году исследователи из Arbor Networks и других компаний зафиксировали атаки на сайты правительств стран Азии с использованием вредоносного ПО PlugX и EvilGrab и передали полученные данные региональной Компьютерной группе реагирования на чрезвычайные ситуации (CERT). Дополнительное ПО было обнаружено и удалено с инфицированных сайтов. Как оказалось, некоторые программы принадлежали семейству RAT под названием Trochilus.

В общей сложности был обнаружен целый кластер из семи вредоносных программ, названный исследователями Seven Pointed Dagger (дословно «Кинжал с семью клинками»). ПО обладало обширным функционалом и могло использоваться для шпионажа – инфицируя систему, трояны перемещались по внутренней сети в поисках стратегических целей. Одним из «клинков» кластера оказался Trochilus.

По словам экспертов, обнаруженный образец обладал стандартным набором функций RAT и способностью полностью или почти полностью обходить обнаружение антивирусными продуктами. Trochilus – весьма редкая программа, обнаруженная пока только в кластере с троянами PlugX, 9002 и EvilGrab ***(Обнаружен редкий троян, практически невидимый для антивирусных систем // IGate (http://igate.com.ua/lenta/12614-obnaruzhen-redkij-troyan-prakticheski-nevidimyj-dlya-antivirusnyh-sistem). – 2016. – 13.01).***

***

В наступившем 2016 г. «вирусописатели» уже успели преподнести пользователям Linux неприятный сюрприз, выпустив в свет новую версию троянца-шифровальщика для данной операционной системы. Специалисты антивирусной компании «Доктор Веб», которые исследовали образец энкодера, получившего название Linux.Encoder.3, в свою очередь решили поделиться с пользователями любопытной информацией об особенностях зловреда. Ведь как водится: предупрежден, значит, вооружён!

Как и более старые версии Linux.Encoder, модифицированный троянец проникает в домашнюю папку веб-сайтов с помощью шелл-скрипта, внедряемого злоумышленниками в различные системы управления контентом, в которых имеются неустановленные уязвимости. Для зашифровки всех файлов в домашней директории сайта Linux.Encoder.3 не требуются привилегии суперпользователя Linux – достаточно того, чтобы троянец запустился с правами веб-сервера.

Ещё одна особенность Linux.Encoder.3 заключается в том, что он способен запоминать дату создания и изменения исходного файла и подменять её для модифицированных им файлов значениями, которые были установлены до вмешательства. Вдобавок каждый экземпляр вредоноса использует уникальный ключ шифрования, генерируемый случайным образом на основе характеристик шифруемых файлов. Вместе с тем Linux.Encoder.3 имеет ряд архитектурных особенностей, которые позволяют специалистам успешно расшифровывать повреждённые файлы ***(На Linux свирепствует новая модификация известного троянца-шифровальщика // InternetUA (http://internetua.com/na-Linux-svirepstvuet-novaya-modifikaciya-izvestnogo-troyanca-shifrovalsxika). – 2016. – 15.01).***

***

Эксперты компании Akamai Technologies сообщили о вредоносной кампании, в ходе которой злоумышленники используют SQL-инъекцию для повышения рейтинга интернет-ресурса с публикациями о неверности и изменах.

По словам специалистов, преступники эксплуатируют на целевых веб-сайтах уязвимости, позволяющие выполнение SQL-кода, и внедряют поддельный веб-контент в базу данных. В случае успешной атаки сайт начнет распространять скрытые ссылки на HTML-страницы. Данные ссылки будут индексироваться поисковыми роботами, в конечном итоге повышая рейтинг ресурса злоумышленников в поисковой системе.

По данным экспертов, в III квартале 2015 г. мошенники подобным образом атаковали свыше 3,8 тыс. интернет-ресурсов. В ходе атак преступники также модифицировали результаты поисковой выдачи. К примеру, при поиске по ключевым словам «неверность» и «измена» на первой странице поисковых результатов появлялась ссылка на принадлежащий хакерам сайт.

По словам старшего вице-президента Akamai Technologies С. Шолли, манипулирование рейтингом интернет-страниц – отличный бизнес для злоумышленников. Успешные атаки могут существенно повлиять на прибыль и, самое главное, на репутацию многих компаний и организаций, использующих Интернет для продвижения ***(Преступники используют SQL-инъекцию для «раскрутки» сайтов в поисковиках // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2016/01/15/SQL-seo.html). – 2016. – 15.01).***

***

90 % популярных банковских и медицинских приложений содержат по крайней мере две уязвимости, входящие в OWASP Top 10 – рейтинг самых актуальных уязвимостей приложений, составляемый сообществом Open Web Application Security Project (OWASP). Данный вывод сделали специалисты компании Arxan Technologies по итогам проведенного исследования.

Эксперты провели опрос среди 1083 пользователей из США, Великобритании, Германии и Японии, а также проанализировали 126 наиболее популярных медицинских и финансовых приложений для iOS и Android, в том числе одобренных Управлением по санитарному надзору за качеством пищевых продуктов и медикаментов США (Food and Drug Administration) и Национальной системой здравоохранения Великобритании (UK National Health Service).

Согласно полученным данным, 84 % респондентов уверены в безопасности приложений. По мнению 63 % опрошенных, разработчики прилагают все усилия для обеспечения защиты программ. Вместе с тем 90 % изученных экспертами медицинских приложений содержали по крайней мере две уязвимости из OWASP Top 10. Эксплуатация данных проблем может привести к нарушению конфиденциальности частной жизни, хищению учетных данных и модификации приложения.

Если говорить о финансовых приложениях, 95 % из протестированных программ содержали минимум одну уязвимость из рейтинга мобильных угроз OWASP. Более того, все исследуемые приложения позволяли осуществить модификацию кода или реверс-инжиниринг.

Как правило, мобильные iOS-приложения считаются более защищенными. Однако согласно результатам данного исследования, 100 % протестированных финансовых программ для iOS содержали по крайней мере три уязвимости из топ-10 OWASP, тогда как для Android-приложений этот показатель составил только 59 % ***(90 % медицинских и финансовых приложений содержат по меньшей мере две уязвимости // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2016/01/15/medical-financial-apps-flawed.html). – 2016. – 15.01).***

***

14 января соцсети начали наполняться фотографиями из киевского метро, в котором пассажиры обнаружили странное изображение на экранах. Вместо привычных роликов о правильном поведении в метрополитене на экранах появился актер Э. Скотт в образе Мориарти из популярного сериала «Шерлок» и подпись Miss Me? («Скучали?») (http://ain.ua/2016/01/15/626718).

Данное изображение является отсылкой к финалу третьего сезона телесериала, когда фотография Мориарти с такой же подписью внезапно появляется на всех рекламных экранах Лондона.

Столичные паблики пишут, что выходка является делом рук хакеров, однако каких именно – не сообщается. Пресс-служба Киевского метрополитена ответила на запрос AIN.UA, что изображения Мориарти – не их рук дело и что в настоящее время идет разбирательство. Также в метро уточнили, что размещением изображений занимается не непосредственно метрополитен, а соответствующее рекламное агентство.

Ситуацию можно считать весьма безобидной, однако она показала уязвимости в системе безопасности киевского метро ***(Хакеры взломали экраны киевского метро и показали пассажирам Мориарти из сериала «Шерлок» // AIN.UA (http://ain.ua/2016/01/15/626718). – 2016. – 15.01).***

***

В международном аэропорту «Борисполь» хакеры инфицировали вирусом Black Energy одну из рабочих станций. Об этом в ходе брифинга сообщил спикер Администрации Президента по вопросам АТО А. Лысенко, пишет 112.ua.

«Вчера специалисты-связисты обнаружили, что одна из рабочих станций в аэропорту “Борисполь” была инфицирована вирусом Black Energy. Инфицированный компьютер изолирован от компьютерной инфраструктуры аэропорта, а об инциденте проинформировали экспертов группы CERT-UA. Сейчас идет расследование обстоятельств инцидента», – сообщил он.

По словам А. Лысенко, то, что подобный тип вируса был выявлен во время хакерской атаки на облэнерго в Ивано-Франковске, может указывать на целенаправленный характер акций как диверсии со стороны России ***(Аэропорт «Борисполь» подвергся кибератаке из России – Лысенко // Обозреватель (http://obozrevatel.com/crime/82049-rossijskie-hakeryi-atakovali-aeroport-borispol-lyisenko.htm). – 2016. – 16.01).***

***

Верховный суд Германии признал незаконной функцию «Поиск друзей», которая получает доступ к контактам пользователя и отправляет им приглашения в соцсеть. Об этом сообщает gazeta.ru.

Комитет Верховного суда Германии постановил, что функция по поиску друзей в Facebook является рекламным нарушением. Сама функция социальной сети, получив доступ к любым контактам пользователя, будь то телефоны или электронные адреса, начинает рассылать приглашения его друзьям присоединиться к Facebook. Суд также отметил, что подобная маркетинговая практика соцсети вводит пользователя в заблуждение, кроме того, она слабо информирует его о том, как и к каким данным она получает доступ.

Общество защиты прав потребителей Германии уже выразило надежду, что подобное решение суда станет предупреждением для компаний, использующих схожие рекламные методы ***(«Поиск друзей» в Facebook признали незаконным в Германии // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45898/118/lang,ru/). – 2016. – 15.01).***

***

В китайской армии официально появились кибервойска

Центральный военный совет (ЦВС) КНР объявил о создании в рамках углубленной военной реформы трех новых родов войск в составе Народно-

освободительной армии Китая (НОАК). Речь идет о ракетных войсках, Центре армейского командования и войсках стратегической поддержки. 31 декабря председатель КНР и глава ЦВС С. Цзиньпин передал руководителям новых родов войск их знамена, сообщается на официальном портале Министерства национальной обороны КНР.

Как отмечает издание South China Morning Post со ссылкой на свои источники, силы стратегической поддержки будут включать космические войска и кибервойска. Основной задачей последних станет ведение интернет- и информационных войн.

Согласно заявлению лидера страны С. Цзиньпина, целью переформатирования структуры войск является превращение НОАК из армии регионального и оборонительного типа в армию, способную вести весь спектр боевых операций. Создание новых родов войск является важным стратегическим шагом по формированию современной военной системы с учетом китайской специфики, отметил председатель КНР.

Завершить процесс преобразования армии китайские власти планируют к 2020 г., основные структурные изменения в рамках реформы будут реализованы до конца текущего года ***(В китайской армии официально появились кибервойска // InternetUA (http://internetua.com/v-kitaiskoi-armii-oficialno-poyavilis-kibervoiska). – 2016. – 6.01).***

***

Американские хакеры New World Hacking, борющиеся со сторонниками террористической группировки «Исламское государство» в Интернете, взяли на себя ответственность за атаку на сайт британской вещательной корпорации «Би-би-си», сообщает The Telegraph.

По данным издания, хакеры «тестировали» работу своих систем. «Мы выбрали своей целью “Би-би-си”, чтобы посмотреть, насколько мощные у нас серверы», – написал один из участников группы в своем Twitter.

Они в очередной раз подчеркнули, что их основной целью являются ИГ и сайты, выражающие поддержку террористам. «Би-би-си» пока не дала комментариев.

Ранее сообщалось, что сайты британской вещательной корпорации «Би-би-си» были частично недоступны для пользователей 31 декабря из-за атаки хакеров ***(Борющиеся с ИГ хакеры взяли на себя ответственность за атаку на сайт «Би-би-си» // InternetUA (http://internetua.com/boruasxiesya-s-ig-hakeri-vzyali-na-sebya-otvetstvennost-za-ataku-na-sait--bi-bi-si). – 2016. – 2.01).***

***

Неутомимые Anonymous продолжают «ради шутки» атаковать международные организации и крупные компании. Спустя две недели после взлома поддоменов сайта Европейского космического агентства (European Space Agency, ESA) жертвой активистов стал автопроизводитель Honda Motor.

При попытке зайти на сайт autos.honda.com.co открывается страница с символьным изображением корабля и измененным текстом заглавной песни американского комедийного сериала «Лодка любви». Слово love в тексте заменено на lulz. Саундтреком к картинке служит все та же «Лодка любви».

В отличие от других атак Anonymous, имеющих политическую или социальную подоплеку, данный взлом был осуществлен исключительно ради развлечения. Если навести курсор на открытую вкладку autos.honda.com.co, появляется сообщение: «Ваша безопасность оставляет желать лучшего, вот и чувствуйте себя так же» ***(Anonymous ради шутки атаковали компанию Honda // InternetUA (http://internetua.com/Anonymous-radi-shutki-atakovali-kompaniua-Honda). – 2015. – 29.12).***

***

Безымянные защитники Интернета. Кто такие Anonymous?

В последнее время хакерская группировка Anonymous все чаще фигурирует в мировых новостях. Они противостоят спецслужбам и авторитарным правительствам, сражаются с членами ку-клукс-клана и террористами ИГИЛ. На фоне столь бурной деятельности у простых обывателей всё чаще возникает вопросы о том, кто такие Anonymous, откуда они взялись и за что, собственно говоря, борются. На эти вопросы мы и попытаемся дать ответ.

Кто они и откуда

Идея Anonymous зародилась еще в 2003 г. в разделе /b/ на имиджборде 4chan – полностью анонимном веб-форуме. Раздел /b/ – единственная категория форума, где отсутствуют какие-либо правила. В этом канале царит первозданный хаос и находят отражение диаметрально противоположные стороны человеческой натуры.

Ошибочно воспринимать Anonymous как некую ограниченную группу лиц с установленной иерархией и лидерами. Anonymous – в первую очередь, идея, которая предполагает, что Интернет должен быть максимально свободным и открытым для всех без исключения. Согласно философии Anonymous, ни спецслужбы, ни государства, ни корпорации не имеют права присваивать себе киберпространство и вмешиваться в него, устанавливая цензуру или иные ограничения.

Такая идея изначально не предполагает никакой жесткой структуры или постоянного состава. Само собой, когда речь идет о резонансных взломах с похищением и обнародованием информации, за этим могут стоять вполне определенные хакеры. Но когда на какой-либо «проштрафившийся» объект совершается мощная скоординированная атака силами десятков тысяч возмущенных пользователей, то каждый из этих пользователей – Anonymous по крайней мере до завершения акции.

Операции Anonymous координируются на анонимных имиджбордах, вроде уже названного 4chan, в социальных сетях, общественных каналах мессенджеров и IRC. Существуют отдельные ресурсы вроде AnonOps, где

желающие могут не только спланировать свои действия, но и получить инструкции о том, как именно помочь общему делу. В общем, Anonymous представляет собой некое самоорганизующееся общественное сознание Интернета.

Борьба и цели Anonymous

Хотя концепция движения Anonymous возникла еще в 2003 г., первая массовая акция датируется 2008 г. Тогда Церкви саентологии попыталась добиться удаления из сети интервью с Т. Крузом, где тот раскрывал некоторую информацию об этой закрытой организации. Интернет-общественность восприняла этот акт как попытку установления цензуры. На Церковь саентологии обрушился град DDoS-атак, спама (в том числе, бумажного), пранков и критики. Люди в масках Гая Фокса, одного из символов Anonymous выходили на реальные протесты. Эти события способствовали широкому распространению информации о движении Anonymous и его популяризации.

Вскоре после этого борьба Anonymous приобрела и политические оттенки. Когда в 2010 г. по фиктивному обвинению в изнасиловании был арестован основатель Wikileaks Д. Ассанж, интернет-общественность снова активизировалась. Тогда гнев Anonymous был направлен на все организации, прямо или косвенно ответственные за любые ограничения свободы в Интернете, преследования пиратов и Ассанжа. Так, в ходе операции «Расплата» были взломаны платежные системы PayPal, Mastercard, Visa, ресурсы банка PostFinance, сайты шведского правительства и нескольких сенаторов США. Крепко досталось даже Amazon, который ранее «выселил» ресурс WikiLeaks с одного из своих серверов.

После этого Anonymous произвели еще множество успешных операций, атакуя всех, кто, по мнению движения, этого заслуживает: от авторитарных правительств до распространителей детской порнографии.

Интересно, что одна из наиболее успешных операций Anonymous была связана с Украиной. Когда в начале 2012 г. правительство В. Януковича попыталось остановить работу EX.UA, крупнейшего файлообменника страны, это вызвало справедливый гнев общественности. Активисты «положили» сайты Президента, Кабинета Министров, МВД, Службы безопасности Украины, Верховной Рады. Кроме того, люди вышли на реальные акции протеста. Всё это вынудило правительство пойти на попятную и вернуть EX.UA в строй. Спустя два года Anonymous помогали украинцам бороться с властями в ходе Революции достоинства, снова атакуя правительственные ресурсы.

В 2015 г. движение Anonymous активизировалось особенно сильно. Объявление войны террористической группировке ИГИЛ и последующее разоблачение 5,5 тыс. аккаунтов боевиков стало одной из самых масштабных акций прошлого года. Впрочем, следует признать, что какая-либо религиозная или национальная дискриминация чужда Anonymous. Так, активисты атакуют боевиков ИГИЛ, но когда Д. Трамп выступает с агрессивными высказываниями против всех мусульман, Anonymous незамедлительно атакует и его.

В общем, никем не контролируемое общественное движение Anonymous борется против какой-либо дискриминации и ограничений, будь то попытка установления религиозной диктатуры на Востоке или ужесточение закона об авторском праве на Западе. У общественного сознания, порожденного самой сетью, есть свое собственное видение мира и справедливости. Это можно восхвалять и считать высшей формой общественной самоорганизации. Это можно ненавидеть и считать проявлениями хаоса и анархизма. Но чего делать совершенно нельзя, так это игнорировать Anonymous. Потому что, если верить лозунгу движения, Anonymous – это Легион, который ничего не прощает и ничего не забывает ***(Безымянные защитники интернета. Кто такие Anonymous? // InternetUA (http://internetua.com/bezimyannie-zasxitniki-interneta--kto-takie-Anonymous). – 2016. – 16.01).***

***

Эксперты Symantec выявили свежую версию Andriod.Bankosy, которая способна перехватывать не только одноразовые SMS-коды, но и коды аутентификации, передаваемые через голосовые звонки. Об этом компания Symantec сообщила в своем блоге.

Как работал троян прежде?

Специалисты Symantec утверждают, что совсем недавно Android.Bankosy мало отличался от своих собратьев. В составе сторонних приложений троян проникал в систему, собирал данные жертвы и перенаправлял их на командный сервер. Если ситуация этого требовала, то Android.Bankosy перехватывал и стирал SMS-сообщения, в том числе и с кодами аутентификации.

Однако в последнее время в обращение вошли системы, сообщающие одноразовые коды голосом: система звонит пользователю, а робот зачитывает одноразовый код. По мнению экспертов Symantec, и этот способ уже нельзя считать надежным.

Как работает троян сейчас?

Свежий релиз Android.Bankosy переводит смартфон в беззвучный режим и перехватывает автоматические голосовые звонки, в ходе которых пользователю сообщается одноразовый код. После успешного перехвата одноразового кода командный сервер «командует» трояну отключить переадресацию. Пока жертва дожидается автоматического вызова с кодом аутентификации, злоумышленники уже завершают транзакцию за нее.

На сегодняшний день такая функция трояна работает лишь для ряда азиатских стран. Здесь переадресацию можно настроить простой командой *21*[номер переадресации]#.

Способы защиты

Специалисты Symantec рекомендуют стандартный набор действий для защиты от подобного вмешательства: вовремя обновлять программное обеспечение, не устанавливать программ и приложений из непроверенных источников, внимательно следить за тем, какие разрешения запрашивает устанавливаемое приложение, а также обзавестись антивирусом ***(Осторожно:***

мобильный троян обходит сверхнадежную двойную защиту // InternetUA (http://internetua.com/ostorojno--mobilnii-troyan-obhodit-sverhnadejnuua-dvoinuua-zasxitu). – 2016. – 17.01).

***

IT-инфраструктура железной дороги уязвима к кибератакам

27 декабря в рамках Всемирного хакерского конгресса (Chaos Communcation Congress) специалисты по безопасности С. Гордейчик, А. Тиморин и Г. Грицай от лица команды SCADA StrangeLove представили анализ компьютерной системы мировой железной дороги. Как пояснил С. Гордейчик в беседе с журналистами портала SecurityWeek, команда проанализировала различные компоненты железнодорожных систем с целью выяснить степень их безопасности.

В ходе презентации специалисты акцентировали внимание на уязвимостях в современной версии системы железнодорожной автоматизации, используемой во многих европейских странах. Данная система работает на компонентах Siemens SIMATIC, таких как контроллеры WinAC RTX. По сути, устройства представляют собой персональные компьютеры семейства x86 на базе Windows. Как указали эксперты, контроллеры подвержены нескольким уязвимостям. В частности, злоумышленник может получить контроль над устройством без прохождения аутентификации.

Уязвимой также оказалась комплексная система централизации и компьютеризированного управления железнодорожными стрелками. Например, современные свидетельства о допуске для нового оборудования, используемые в решении для безопасного усовершенствования управления лондонским метро, содержат такие странные требования, как Windows XP или даже «Windows NT 4.0 Service Pack 6 или выше».

Еще одна потенциальная проблема заключается в нарушении правил базовой безопасности некомпетентными сотрудниками, работающими с оборудованием. Нередко бумажка с логином и паролем от системы управления железнодорожными стрелками хранится на рабочем столе обычного клерка.

Системы связи на железной дороге также несовершенны. К примеру, в пути поезд подключается к системе железнодорожного контроля по сети GSM-R, по сути, не сильно отличающейся от обычной GSM-системы с присущими ей недостатками, в том числе возможности клонирования SIM-карт, используемых для связи машиниста с диспетчером, несовершенных систем обновления ПО, передачи команд по SMS (с PIN-кодом 1234 по умолчанию) и т. д. Зачастую железнодорожные сети используют логины и пароли, заданные производителем по умолчанию.

По словам исследователей, хотя железнодорожные системы не связаны с Интернетом, злоумышленники могут эксплуатировать различные ошибки в компонентах и получить удаленный доступ к критическим системам ***(IT-инфраструктура железной дороги уязвима к кибератакам // InternetUA***

(http://internetua.com/IT-infrastruktura-jeleznoi-doroqi-uyazvima-k-kiberatakam). – 2015. – 31.12).

***

Исследователи компании Symantec обнаружили новый образец вредоносного ПО для Android, использующий межсетевой экран DroidWall для избежания обнаружения антивирусным ПО. Вредонос под названием Android.Spywaller собирает персональные данные жертв и отправляет информацию на подконтрольные злоумышленникам серверы.

При инфицировании системы Android.Spywaller внедряется в память устройства и отображается под видом приложения Google Service. Вредонос пытается получить права суперпользователя и в случае успеха начинает сбор персональных данных в фоновом режиме.

Отличительной особенностью данного вредоноса является использование мобильного межсетевого экрана DroidWall для предотвращения обнаружения антивирусным ПО. Android.Spywaller сканирует систему на предмет наличия популярного китайского антивируса Qihoo 360, после чего блокирует уникальный идентификатор программы с помощью DroidWall.

Вредонос нацелен на китайских пользователей. В КНР большая часть устройств имеет привилегии суперпользователя, упрощая процесс установки вредоносного ПО. К тому же, в связи с интернет-цензурой пользователи не могут получить доступ к официальным сервисам Google, в то время как Android.Spywaller имитирует одно из приложений компании.

Android.Spywaller перехватывает и отправляет злоумышленникам данные о журнале звонков, SMS-сообщениях, местоположении, а также журнал браузера, электронные сообщения, изображения и контакты жертвы. Кроме того, собирается информация из популярных мессенджеров, включая BlackBerry Messenger, Oovoo, Coco, QQ, SinaWeibo, Skype, Talkbox, TencentWeibo, Voxer, Wechat, WhatsApp и Zello ***(Новый Android-вредонос блокирует работу антивирусов // InternetUA (http://internetua.com/novii-Android-vredonos-blokiruet-rabotu-antivirusov). – 2015. – 31.12).***

***

Специалист по компьютерной безопасности, который в конце сентября выявил серьёзный недостаток в системе Gatekeeper от Apple, заявил, что данная проблема до сих пор не решена. Компания Apple выпустила два патча, которые должны были закрыть уязвимости в Gatekeeper. На деле же оказалось, что выпущенные обновления лишь блокируют работу отдельных приложений, но не решают проблему целиком. Напомним, система контроля Gatekeeper позволяет пользователю убедиться, что его компьютер Mac будет запускать только скачанные из Mac Store приложения. Как вариант – приложения, подписанные известным разработчиком, если снизить соответствующий уровень защиты.

П. Уордл, тот самый специалист по компьютерной безопасности, смог выявить уязвимость системы защиты Gatekeeper в сентябре прошлого года. Используя найденную брешь в системе безопасности, злоумышленник мог устанавливать любое приложение с вредоносным кодом вне зависимости от уровня установленной в Gatekeeper защиты. П. Уордл поспешил сообщить о найденной уязвимости Apple, после чего купертинцы пообещали оперативно выпустить соответствующие правки в программном коде.

Представленные вскоре патчи были изучены П. Уордлом, после чего специалист и сделал заявление о недостаточной эффективности предпринятых Apple мер по устранению «дыр» в Gatekeeper. Система блокирует избранные приложения, но не решает проблему целиком. Apple пообещала в скором времени представить более комплексное решение возникшей проблемы ***(Серьёзная уязвимость в OS X не исправлена спустя 3 месяца после обнаружения // InternetUA (http://internetua.com/ser-znaya-uyazvimost-v-OS-X-ne-ispravlena-spustya-3-mesyaca-posle-obnarujeniya). – 2016. – 17.01).***

***

Банковский Android-троян SlemBunk продолжает эволюционировать

В декабре прошлого года эксперты FireEye сообщили о продолжающейся вредоносной кампании с использованием банковского Android-трояна SlemBunk, распространяемого через вредоносные ресурсы и сайты с контентом «для взрослых». Троянские программы маскируются под легитимные приложения наподобие Adobe Flash Player, и перехватывают конфиденциальные данные пользователей.

Специалисты выявили 170 образцов вредоноса, разработанного для атак на пользователей 33 финансовых приложений от банков и сервис-провайдеров из Северной Америки, Европы и Азиатско-Тихоокеанского региона.

Как показал анализ вредоносной кампании, троян SlemBunk использует больше механизмов доставки полезной нагрузки, чем предполагалось ранее. На первом этапе при посещении жертвой подконтрольного злоумышленникам веб-сайта на компьютер загружается дроппер. Затем дроппер распаковывает троян-загрузчик. На завершающем этапе последний отправляет запрос на C&C-сервер злоумышленников и загружает полезную нагрузку.

По словам экспертов, вредоносная кампания хорошо организована и продолжает развиваться. Помимо прочего, злоумышленники могут изменять способ, используемый загрузчиком для доставки финальной полезной нагрузки.

Исследователи обнаружили несколько C&C-доменов, зарегистрированных в разные периоды 2015 г. Как позволяет предположить анализ используемой Android-трояном C&C-инфраструктуры, в будущем вредоносная кампания может принимать иные формы ***(Банковский Android-троян SlemBunk продолжает эволюционировать // InternetUA (http://internetua.com/bankovskii-Android-troyan-SlemBunk-prodoljaet-evoluacionirovat). – 2016. – 17.01).***

***

Воры начали слежку за украинцами в соцсетях

На время длинных новогодних и рождественских праздников увеличилось количество квартирных краж.

Причем воры стали более изобретательными. Теперь они активно отслеживают соцсети, в которых наивные граждане выкладывают не только фото с горнолыжных курортов или экзотических островов, но даже снимки посадочных талонов на самолет. Из них преступники могут почерпнуть немало информации.

Билеты и посадочные талоны

В последнее время домушники стали более продвинутыми. Им хватит фото ваших билетов в театр, кино или посадочного талона на самолет, которыми вы похвастаетесь в соцсетях. По билету в театр они легко определят, сколько времени вас не будет дома. А по посадочному талону хорошо видно, в какое время и куда вы отправляетесь.

«На всякий случай они будут прозванивать вашу квартиру, чтобы убедиться, что вместо вас там не поселились родственники или домработница. А потом просто взламывают замки. Могут наблюдать за вашей квартирой под видом прогулок с собакой во дворе. А по штрих-коду вашего посадочного талона они могут даже вычислить ваши паспортные данные, адрес и номер телефона – просто зайдут на сайт авиакомпании и посмотрят. Такое вполне возможно», – рассказал один из оперуполномоченных Нацполиции в Киеве.

Не используйте соцсети

Президент Всеукраинской федерации профессионалов безопасности С. Шабовта советует в первую очередь ограничить свою активность в соцсетях. «Не стоит выкладывать фото своей квартиры, новых гаджетов в Facebook. А также билеты и прочее. Отследить адрес и личные данные опытному вору труда не составит. Многие просто подслушивают разговоры подростков и маленьких детей, которые хвастаются, что им купили гаджеты или что они поедут в отпуск. А потом уже в два счета вычисляют жертву», – сказал он ***(Воры начали слежку за украинцами в соцсетях // InternetUA (http://internetua.com/vori-nacsali-slejku-za-ukraincami-v-socsetyah). – 2016. – 16.01).***

***

Головним комп’ютерним «ворогом» українців у 2015 р. стали не програми-здирники і навіть не віруси, що крадуть дані. У списку «лиходіїв» лідирує adware – програмне забезпечення, яке показує банери, підміняє пошукову видачу і «накручує» рекламний трафік. Чим небезпечні такі віруси, та які загрози чекають на українців у новому році?

Рік у кіберзагрозах

Минулий рік для України був насиченим на події у сфері кібербезпеки. Наприкінці жовтня під час місцевих виборів атакам піддалися телеканали та сайти найбільших медіагруп – «Медіа групи Україна», Starlightmedia, «Інтер Медіа Груп», а також телеканалів ATR, «5 канал», сайти політичних сил.

Зовсім недавно, у грудні, також стало відомо про велику атаку, яка частково вивела з ладу українську енергосистему і залишила велику частину Прикарпаття без електрики.

Життя простих користувачів Інтернету теж не було нудним. Кібешахраї весь рік намагалися виманювати у них гроші і інформацію. У першу чергу для цього використовували методи соціальної інженерії: фішинг і вивідування конфіденційної інформації – логінів і паролів, даних банківських карт.

«При цьому шахраї стали часто грати на таких болісних і тонких темах як війна, маніпулювали на тему волонтерства», – розповів технічний директор компанії «Zillya! Антивірус» (виробляє антивірусне ПО. – Ред.) О. Сич. Крім того, на комп'ютери жертв потрапляли шкідливі програми, у тому числі шпигунські.

За даними Міністерства внутрішніх справ України, тільки за вісім місяців 2015 р. хакери вкрали з банківських карток українців близько 500 млн грн. Всього за цей період було зафіксовано 20 тис. випадків незаконних операцій з картками.

У «Лабораторії Касперського» порахували, що у 2015 р. кількість користувачів, атакованих програмами-вимагачами, зросла в 1,7 раза. При цьому Україна виявилася другою в списку країн, найбільш схильних до ризику зіткнення з цією загрозою, поступаючись за цим показником лише Казахстану.

Головні обдурювачі рекламодавців

Але найбільш активними «вірусами» в Україні стали аж ніяк не програми-здирники. За даними Zillya, близько 51 % всіх зафіксованих атак довелося на adware – програми, які показують користувачам рекламні банери, підміняють пошукову видачу. Мета таких програм – накрутка рекламних переходів і відвідуваності різних ресурсів.

Популярність цих програм підтверджують і в «Лабораторії Касперського», хоча компанія зафіксувала меншу частку атак з їх використанням . За її даними, рекламні програми та їх компоненти зайняли 12 позицій у ТОП-20 загроз. І вони були зафіксовані на 26,1 % всіх комп'ютерів, на яких спрацював веб-антивірус «Лабораторії».

Агресивна реклама не завдає шкоди комп'ютеру, але доставляє незручність користувачам, заважає комфортно переглядати сайти. Наприклад, як розповів О. Сич, найпоширеніше сімейство вірусів, Adware.Agent, встановлюється на комп'ютер потай від користувача і виявляє свою активність у вигляді нав'язливих спливаючих вікон з рекламою або підміною результатів пошуку.

Програми другого за популярністю сімейства, Adware.Eorezo, мають прихованим функціоналом, таким, як показ спливаючої реклами, відкриття додаткових вікон в браузері і перенаправлення користувача на рекламні сайти і сайти із шкідливим програмним забезпеченням. Також, потай від користувача, на комп'ютер завантажуються інші рекламні модулі.

Ще одне сімейство рекламного ПЗ, Рекламне.CrossRider, в основному використовується для чорного SEO, тобто для розкрутки або підвищення

рейтингу сайту за рахунок перенаправлення на нього користувачів, що заразилися вірусом.

А нав'язливе програмне забезпечення Adware.ConvertAd при перегляді веб-сторінок показує квадратні спливаючі вікна з рекламою. Крім того, на сторінках можуть з'являтися банери з рекламою, а посилання підміняються на рекламні. На комп'ютер користувача також будуть завантажуватися інші програми рекламного характеру.

Замикає п'ятірку найпоширеніших «вірусів» сімейство шкідливих програм Exploit.Black.Win32, упакованих протектором Themida. Слід зазначити, що так може бути упакована будь-троянська програма, не тільки adware.

Збільшення кількості рекламних програм, агресивні способи їх поширення та їх протидія детектування з боку антивірусів продовжують тренд 2014 р., вважають у «Лабораторії Касперського».

У свою чергу фахівці Zillya прогнозують, що у 2016 р. усі тренди минулого року збережуться. Однак у лідери впевнено вийде соціальна інженерія як метод кібершахрайства. Особливо її аспект, пов'язаний із соцмережами. Для підвищення кібербезпеки користувачам необхідно більш відповідально підходити до своєї інформації, розміщеної у соцмережах ***(Неуявна загроза: хто атакував комп'ютери українців у 2015 році // Finance.ua (http://news.finance.ua/ua/news/-/366952/neuyavna-zagroza-hto-atakuvav-kompyutery-ukrayintsiv-u-2015-rotsi). – 2016. – 11.01).***

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»

Упорядник **Касаткіна** Тетяна

Редактори: Т. Дубас, О. Федоренко, Ю. Шлапак

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.