СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(28.04–11.05)

2015 № 9

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(28.04–11.05)
№ 9

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

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Facebook усовершенствовала свой сервис Messenger. В фирменный чат добавили функцию видеозвонков. Приложение, созданное программистами социальной сети, позволяет устроить видеоконференцию в любой момент одним нажатием кнопки, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-dobavila-v-messenger-videozvonki-44145/).

Facebook в роли догоняющей

Компания М. Цукерберга добавила в Messenger функцию, которой нет у принадлежащей Facebook WhatsApp. В то же время на рынке уже давно есть другие мессенджеры с интегрированными видеозвонками. Общаться «с глазу на глаз» позволяют такие приложения, как FaceTime от Apple, Google Hangouts и принадлежащий Microsoft сервис Skype, а также ряд азиатских мессенджеров.

Если рассматривать видеоконференции в Messenger с технологической точки зрения, ничего нового мы не видим. Разве что много внимания программисты Facebook уделили неприхотливости системы. Даже в местах, где сигнал LTE ловится достаточно плохо, можно будет попытаться сделать видеовызов.

Но стоит обратить внимание на эргономику и на то, как новая возможность вписывается в экосистему социальной сети. Устроить видеозвонок можно при наличии устойчивого соединения по LTE или Wi-Fi с любым из контактов в Messenger. Это обеспечивает данному сервису серьезное преимущество, ведь в списке контактов будут все ваши друзья из Facebook. У большинства пользователей их количество составляет не менее сотни, в то время как список контактов в Skype гораздо короче.

С прицелом на корпорации

М. Цукерберг не боится, что разработка вышла на рынок так поздно. В Facebook рассчитывают, что ниша для обновленного мессенджера на рынке найдется, как это было и с предыдущей его версией, даже несмотря на внутреннюю конкуренцию с WhatsApp. Идея в этом случае заключается в том, что видеоконференции необходимы для развития корпоративной версии социальной сети – Facebook At Work.

О системе Facebook At Work заговорили совсем недавно – в январе 2015 г. В каком-то смысле эта версия портала – альтернатива сети для профессионалов LinkedIn. Одно из ключевых отличий от обычной Facebook – отсутствие рекламы и сбора информации о пользователях.

Развивая свой бизнес и выходя в корпоративный сектор, Facebook должна получить преимущество в функционале. Сегодня практически все преуспевающие компании используют такие инструменты, как Skype, для организации междугородних и международных видеоконференций. А в последнее время набирают популярность и корпоративные видеозвонки по мобильному. Теперь можно использовать альтернативу.

Отметим, что пока нет информации о том, возможно ли будет общаться коллективно в Messenger. До сих пор лишь в браузерной версии Messenger, интегрированной в портал Facebook для настольных компьютеров, существовала функция видеовызова, и количество собеседников увеличить было нельзя. Очевидно, что на небольшом экране смартфона несколько окон с видео будут слишком маленькими, а канал Интернета быстро забьется, так что полностью заменить все функции того же Skype решение Facebook не сможет, да и не должно.

В настоящее время у приложения Messenger на одном только Google Play скачиваний более 500 млн. Количество пользователей, которые активно пользуются мессенджером, по оценкам Facebook, достигает 600 млн. 10 % от всех телефонных звонков в Интернете уже совершается через это приложение. Чтобы ускорить свое развитие на прошлой неделе Facebook представила сервис Hello – приложение для управления контактами для Android. Несмотря на то что общение через Messenger не приносит Facebook прибыли, в итоге его могут попытаться превратить в огромную платформу для монетизации, подобную азиатским LINE и WeChat.

Число активных пользователей соцсети на конец I квартала составляло 1,44 млрд – за год их число возросло на 13 %. С мобильных устройств не реже раза в месяц Facebook использовали 1,15 млрд человек, что на 24 % больше, чем годом ранее ***(Facebook добавила в Messenger видеозвонки // Marketing Media Review (http://mmr.ua/news/id/facebook-dobavila-v-messenger-videozvonki-44145/). – 2015. – 28.04).***

***

Пользователи Facebook в Европе могут получать доступ к новым функциям социальной сети позже пользователей остального мира или не получать их вообще, заявил представитель компании в ЕС изданию Financial Times.

Facebook связывает это с ростом затрат в результате увеличения законодательного давления на социальную сеть в ЕС.

Европейские власти не согласны с тем, что законодательство Ирландии, в чьей юрисдикции находится компания, в области использования персональных данных и приватности, не должны распространяться на всех граждан Европы. За последнее время Facebook столкнулась с рядом соответствующих обвинений во Франции, Испании, Нидерландах, Германии и Бельгии ***(Facebook пригрозил Евросоюзу ограничением доступа к функционалу // InternetUA (http://internetua.com/Facebook-prigrozil-evrosouazu-ogranicseniem-dostupa-k-funkcionalu). – 2015. – 29.04).***

***

Анонимная соцсеть Secret прекратит существование

Основатель приложения по анонимному общению Secret Д. Биттау объявил о закрытии сервиса. Об этом он написал в своем блоге на Medium.

«К сожалению, Secret уже не отражает видение, которое у меня было изначально, когда я основал компанию. Поэтому считаю это [закрытие сервиса] правильным решением для себя, инвесторов и команды», – отметил он.

Д. Биттау добавил, что в ближайшее время будет работать над достойным завершением дела Secret. Он также рассказал, что поможет команде найти новые рабочие места и вернет деньги, вложенные инвесторами.

Сервис для обмена анонимных сообщений Secret был запущен в феврале 2014 г. бывшими сотрудниками Google К. Бадер-Векселером и Д. Биттау. Доступ к Secret в странах за пределами США открыли 21 мая прошлого года, и сразу после запуска он начал набирать вирусную популярность и в рунете. После регистрации пользователь может отправлять анонимные сообщения и читать публикации других. Если он интегрирует приложение со списком контактов на смартфоне и укажет свое местоположение, то приложение выделит для него «секреты» от друзей, друзей его друзей и от пользователей, находящихся неподалеку.

Сервис привлек в общей сложности 35 млн дол. от различных инвесторов и фондов, в частности таких известных, как Google Ventures и Kleiner Perkins. По данным The New York Times, в ходе последнего раунда (в июле 2014 г.) стоимость Secret оценивалась в 100 млн дол. Мобильным приложением по всему миру пользуются более 15 млн человек ***(Анонимная соцсеть Secret прекратит существование // InternetUA (http://internetua.com/anonimnaya-socset-Secret-prekratit-susxestvovanie). – 2015. – 1.05).***

***

Instagram запускает хэштеги с Emoji и новые фильтры

Почти в половине всех подписей к снимкам в Instagram используется эмодзи (смайлики). Теперь эмодзи будут работать совместно с хэштегами, и у пользователей появится возможность добавлять их к своим постам, искать их через страницу поиска и использовать их в подписях к своим инста-снимкам. Пользователи также смогут добавлять один или несколько эмодзи сразу, а также использовать комбинацию текста и смайла, создавая креативные хэштеги.

В Instagram также появилось три новых фильтра: Lark, Reyes and Juno ***(Instagram запускает хэштеги с Emoji и новые фильтры // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/instagram_zapuskaet_heshtegi_s_emoji_i_novye_filtry). – 2015. – 5.05).***

***

Поиск внутри устройств Apple будет отображать данные из Twitter

В iOS и Mac присутствует встроенная системная служба поиска Spotlight, которая позволяет находить людей, приложения, документы, картинки и другие виды файлов. Утилита работает очень интуитивно, предугадывая, что именно пользователь пытается найти в текущий момент.

В ближайшее время в выдаче Spotlight начнут появляться твиты пользователей, имя которых было введено в строку поиска. Как сообщает PCWorld со ссылкой на CEO Twitter Д. Костоло, соцсеть и Apple в настоящее время совместно работают над новыми функциями.

Обычными источниками поиска Spotlight являются локальные файлы, данные из документов в облаке, в том числе совместно редактируемых, сообщения электронной почты, Википедия и поисковая выдача Bing.

Д. Костоло не стал раскрывать подробностей проводимой работы, но добавил, что изменения позволят сторонним пользователям получать контент из Twitter. Это, в свою очередь, поможет компании преодолеть проблему роста и привлечения новых клиентов, которую она переживает последний год ***(Поиск внутри устройств Apple будет отображать данные из Twitter // InternetUA (http://internetua.com/poisk-vnutri-ustroistv-Apple-budet-otobrajat-dannie-iz-Twitter). – 2015. – 1.05).***

***

С начала мая два интернет-гиганта Google и Twitter сообщили о старте плотного сотрудничества.

В результаты поиска Google теперь будут включаться и результаты по поиску среди твитов, подходящих по ключевым словам.

Как известно, ранее сотрудничество уже имело место быть, но в 2011 г. руководство компаний сильно повздорило и прекратило любые взаимоотношения. Лишь недавно было объявлено, что «лёд» между компаниями тронулся.

Дабы получить твит в результате поиска, не нужно быть авторизованным в социальной сети. Таким образом Twitter планирует привлечь большее внимание к сервису микроблогов.

По неподтвержденной информации, в настоящее время подобное сотрудничество также планируется наладить и между Apple и Twitter, но подробности пока неизвестны ***(В поиске Google теперь отображаются твиты // iLenta.com (http://ilenta.com/news/internet/news_6666.html). – 2015. – 5.05).***

***

Социальная сеть «ВКонтакте» превзошла в марте федеральные телеканалы по дневной и недельной аудитории. Об этом сообщил у себя в Facebook пресс-секретарь социальной сети Г. Лобушкин со ссылкой на данные исследовательской компании TNS, пишет gazeta.ru.

Суточный охват «ВКонтакте» составил 13,3 млн человек. У ближайшего преследователя, Первого канала, этот показатель составил 10,9 млн человек. В случае с недельной аудиторией у Первого и у «ВКонтакте» показатели одинаковые – 20,1 млн человек. На третьем месте по показателю недельного охвата находится канал ТНТ – его за неделю посмотрели 18,4 млн человек, почти на 2 млн меньше. Дневной охват ТНТ составил 9,8 млн человек.

Исследование TNS по охвату аудитории проводилось во всех городах России с населением свыше 100 тыс. человек. В исследовании принимали участие лица в возрасте от 12 до 44 лет ***(«ВКонтакте» опережает по популярности телевидение // МедиаБизнес (http://www.mediabusiness.com.ua/?option=com_content&task=view&id=43304&Itemid=). – 2015. – 6.05).***

***

В маєFacebook начнёт в полном объёме публиковать статьи и видеоролики ведущих издателей, таких как Buzzfeed, National Geographic и The New York Times. Новая функция получила название «Мгновенные статьи» (Instant Articles).

Социальная сеть работает над новым функционалом, как минимум, с марта этого года. Facebook предлагает новостным организациям специальные рекламные модели, поощряя их принять участие в проекте. По одной из предлагаемых моделей, компания позволит издателям сохранить 100 % дохода от рекламы, которую они продают сами, а также 70 % от рекламы, которую для них продаёт Facebook.

По данным The Wall Street Journal, руководство Facebook вполне устраивает небольшой доход от этой сделки, поскольку цель проекта – не заработать деньги, а поощрить пользователей оставаться на сайте дольше. Руководство социальной сети предполагает, что пользователи предпочтут читать публикации и смотреть видео в своих новостных лентах вместо загрузки материалов по ссылке, что каждый раз, в среднем, занимает около 8 секунд.

Несмотря на заманчивое предложение, многие издатели не горят желанием быть более тесно связанными с социальной сетью. Они не в восторге от идеи предоставления Facebook контроля над своим контентом и отсутствием доступа к информации о своих читателях.

В настоящее время Facebook всё ещё в процессе закрытия сделки с тремя партнёрами по запуску. Таким образом, дебют «Мгновенных статей» может быть перенесён на более позднюю дату ***(С мая новости ведущих издателей будут публиковаться напрямую в Facebook // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/s_maya_novosti_veduschih_izdateley_budut_publikovatsya_napryamuyu_v_facebook). – 2015. – 6.05).***

***

Facebook тестирует новую опцию, позволяющую пользователям выбрать друзей или публичные страницы, чьи посты они не хотели бы пропустить. Публикации от указанных аккаунтов будут отображаться в топе новостной ленты пользователя, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-pozvolil-polzovateljam-vybirat-chto-budet-v-tope-ih-novostnoj-lent-44256/).

В настоящее время новый функционал доступен ограниченному количеству мобильных пользователей Facebook. Они видят окно с анимированным щенком и сообщением «Просматривайте больше того, что вы любите».

Нажатие на сообщение приводит к появлению окна, отображающего друзей и страницы, на которые пользователь подписан.

В диалоговом окне сообщается, что постам от выбранных страниц и людей будет отдаваться приоритет в новостной ленте: «Их посты появятся в топе вашей новостной ленты, так что теперь вы их точно не пропустите».

Пресс-секретарь Facebook подтвердил проведение небольшого теста в комментарии изданию Marketing Land.

Если тест будет запущен в полноценном масштабе, это будет значительным изменением механизма работы новостной ленты социальной сети, считает М. Бэк из Marketing Land.

Обычно, контент ленты основан на поведенческих сигналах, а не выраженных предпочтениях пользователей. Facebook обычно больше полагается на то, с чем люди взаимодействуют, а не чего они хотят.

Это нововведение также может помочь брендам усилить доставку их сообщений до потребителей в новостной ленте. Поскольку органический охват публичных страниц сократился, многие компании разочарованы тем, что теперь им сложнее достигать тех пользователей, которые «лайкнули» их страницы. Пользователи могут отключить получение уведомлений от публичных страниц, но пространство новостной ленты потребителей более желанно для компаний.

Чтобы воспользоваться преимуществами потенциального нововведения, брендам и компаниям нужно будет убедить своих фанов отдать приоритет их страницам в ленте. Компании смогут выполнить эту задачу, если будут предоставлять своим подписчикам вовлекающий и подпитывающий их лояльность контент.

«Медиа издатели получат неоспоримое преимущество, поскольку их задача – создавать отличные истории. Тем не менее, любой бренд, который сможет предложить реально хороший контент, сможет повысить лояльность своих фанов», – считает У. Ларсен, основатель и директор платформы Falcon Social ***(Facebook позволил пользователям выбирать, что будет в топе их новостной лент // Marketing Media Review (http://mmr.ua/news/id/facebook-pozvolil-polzovateljam-vybirat-chto-budet-v-tope-ih-novostnoj-lent-44256/). – 2015. – 7.05).***

***

Социальная сеть Google+ не оставляет надежд сделать своих пользователей активнее. Сервис запустил новую функцию Collections (Подборки), которая позволяет создавать сборники из понравившихся материалов. Таким образом соцсеть практически скопировала основной функционал сервиса Pinterest. Об этом пишет vesti.ru.

В подборки можно добавлять тексты, фотографии, видео и другой контент. Одну и ту же коллекцию могут вести сразу несколько администраторов. Имеется возможность настраивать цвет обложки, также предусмотрены гибкие настройки приватности.

Тем не менее, полностью Pinterest новая функция Google+ заменить пока что не сможет, так как в ней крайне ограничены возможности по поиску нового контента. Вероятно, Google доработает сервис в будущем. В течение ближайшего времени новой функцией можно будет воспользоваться при помощи браузерной версии сайта, а также обновленного приложения для Android. До конкурирующей платформы iOS «Подборки», по всей видимости, доберутся позже ***(В Google+ появились подборки на манер Pinterest // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43336/118/lang,ru/). – 2015. – 8.05).***

***

Социальная сеть Google+ напомнила о себе, опубликовав сообщение в Twitter: «Привет, Twitter-версия! Можем ли мы привлечь внимание к нашему первому твиту?»

Быстрая проверка страницы показала, что аккаунт на самом деле ведут сотрудники Google, причем дата его создания – июль 2011 г. – совпадает с настоящей датой создания социальной сети Google+. Специалисты Google+ написали, что они были в Twitter, осматривались и ждали удачного момента, чтобы атаковать.

Люди, управляющие аккаунтом Google+ в Twitter, отличаются хорошим чувством юмора и разумно используют активную социальную платформу, чтобы привлечь внимание к своей собственной. Один из комментариев Google+ гласит: «Там есть еще некоторые люди, которые не знают, насколько хорошо здесь, поэтому мы решили сообщить им об этом. :)»

Является ли это признаком того, что Google решил снова активно продавать свою социальную сеть, пока неизвестно.

В прошлом году основатель Google+ В. Гандотра покинул компанию. Предполагалось, что сеть будет разделена на составляющие части – Фото (Photos), Встречи (Hangouts) и Потоки (Streams). 2 марта текущего года главой социальной сети стал Б. Хоровиц ***(Google+ написал первый твит // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/google_napisal_pervyy_tvit). – 2015. – 8.05).***

***

Instagram запустил новый канал @Music, который предназначен для презентации музыкантов и исполнителей сообществу социальной сети.

По данным компании, 25 % самых популярных аккаунтов в Instagram принадлежат музыкантам. С момента запуска в 2010 г., платформа стала для

артистов инструментом продвижения и коммуникации, а для фанатов – источником новостей и развлечений.

Аккаунт @Music будет обновляться один раз в день со вторника по воскресенье. Его контент будет включать краткие анкеты музыкантов и исполнителей и серии редакционных материалов, включая 15-секундные музыкальные уроки. Помимо привлечения внимания к популярным артистам, так называемым «сливкам» музыкального сообщества, ведущей целью канала будет продвижение новых и ранее незамеченных талантов.

«Один из фокусов нашего внимания – это зарождающиеся таланты, которые посредством платформы делятся своей музыкой и историями уникальным способом», – отметил А. Зюскинд, музыкальный редактор в Instagram.

Создавая эксклюзивный редакционный контент, Instagram надеется стать «конечным пунктом назначения» для любителей музыки, предлагая им всю необходимую информацию об артистах. Кроме того, компания также хочет усилить свою позицию в качестве важнейшего союзника для исполнителей и музыкальных лейблов.

В настоящее время пользователи в среднем используют около 21 мин в день на приложение. Instagram надеется увеличить эту цифру, предлагая высококачественный редакционный контент на специализированных каналах.

«Если мы поможем нашим пользователям найти эти замечательные аккаунты, это значительно обогатит их опыт в Instagram», – сказал глава по вопросам музыкального партнёрства Instagram Д. Халл.

Instagram – не единственная социальная сеть, которая пытается усилить популярность музыкальной индустрии. В 2013 г. Twitter запустил #Music – канал для музыкальных фанатов и одноименное музыкальное приложение. Однако пользователи не проявили особого интереса ни к приложению, ни к аккаунту, и компания вынуждена была свернуть это направление спустя всего лишь полгода после запуска.

По словам представителей Instagram, у них другой подход к @Music: «Это не новый продукт. Мы всего лишь расширяем ту отличную работу, которую уже проделало наше сообщество» ***(Instagram запускает музыкальный канал @Music // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/instagram_zapuskaet_muzykalnyy_kanal_music). – 2015. – 8.05).***

***

LinkedIn объявил о запуске панели аналитики для издателей.

Компаниям предлагаются стандартные метрики, такие как количество просмотров, комментарии, лайки и расшаривания постов. Также в панели будут отображаться пользователи, которые взаимодействовали с постом, демографические данные о читателях, разбивка по географии, отраслям, должностям и источникам трафика, пишет Marketing Media Review (http://mmr.ua/news/id/linkedin-zapustil-analitiku-dlja-izdatelej-44267/).

Новая функция LinkedIn облегчит постановку и корректировку целей издателей, поможет им отслеживать трафик и стимулировать его в случае необходимости. Также издателям будет легче вовлекать и благодарить людей, читающих, лайкающих и комментирующих их работу ***(LinkedIn запустил аналитику для издателей // Marketing Media Review (http://mmr.ua/news/id/linkedin-zapustil-analitiku-dlja-izdatelej-44267/). – 2015. – 8.05).***

***

Приложение Facebook тестирует внутреннюю поисковую систему по ключевому слову, которая позволяет найти сайты и статьи для добавления в обновления статуса, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-testiruet-poisk-ssylok-vnutri-prilozhenija-44279/).

Рядом с кнопками добавления фотографий или информации о местоположении некоторые пользователи iOS увидели новую опцию «Добавить ссылку». В результате запуска запроса Facebook показывает список подходящих ссылок, которыми пользователь, возможно, захочет поделиться. Кроме ссылок, пользователю доступен предварительный просмотр сайтов и возможность добавить сайт в статус одним касанием. Результаты сортируются по степени популярности сайтов среди других пользователей, выделяя на первые места выдачи сайты, опубликованные недавно значительным количеством пользователей.

Представители Facebook подтвердили запуск нового способа добавлять ссылки в сообщения и комментарии. Тестовая версия доступна небольшой группе пользователей в США. В Facebook утверждают, что индексируют более триллиона сообщений для поиска ссылок. При этом поисковая система не пользуется данными Google.

Когда функция станет доступна всем пользователям, это позволит им избежать необходимости поиска в Google или пролистывания новостной ленты Facebook для поиска ссылки, которой они хотят поделиться. Кнопка «Добавить ссылку» может заставить пользователей размещать больше новостей и другого контента. Это не только заполнит ленту новостей контентом, рядом с которым можно расположить рекламу, но и создает структурированные данные об интересах пользователей и их друзей ***(Facebook тестирует поиск ссылок внутри приложения // Marketing Media Review (http://mmr.ua/news/id/facebook-testiruet-poisk-ssylok-vnutri-prilozhenija-44279/). – 2015. – 11.05).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Міністерство культури України зареєструвало нові сторінки у популярних соціальних мережах Twitter та Facebook.

Як повідомляє прес-служба відомства, 22 квітня запрацював Twitter аккаунт @MinCult_ua. З 4 травня працює англомовна сторінка Мінкультури у Facebook.

«Для графічного оформлення сторінок Мінкультури обрано твори всесвітньо відомої художниці М. Примаченко. Так, для фотографії профілю в Facebook обрано картину "Наша армія, наші захисники"», – ідеться у повідомленні.

Підтримуватиме діяльність аккаунтів Міністерства культури України у соцмережах його прес-служба.

Нині у Twitter-аккаунті міністерства 158 твітів, читає його 58 користувачів. Англомовна сторінка у Facebook має 26 фоловерів.

Донині офіційну сторінку Мінкульту у Facebook вели лише українською мовою. Діяв також Twitter-аккаунт віце-прем'єр-міністра, міністра культури В. Кириленка ***(Міністерство культури розширює присутність у соцмережах // Телекритика (http://osvita.mediasapiens.ua/web/social/ministerstvo_kulturi_rozshiryue_prisutnist_u_sotsmerezhakh/). – 2015. – 5.05).***

***

Днями в социальной сети Facebook создали группу для сбора информации о сепаратистах, проживающим на территории Херсонской области.

«Каждая война рано или поздно заканчивается. Но тех "героев", которые поехали "расширять русский мир" с помощью оружия, нужно знать в лицо. Потому что они еще вернутся, и будут пытаться жить среди нас с вами. Собственно, для того чтобы не забыть кто есть кто и создана эта маленькая база данных», – пишет администратор группы.

Пока собрана информация только о трех «героях», двое из них – каховчане, знакомые местным жителям по биг-борду.

«Они хотят в твоем городе войны. Если вам что-либо известно о каховских сепаратистах, вступайте в группу и делитесь информацией», – пишет издание «Каховские новости» ***(На Facebook разыскивают сепаратистов Херсонщины // ХЕРСОН Онлайн (http://khersonline.net/novosti/obschestvo/39001-na-facebook-razyskivayut-separatistov-hersonschiny.html). – 2015. – 28.04).***

***

Нещодавно в соціальній мережі «ВКонтакте» у групі «Типова Олександрія» було запущене опитування на тему: «Оберіть кандидата в мери, якого ви підтримали б». Переважна більшість користувачів проголосувала за С. Кузьменка.

Усього в опитуванні взяло участь 1035 користувачів, що відповідає параметрам ґрунтовного соціологічного дослідження. Але, звичайно ж, порівнювати голосування в соціальних мережах та опитування різних поколінь на вулиці нерозумно. Утім, увагу на результати звернути варто.

Більшість користувачів хотіли б бачити в кріслі мера голову Кіровоградської ОДА С. Кузьменка (27,4 %). Друге місце в опитуванні зайняв діючий міський голова С. Цапюк – 18,3 %. Третє місце посів місцевий бізнесмен М. Лавренко (15 %). Ще 19,7 % респондентів мають свій варіант кандидата, якого немає в запропонованих кандидатах ***(Констатація факту: олександрійці не бажають бачити Кузьменка головою ОДА? // akulamedia.com (http://akulamedia.com/konstatatsija-faktu-oleksandriitsi-ne-bazhajut-bachiti-kuzmenka-golovoju-oda-fotofakt). – 2015. – 29.04).***

***

Канадские разработчики выпустили медицинское приложение для социальной сети обмена видеозаписями и фотографиями Instagram.

Приложение Figure 1 позволяет докторам-пользователям iPhone и Android обмениваться изображениями на медицинскую тематику – внешними симптомами болезни, ранами и т. д.

Предполагается, что таким образом врачи смогут получить консультацию от своих коллег со всего мира, и более точно поставить диагноз, или выбрать максимально правильный курс лечения.

Функции приложения Figure 1 в целом повторяют возможности Instagram, с поправкой на специфику – например, все фильтры для фотографий отключены, как и отметки Like.

Пользователи, зарегистрировавшись в приложении, могут выкладывать картинки, получать и оставлять комментарии, а изображения можно вносить в закладки.

Присоединиться к сервису может любой пользователь, однако делать какие-то заметки и комментарии – только медицинский персонал, который верифицировался у администраторов сервиса.

Подтверждение врачебного статуса происходит в двустороннем порядке: пользователь должен предоставить доказательства того, что он практикующий врач, а администрация, связавшись с медицинским учреждением в котором он работает, получает соответствующее подтверждение.

Сервис для обмена фотографиями уже используют для получения выгоды и бизнесмены. Ранее американские предприниматели нашли способ коммерциализирвать сервис Instagram ***(Медицинское дополнение для***

Instagram позволит врачам консультироваться друг с другом // Блог Imena.UA (http://www.imena.ua/blog/instagram-figure-1/). – 2015. – 28.04).

***

Кількість ладижинців, які використовують український інтерфейс соціальної мережі «ВКонтакте» вперше перевищила російськомовний сегмент.

Про це повідомляє у своєму блозі дослідник А. Лопата.

«Півроку тому публікував схожу мапу українська vs російська у “ВКонтакте”. За півроку вирішив оновити дані», – пише А. Лопата.

Згідно з даними досліджень, за цей проміжок часу серед користувачів російської соцмережі в Ладижині українська мова інтерфейсу почала домінувати.

Аналогічна ситуація, за твердженням автора, спостерігається також у Білій Церкві, Обухові, Узині, Фастові (Київська область), Новоград-Волинському, Овручі (Житомитроська область), Золотоноші, Каневі та Чигирині (Черкаська область), Зінькові, Кобеляки, Пирятині (Полтавська область), Ічні (Чернігівська область).

«Усюди, включно з Кримом, державна мова демонструє постійне зростання. За півроку українська переважатиме у Житомирі та Черкасах, а за рік-два і у Києві, а також з’являться перші міста на південному сході, які підкорить українська (смт. Березнегувате Миколаївська обл.). Загалом серед молоді кількість профілів з українською вже переважає над російською і в Києві, і в Черкасах», – відзначає автор дослідження ***(Все більше ладижинців переходять на українськомовний інтерфейс у «Вконтакті» // Lada.FM (http://lada.fm/2015/05/06/vse-blshe-ladizhincv-perehodyat-na-ukrayinskomovniy-nterfeys-u-vkontakt.html). – 2015. – 6.05).***

***

Патриарх Кирилл призывал священников активнее проповедовать в соцсетях. Православная миссия должна осуществляться в социальных сетях более активно, считает патриарх Московский и всея Руси Кирилл.

«Мы не имеем права не быть там, где есть или может быть наша паства, а наша паства сегодня в том числе и в социальных сетях, причем самая активная часть нашей паствы», – сказал патриарх, выступая 29 апреля в Москве на заседании Высшего церковного совета Русской церкви.

По словам предстоятеля, жизнь современного человека во многом сосредоточена в социальных сетях, «которые для некоторых становятся универсальным, но далеко не самым достоверным и глубоким источником информации».

«И если у нас вызывает неудовлетворение реакция паствы на какие-то события, в том числе церковной жизни, то возникает вопрос, а что мы сделали для того, чтобы не было этой реакции, насколько мы активны в разъяснении позиции Церкви, в участии в обсуждении актуальных проблем?» – сказал он.

Как подчеркнул патриарх, Церковь является хранительницей евангельских ценностей, и ее задача заключается в том, чтобы на понятном современному человеку языке доводить эти ценности до сознания людей.

При этом он указал на то, что виртуализация человеческой жизни таит в себе опасность, особенно в том случае, когда виртуальный мир начинает вытеснять мир реальный.

«И это особенно опасно в юношеском детском возрасте. Если ребенок, не отрываясь, сидит у своего гаджета и занимается чем-то, что не связано с реальностью, то хотим мы или не хотим, но формируется неправильное отношение к реальности. Потому что наиболее интересным им и комфортным становится виртуальный мир», – отметил патриарх Кирилл.

«Таинство спасения осуществляется в реальной жизни. И поэтому если мы не хотим, чтобы виртуальная реальность стала тоже атеизированным таким явлением, мы должны будем серьезно думать о том, как Церковь сегодня может присутствовать в этом мире более эффективно, более надежно с точки зрения передачи миру и особенно молодежи своего послания», – сказал предстоятель ***(Патриарх: священники должны быть поактивнее в соцсетях // Newsland (http://newsland.com/news/detail/id/1538258/). – 2015. – 29.04).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Правила успешного продвижения в Instagram

С ростом аудитории социальных сервисов возрастает и их роль как рекламных каналов. Но, как и любой инструмент, маркетинг в социальных сетях требует навыков и знания целого ряда правил и особенностей работы, пишет Marketing Media Review (http://mmr.ua/news/id/pravila-uspeshnogo-prodvizhenija-v-instagram-44156/).

Возьмем, к примеру, социальную сеть для обмена изображениями Instagram. Исследования показали, что уровень конверсии этого рекламного канала составляет обычно от 10 до 30 %, в зависимости от качества контента и от точности попадания в целевую аудиторию. Это означает, что пользователь, подписавшийся или поставивший «лайки» на 1000 профилей пользователей, может получить в ответ от 100 до 300 подписчиков на свой аккаунт.

Но для того, чтобы добиться такой эффективности, недостаточно просто размещать какие-то фотографии в Instagram и лайкать всех подряд – нужно делать это с умом, следуя правилам продвижения продуктов и услуг в Instagram.

1. Публикуйте только самое лучшее

Чтобы привлечь внимание целевой аудитории, необходимо тщательно подходить к выбору изображений продукта. Постить нужно только самое

лучшее. Если в настоящий момент подходящего изображения нет, лучше вообще отказаться от публикации, вместо того, чтобы засорять свою ленту тем, что подвернулось под руку.

2. Составляйте контент-план на несколько дней вперёд

Как и любой маркетинговый канал, реклама в Instagram требует плана. Об акциях, скидках и мероприятиях компании нужно сообщать заранее, а не в день их проведения. Кроме того, публикации материалов должны быть регулярными, не следует допускать длительных перерывов и пауз, чтобы у целевой аудитории не остыл интерес к вашим продуктам (компании).

3. Используйте теги правильно

Одним из основных заблуждений начинающих пользователей и некоторых псевдо-экспертов в SMM – убеждение, что фотографию обязательно «метить» популярными тегами, чтобы якобы показать эти фото большему количеству пользователей.

Следует помнить, что с помощью #тегов пользователи в первую очередь ищут фотографии и аккаунты в соответствии своим интересами. От релевантности выдачи при поиске по тегу и от качества самого контента, в большой степени зависит, подпишется ли человек на ваш аккаунт или нет. Поэтому используйте только те теги, которые действительно относятся к содержанию вашей публикации.

Кроме того, соответствие #тегов содержанию страницы будет способствовать повышению #доверия к вам.

А вот #нагромождение#из#множества#бесполезных#тегов#под#вашими #фото#выглядит#глупо#и#совсем#не#читается#Много#тегов будет не только подчеркивать вашу некомпетентность и отпугивать случайных посетителей вашего аккаунта, но и раздражать ваших подписчиков, которые желают видеть у себя в ленте только качественные изображения.

4. Описывайте фотографии кратко и понятно

Старайтесь быть лаконичными в описании своих изображений. Не стоит утяжелять его излишними мелкими подробностями. В то же время, информация о продукте или услуге должна быть понятной и, по возможности, исчерпывающей.

5. Не засоряйте свою ленту «откровенной» рекламой

Чрезмерная реклама может отпугнуть пользователей, стремящихся узнать что-то новое и интересное, поэтому не следует каждый день публиковать рекламные посты. Вместо этого, добавляйте в свою ленту интересные и «живые» фотографии, чтобы ваши подписчики видели, что аккаунтом управляет живой человек. Это укрепит ваши связи с клиентами, повысит их лояльность к вам и вашей компании.

6. Уделяйте внимание комментариям

Работа с комментариями под постами в любой социальной сети, включая Instagram, очень важна для удержания аудитории и конвертирования её в клиентов. Главным предназначением социальных сервисов остаётся общение, поэтому общайтесь, делитесь полезной информацией, задавайте вопросы своим

пользователям, дарите подарки, давайте скидки за упоминание вас с вашим тегом.

Следует также удерживаться от рассылки бессодержательных комментариев или спама, вроде «Класс!», «Круто!», «Шикарно!», «Здорово!», «Заходи ко мне в профіль, у меня много интересного!». Это с большой долей вероятности приведёт к тому, что ваш аккаунт будет забанен большинством получателей спама, а в итоге, с большой вероятностью, будет забанен и сам источник спама.

7. Правило трёх постов

Да, это банальное правило, но не стоит забывать, что ваш аккаунт – не единственный на кого подписаны пользователи, и не следует засорять ленту только вашими постами. Настройте отложенный постинг или делайте сами по 2–3 поста в день (утро-день-вечер) – этого более чем достаточно ***(Правила успешного продвижения в Instagram // Marketing Media Review (http://mmr.ua/news/id/pravila-uspeshnogo-prodvizhenija-v-instagram-44156/). – 2015. – 28.04).***

***

Социальные сети могут рассказать о потенциальном заемщике больше, чем иные документы – считают в некоторых западных компаниях. Что может быть интересно банку в вашем профиле в сети и в каком случае он может это использовать – узнавал Prostobank.ua.

Впервые западные компании начали изучать профили клиентов в социальных сетях четыре года назад. Среди пионеров – Lenddo из Гонконга. Эта компания построила модель анализа данных, которая включала более 12 тыс. пунктов, собранных на основе информации из мобильных приложений, электронной почты и социальных сетей. На основе этой модели клиенту присваивали кредитный рейтинг.

Другой подход выбрала три года назад немецкая компания Kreditech: при построении кредитного рейтинга заемщика она подробно анализировала покупки клиента на американских Amazon и eBay.

Сегодня подобный подход используют в западных странах все чаще. В Украине пока такой подход в новинку. «В системе скоринга банка социальные сети не рассматриваются как источник релевантной информации», – ответили Prostobank.ua в пресс-службе одного крупного банка.

Однако сама идея может оказаться полезной для скоринга – считают некоторые банкиры. «Профиль заемщика в социальной сети вполне можно использовать для оценки кредитоспособности и принятия решения о выдаче займа, но только как дополнительный способ сбора информации.

Кроме того, объем информации, которую банк может получить, ограничен личными настройками доступа, а информация не всегда отражает реальное положение дел», – говорит В. Марынченко, начальник отдела кредитования физических лиц АгроКомБанка.

По мнению В. Марынченко, по страничке потенциального заемщика в соцсети можно установить настоящее состояние дел человека. Действительно: если раньше банки во время принятия решения о выдаче кредита принимали во внимание чеки на крупные покупки, которые он совершал, то сегодня подобную информацию вполне можно почерпнуть из соцсетей.

«В основном, можно выбрать информацию по значимым параметрам, таким как пол, возраст, увлечения, кто его родственники, чем они занимаются, количество друзей и кто они. Интересно, что профиль в соцсетях теоретически позволяет увидеть то, что напрямую говорит о кредитоспособности человека: с помощью какого устройства заходит в Интернет, на каких курортах и в каких странах проводит отпуск», – отмечает эксперт.

Если подобный подход к анализу надежности заемщика станет распространенным среди украинских банков, то его будут использовать для нецелевых кредитов наличными на небольшие суммы. По ипотеке и автокредитам существенного значения профили в социальных сетях иметь не будут.

«Скорее всего, профиль в соцсетях может приниматься во внимание при выдаче потребительских кредитов, так как при получении таких кредитов банк запрашивает минимум документов и требует минимальную информацию о заемщике. Но все равно, профиль заемщика в соцсети рассматривается как вспомогательный инструмент и не значительно влияет на принятие решения по выдаче кредитов», – говорит В. Марынченко ***(Банки могут оценивать заемщика через социальные сети // Днепропетровская Панорама (http://dnpr.com.ua/content/banki-mogut-ocenivat-zaemshchika-cherez-socialnye-seti). – 2015. – 30.04).***

***

Новое биометрическое исследование показало, что традиционные ТВ-ролики превосходят видеорекламу на Facebook по вовлечению в четыре раза, пишет Marketing Media Review (http://mmr.ua/news/id/issledovanie-tv-roliki-bolee-effektivny-chem-videoreklama-na-facebook-44200/).

Бостонская компания Innerscope Research использовала биометрический мониторинг, метод отслеживания взгляда и традиционные методы исследования, чтобы изучить бессознательные и сознательные реакции 390 потребителей от 18 до 34 лет. Участникам показывали одни и те же ролики в Facebook, на ТВ и диджитал пре-роллы на ПК, планшетах и смартфонах.

Биометрические данные включали в себя колебания в сердечном ритме, характер дыхания и электропроводность кожи.

Компания также отметила, что у зрителей повышалось внимание при финальном обозначении продукта и появлении лого бренда в ТВ-рекламе, что возможно является результатом больше экрана, чем при просмотре онлайн роликов в качестве пре-роллов на любом девайсе.

47 % пользователей отметили, что сразу же пропускали или игнорировали видео рекламу на Facebook до ее просмотра.

25 % потребителей отметили, что попробовали или купили бы бренды после просмотра роликов на ТВ по сравнению с 9 %, которые посмотрели эти ролики на Facebook.

Innerscope отметил, что небольшие экраны являются большим фактором в более низком воздействии видео рекламы, а визуальное внимание, затраченное на лого, тэглайны и брендинг продукта, уменьшается с размером экрана.

Лучший результат взаимодействия с видео рекламой на малых экранах приходится на начало рекламы, эмоциональное вовлечение достигает пика в первые три-пять секунд. Компания советует брендам создавать яркие смелые копии рекламных сообщений с ранним брендингом продуктов для небольших экранов.

Исследования показали, что потребители по-разному воспринимают и имеют разные ожидания от различных медиа платформ ***(Исследование: ТВ-ролики вызывают больше вовлечения, чем видеореклама на Facebook // Marketing Media Review (http://mmr.ua/news/id/issledovanie-tv-roliki-bolee-effektivny-chem-videoreklama-na-facebook-44200/). – 2015. – 30.04).***

***

В марте 35 % рекламных видеороликов брендов было просмотрено в Facebook, сообщается в отчёте агентства по контент-маркетингу Visible Measures. Однако в долгосрочной перспективе преимущество – на стороне YouTube. Об этом пишет searchengines.ru.

При этом в отчёте Visible Measures акцентируется внимание на том, что каждая из платформ имеет свои сильные стороны, которые отлично подходят под стратегии брендов.

В частности, Facebook лучше работает на старте видеокампании, благодаря обширному охвату и более высокой вовлечённости пользователей, что позволяет максимально быстро получить первые результаты.

В YouTube этот процесс занимает более длительное время, но в долгосрочной перспективе он выигрывает у Facebook.

К этим выводам аналитики Visible Measures пришли, изучив 82 видеокампании, запущенные брендами в марте и выбранные в случайном порядке. В общей сумме они сгенерировали 437,5 млн просмотров в системе True Reach агентства. YouTube опережает Facebook по количеству просмотров в соотношении 65–35 % соответственно.

Не все бренды используют Facebook для дистрибуции видео.

В 53 кампаниях видео публиковались напрямую в Facebook. В 33 % кампаний Facebook опережает YouTube по общему количеству просмотров, включая видеоролик #LikeAGirl от Always. Эта реклама получила 4,2 млн просмотров в Facebook и только 478 тыс. в YouTube.

С другой стороны, видео Air France собрало 49 млн просмотров в YouTube и только 57 тыс. в Facebook

В любом случае, Facebook имеет тенденцию к снижению количества перепостов видео с течением времени, как выявилось в ходе исследования

Visible Measures. С быстрым ускорением просмотры видео в Facebook достигали 85 % от общего числа просмотров в первую неделю после запуска кампании. Видео в YouTube получили 63 % просмотров в первые семь дней, но в, конечном итоге, опередили видео в Facebook.

Полученные результаты отражают природу каждой платформы, считает основатель и исполнительный директор Visible Measure Б. Шин. Он отметил, что очень сложно найти видеоролики в Facebook, после того, как они больше не транслируются в новостной ленте.

«Преимущество Facebook – в быстром продвижении трендового контента, в то время как YouTube остаётся платформой для продолжающихся просмотров».

Напомним, что о конкуренции между YouTube и Facebook за видео брендов в отрасли заговорили ещё в прошлом году.

Как показали данные SocialBakers за декабрь 2014 г., большинство брендов загружают видео в Facebook, минуя YouTube. Быстрый рост использования Facebook брендами для размещения видео наблюдался еще в октябре 2014 г. Нативные загруженные видео в Facebook догнали YouTube по количеству сообщений и превзошли с точки зрения взаимодействия.

По данным апрельского прогноза рекламной компании Mixpo, в этом году Facebook обгонит YouTube в качестве ведущей платформы видеорекламы. 87 % маркетологов планируют проводить рекламные видеокампании в Facebook, 81,5 % – в YouTube. Представленные данные получены путём опроса 125 агентств, брендов и издателей видеоконтента ***(YouTube превосходит Facebook по просмотрам видео брендов в долгосрочной перспективе // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43295/118/lang,ru/). – 2015. – 5.05).***

***

Twitter заключил соглашение о партнёрстве с DoubleClick Google и приобрёл кроссэкранную платформу ретаргентинга TellApart.

Впервые об этом стало известно во время отчёта о финансовых результатах Twitter за I квартал 2015 г. Оба шага компании направлены на предоставление маркетологам, работающим с Twitter, возможностей для более эффективных кроссэкранных измерений и атрибуции.

Партнёрство с DoubleClick даст рекламодателям Twitter возможность отслеживать конверсии, произошедшие в результате просмотров или других действий в Twitter. Они также смогут покупать продвигаемые твиты через платформу DoubleClick Bid Manager. Этот функционал будет запущен позже в этом году и позволит рекламодателям увидеть, какую отдачу приносит реклама в Twitter.

«В настоящее время потребители постоянно перемещаются между приложениями, устройствами и платформами. Нам нужны модели измерений, которые берут это поведение в расчёт. Для того чтобы рекламодатели понимали

путь конверсии покупателя, который проходит через несколько устройств и платформ, системы измерений должны выйти за пределы традиционных моделей атрибуции. Мы хотим, чтобы рекламодатели обладали информацией не только о кликах, которые осуществляются в рамках платформ, подобных нашей (т. е. ретвиты), но и о других действиях покупателей, и о той роли, которую они играют в определении ROI кампаний», – пояснил старший директор по продакт-менеджменту Twitter А. Ранадив.

Приобретение кроссэкранной платформы ретаргетинга TellApart направлено на улучшение рекламного функционала сервиса микроблогов, в частности рекламы прямого отклика. Tell Apart предоставляет ритейлерам и компаниям, работающим в сфере e-commerce, возможности кроссэкранного таргетинга посредством динамических товарных объявлений и email-маркетинга.

Пока этот функционал доступен лишь ограниченному числу компаний. В будущем руководство Twitter намерено расширить услуги TellApart на другие страны и отрасли.

Напомним, что на днях Twitter огласил финансовые результаты за I квартал 2015 г. После отчёта акции компании подешевели на 18 %. Этому предшествовала утечка данных о более низких доходах Twitter в отчётном квартале, чем ожидалось аналитиками ***(Twitter вступил в партнёрство с DoubleClick и приобрёл платформу ретаргетинга TellApart // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/internet_reklama/novosti/twitter_vstupil_v_partnyorstvo_s_doubleclick_i_priobryol_platformu_retargetinga_tellapart). – 2015. – 6.05).***

***

IBM и Facebook объединились, чтобы улучшить свои продукты и стимулировать персонализированные кампании в социальной сети и на других digital каналах, пишет Marketing Media Review (http://mmr.ua/news/id/ibm-obedinilis-s-facebook-dlja-predostavlenija-personalizirovannoj-reklamy-44238/).

Первоначальный фокус союза состоит в объединении данных: инсайты Custom Audience Facebook становятся доступными для брендов, которые используют Marketing Cloud IBM для управления своими кампаниями.

У Facebook простой мотив: платформа хочет, чтобы реклама в сети стала более полезной для ее членов. «Для нас очень важно предоставить потребителям более релевантную рекламу», отметил вице-президент по партнерству для Facebook.

Со своей стороны IBM надеется, что союз даст компаниям еще одну причину использовать приложения Marketing Cloud, а не решения от конкурентов, таких как Adobe, Marketo или Salesforce. Marketo объявил о похожем альянсе с LinkedIn в середине апреля ***(IBM объединились с Facebook для предоставления персонализированной рекламы // Marketing Media Review (http://mmr.ua/news/id/ibm-obedinilis-s-facebook-dlja-predostavlenija-personalizirovannoj-reklamy-44238/). – 2015. – 6.05).***

***

Facebook запустил «глубокие ссылки» (deep linking) в рекламе установки приложений. Нововведение позволит рекламодателям направлять пользователей на конкретные страницы приложений, где они смогут приобрести виртуальные товары или получить информацию. Ранее «глубокие ссылки» были в рекламе, продвигающей ранее установленные приложения, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-glubokie-ssylki-v-reklame-ustanovki-prilozhenij-44272/).

Разработчики Facebook отметили, что «глубокие ссылки» помогут пользователям сразу найти интересующую их информацию, пропустив несколько ненужных шагов. К примеру, если в туристическом приложении демонстрируется реклама установки приложения, рассказывающая об отпуске в Сан-Франциско, пользователи, которые установят приложение и откроют его, будут перенесены прямо на страницу с информацией о поездке в Сан-Франциско.

Подробнее о функционале «глубоких» ссылок можно узнать в блоге для разработчиков ***(Facebook запустил глубокие ссылки в рекламе установки приложений // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-glubokie-ssylki-v-reklame-ustanovki-prilozhenij-44272/). – 2015. – 8.05).***

***

4 совета от команды Facebook в сфере кросс-платформенной рекламы.

Размещение рекламных материалов в Facebook чаще интересует бизнес-пользователей, чем рядовых потребителей. Именно для них маркетологи социальной сети приготовили несколько полезных рекомендаций по настройке кросс-платформенных рекламных кампаний, пишет Marketing Media Review (http://mmr.ua/news/id/4-soveta-ot-komandy-facebook-v-sfere-kross-platformennoj-reklamy-44261/).

Как рекламировать товары и услуги реальным потребителям на разных устройствах с помощью Facebok

Проблема:

Обычная реклама в Интернете основана на учёте cookies, но точность такого отслеживания не слишком высока. Если рекламные переходы осуществляются с компьютера в общественном месте (интернет-кафе, учебное заведение) либо пользователь постоянно заходит на один и тот же сайт между ПК, планшетом и смартфоном – бюджет на рекламу вы тратите впустую.

Решение:

Таргетинг стоит осуществлять по ряду критериев, а не только лишь по файлам cookies.

Один из лучших способов провести кампанию эффективно – инструмент Custom Audiences (он помогает идентифицировать конкретных пользователей на определённых страницах). Для мониторинга можно использовать

устанавливаемый пиксель, который фиксирует переходы с конкретного типа устройств при кросс-платформенном маркетинге.

Что надо попробовать:

Для проверки эффективности ретаргетинга настройте инструмент Custom Audience.

Как персонализировать пользовательский опыт для уже существующих клиентов

Проблема:

У каждого бизнеса есть покупатели, находящиеся на разных стадиях маркетингового цикла продукта. Есть покупатели-новички, есть «ранние последователи», есть те, кто покупает только в период распродажи, те, кто покупает только с мобильных устройств или заказывает время от времени и многие другие. Каждой группе потребителей надо показывать конкретную рекламу с самым высоким уровнем релевантности.

Решение:

Для начала стоит упорядочить свою базу электронных адресов согласно сегментации аудитории. Затем используйте Custom Audience для сопоставления аудитории соцсети с группами подписчиков. Каждый пакет рекламных объявлений должен по частоте показов и содержимому рекламы совпадать с ожиданиями потребителя (равно как с тем каналом / платформой, где показывается реклама).

Что стоит попробовать:

Добавьте инструмент Conversion Pixel к любой странице, по которой надо отследить конверсию, затем создайте для каждого сегмента аудитории конкретное объявление и свяжите с пикселем конверсии.

Как снизить стоимость поиска новых покупателей в Facebook

Проблема:

Поиск новых лидов, соответствующих конкретному рекламному объявлению, без необходимости выбросить на поиск весь бюджет.

Решение:

Новых потенциальных покупателей можно определить за счёт моделирования аудитории по критериям поведенческой оценки. Алгоритм социальной сети вычислит тех, кто подпадает под смоделированный портрет аудитории.

Что стоит попробовать:

Моделирование аудитории с инструментом Similarity Match позволит составить разные профили и получить по ним прогнозируемую конверсию, а затем отобрать тот сегмент, который обладает наиболее высокой потенциальной способностью к покупке.

Как автоматизировать и оптимизировать отслеживание конверсии по рекламе в Facebook

Проблема:

Отслеживание покупок – ключевая задача, которую трудно решить, если один и тот же покупатель использует сразу несколько устройств для доступа.

Решение:

Используйте пиксель отслеживания конверсии для трекинга взаимодействий между стартовым кликом и совершением покупки. Facebook – единственная платформа, которая отслеживает конверсии по всем устройствам и позволяет понять, с помощью какого именно устройства совершена покупка. Также можно автоматически оптимизировать рекламу для показа её только тем, кто наиболее склонен совершить покупку.

Что стоит попробовать:

Оптимизируйте CPM, дав возможность Facebook автоматически определять величину ставки по кампании. Для этого используйте инструмент Website Conversions. Система отберёт самые высокие показатели показов по вашим ключевым целям в рамках заданного бюджета. В результате возрастет ROI по рекламной кампании чем бы вы ни пользовались – показателем CPC или CPA ***(4 совета от команды Facebook в сфере кросс-платформенной рекламы // Marketing Media Review (http://mmr.ua/news/id/4-soveta-ot-komandy-facebook-v-sfere-kross-platformennoj-reklamy-44261/). – 2015. – 8.05).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Аналитики ресурса StudyWeb опубликовали исследование, которое проливает свет на самые серьёзные виды цифровой зависимости.

Специалисты подметили большую часть социальных, культурных, эмоциональных и интеллектуальных эффектов постоянной «подключённости».

Одной из главных цифровых зависимостей современного человека является невозможность оторваться от собственного телефона. По результатам исследования, более 17 % людей проверяют сообщения даже во время еды.

Другой традиционной проблемой, согласно выводам StudyWeb, оказалась игромания. На сегодняшний день на планете Земля зависимость от игр имеют даже около 9 % детей.

На жизнь человека имеет слишком серьёзное влияние нездоровое увлечение социальными медиа. Среднестатистический американец только в Facebook проводит около 40 минут ежедневно.

В Великобритании подсчитали, что современные дети проводят у монитора примерно 25 % свободного времени. Если предположить, что человек смотрит на экран ещё 40 часов, что составляет минимальную рабочую неделю,

то процент времени, проведённого перед монитором, увеличивается с 25 % до 49 % ***(Специалисты назвали вредные цифровые привычки, которые мешают работать // Блог Imena.UA (http://www.imena.ua/blog/studyweb-6-bad-digital-habits/). – 2015. – 29.04).***

***

Facebook, Twitter и другие соцсети стали серьезной угрозой браку, пишет The Daily Mail со ссылкой на новое исследование. По словам юристов, теперь социальные сети являются фактором во все большем количестве дел о разводе.

Выяснилось, что один из семи находящихся в браке респондентов задумывался о разводе из-за постов супруга или супруги в Facebook или на других онлайн-сайтах. Столько же опрошенных признали, что ищут в Интернете доказательства неверности партнера. Каждый пятый сообщил, что ежедневно ссорится со своей второй половиной из-за использования мужем или женой социальных сетей.

Исследование проводилось транснациональной юридической фирмой Slater and Gordon. Все большее число клиентов этой компании заявляют, что Facebook, Skype, Snapchat, Twitter, What'sApp и другие соцсети сыграли свою роль в разводе. «Пять лет назад Facebook редко упоминался в контексте расторжения брака, но теперь это типичный случай. Социальные сети стали новым минным полем для брака», – заявил Э. Ньюбери из Slater and Gordon ***(Facebook и Twitter стали серьезной угрозой браку // InternetUA (http://internetua.com/Facebook-i-Twitter-stali-sereznoi-ugrozoi-braku). – 2015. – 3.05).***

***

Ученые общественного исследовательского университета США в Хьюстоне во время нового исследования выяснили, что пользователи социальной сети Facebook склонны к депрессии.

Результаты исследования ученых Хьюстонского университета, опубликованные в Guilford Press, доказывают, что пользователи популярной социальной сети страдают от депрессивных расстройств чаще, чем те, кто не имеет собственного профиля в Facebook.

По данным исследователей, всему виной радостные события в жизни друзей в социальной сети – яркие фото из отпуска, новости о свадьбе, а также фотографии нового автомобиля способствуют развитию депрессивных состояний и неуверенности в себе. Им также удалось выяснить, что мужчины страдают от Facebook-депрессии чаще, чем женщины.

«Facebook дает возможность узнать о тех моментах в жизни наших друзей, о которых мы обычно не знаем, вследствие чего происходит оценка уровня жизни и, иногда осознанно, а иногда нет, мы начинаем проводить сравнительный анализ. Невозможно контролировать импульс "сравнивать". В большинстве своем пользователи Facebook публикуют посты о радостных событиях из своей жизни, что побуждает человека думать, что его жизнь не так

прекрасна, как жизнь его друзей в социальной сети», – говорят авторы исследования ***(Facebook вызывает депрессию // Весь Харьков (http://all.kharkov.ua/news/science/facebook-vyzyvaet-depressiu.html). – 2015. – 5.05).***

***

Исследование, проведенное учеными, продемонстрировало, что люди, читающие ленту Facebook, сами замыкаются в своих убеждениях и остаются в собственном информационном пузыре.

Исследование ученых Мичиганского университета было опубликовано в журнале Science. Согласно ему, пользователи в большинстве своем получают новостную ленту, которая соотносится с их политическими и жизненными взглядами и замыкает их в своеобразном информационном пузыре.

Таким образом, согласно исследованию, проведенному среди более чем 10,1 млн пользователей самой популярной в мире социальной сети Facebook, алгоритмы выдачи информации соотносятся с той точкой зрения, которой придерживаются пользователи.

В итоге это не позволяет им взглянуть на многие ситуации с альтернативной позиции.

Исследование проводилось следующим образом: ученые отбирали все ссылки на серьезные материалы и делили их на более либеральные и консервативные в зависимости от того, кто их чаще публиковал – те, кто считает себя либералом или консерватором. В дальнейшем они отслеживали их пути распространения и рассматривали, насколько часто эти ссылки появлялись в ленте у людей с альтернативной точкой зрения и как часто те, кто не был согласен с опубликованными материалами, делились ими.

В конце концов по результатам исследования ученые пришли к тому, что если вы либерал, то у статьи от консерваторов шансы попасть к вам в ленту новостей на 8 % меньше.

В свою очередь, если вы консерватор, то либеральная статья имеет на 5 % меньше вероятности попасть в ваш кругозор.

Например, примерно 23 % из того, что распространяют либералы, относится к контенту, присущему консервативным пользователям. Видят либералы 22 % из противоположного им, а кликают только на 20 % из увиденного в ленте, то есть консервативный лишь каждый пятый клик у либералов.

В свою очередь, у консерваторов из публикуемого контента на либеральный приходится 34 %, при этом видят они 31 %, а кликают на 29 %. Это говорит о том, что консерваторы немного, но более открыты к альтернативным суждениям, нежели либералы.

Более того, в дальнейшем это приводит к тому, что люди сами начинают кликать на то, что им по душе, и алгоритмы формирования ленты новостей автоматически оптимизируются на выдачу близкой к мировоззрению пользователя информации.

Таким образом, как показало исследование, пользователи даже в большей мере сами замыкаются в своем круге интересов, нежели это делает за них Facebook. Если говорить о конкретных примерах, то либералы чаще публикуют у себя ссылки на Huffington Post, а консерваторы – на Fox News. И в итоге эти пользователи и видят публикации от соответствующих ресурсов чаще, чем от других. И алгоритмы работы новостной выдачи Facebook здесь уже не имеют большой власти.

Но в любом случае примерно 25 % контента, который показывает социальная сеть своим пользователям, в той или иной мере идет вразрез с их убеждениями.

Впрочем, это исследование нельзя называть на 100 % репрезентативным: в нем отслеживалось поведение только тех пользователей, которые в ясной мере декларировали свои политические взгляды. Таковых, как уточняют ученые, набралось всего около 9 %.

Исследование показало, что люди склонны сами тяготеть к замыканию в собственном информационном мирке, а алгоритмы формирования ленты новостей Facebook лишь помогают им в этом ***(Исследование продемонстрировало, что лента Facebook замыкает людей в своих убеждениях // InternetUA (http://internetua.com/issledovanie-prodemonstrirovalo--csto-lenta-Facebook-zamikaet-luadei-v-svoih-ubejdeniyah). – 2015. – 10.05).***

***

Некоторые самые популярные социальные сайты заполнены изображениями очень худых женщин, которые могут быть вредны для тех, кто их рассматривает, считают исследователи Калифорнийского университета в Дэвисе. Изображения часто обрезаются, чтобы удалить голову или сосредоточиться только на некоторых частях тела.

Докторант Д. Газнави и доцент Л. Тейлор из Департамента коммуникаций исследовали около 300 фотографий из Twitter и Pinterest с метками «тонкий», «худой», которые поощряют чрезмерную худобу и показывают пищевые расстройства в положительном свете.

Их статья «Кости, части тела и сексуальная привлекательность: анализ изображений в популярных социальных медиа» была недавно опубликована в «Изображения тела: Международный журнал исследований».

Исследователи признают, что неоднократные просмотры таких изображений могут привести к неудовлетворенности своим телом и расстройствам пищевого поведения.

«Молодая женщина, рассматривающая эти изображения, может подумать, что она должна выглядеть так же, – сказала Д. Газнави. – Это может подтолкнуть девушек и женщин прибегать к строгим диетам, чрезмерным физическим нагрузкам или другим крайним мерам для достижения тонкого идеала» ***(Социальные сети приводят к анорексии // Newsland (http://newsland.com/news/detail/id/1542754/). – 2015. – 11.05).***

Бесплатная Tesla каждому дозвонившемуся, взрывы в Белом доме и ранение Б. Обамы, уход Д. Медведева, планы атаки Пентагона на Китай – все это может быть легко принято за чистую монету и растиражировано по всему миру благодаря взлому официальных аккаунтов в Twitter.

Очередная халатность и пренебрежение двухфакторной авторизацией (когда ввод пароля к аккаунту дополняется подтверждением по SMS) снова привели к нездоровому ажиотажу в Интернете. На этот раз жертвой «розыгрыша» стал известный производитель электромобилей Tesla. Неизвестные взломали сайт, корпоративную почту и официальный Twitter-аккаунт компании и разместили там сообщение, что каждый дозвонившийся по некоему мобильному номеру получит электромобиль Tesla бесплатно. Аудитория Twitter Tesla из 564 тыс. подписчиков мгновенно распространила новость. Блогер rootworx, чей номер был указан в объявлении, получал пять звонков в минуту.

На запрос СМИ к представителю пресс-службы Tesla также ответил взломщик и заверил журналистов, что аккаунт не был взломан. После восстановления контроля над официальным Twitter компании хакеры взломали аккаунт Э. Маска, руководителя Tesla, и разместили аналогичное объявление от его имени.

Аудитория Twitter самого Э. Маска насчитывает уже 1,9 млн подписчиков.

Следует отметить, что взлом Twitter Tesla далеко не первое резонансное хулиганство в сети. До сих пор такие случаи носили нарочито грубый и показной характер, и даже при этом они умудрялись не только наделать шуму, но и нанести вполне ощутимый вред. Если же подобный взлом будет использован в рамках профессионально спланированного воздействия в рамках кибервойны, последствия могут быть куда серьезнее. Достаточно вспомнить аналогичные взломы официальных аккаунтов в социальных сетях последних двух-трех лет.

Так, в январе 2015 г. активисты группировки «Киберджихад», принадлежащие к ИГИЛ, взломали официальные Twitter-аккаунты Пентагона и центрального военного командования США и разместили угрозы в адрес американских военнослужащих, подкрепив их скриншотами ведомостей и других документов, похищенных с серверов американского ведомства.

Также были опубликованы схемы якобы сценариев военных действий на территории Китая и Северной Кореи, однако, по счастью, они и без детального изучения выглядели любительскими.

После этого инцидента меры безопасности в американском военном ведомстве были пересмотрены.

Еще одним громким событием стал взлом Twitter-аккаунта новостного агентства Associated Press, в котором была размещена информация о взрывах,

прогремевших в Белом доме, и ранении президента США Б. Обамы. Агентство опровергло публикацию и сообщило, что ответственность за взлом взяла на себя «Сирийская электронная армия». Результатом скандала стало падение американских биржевых индексов.

В России взломщики в августе 2014 г. дискредитировали в Twitter председателя правительства РФ Д. Медведева. От его имени в социальной сети были размещены сообщения о том, что он якобы испытывает стыд за последние действия правительства, ужесточение правил доступа к публичному Wi-Fi и другие изменения законодательства и покидает свой пост. Пресс-служба премьера сообщения в Twitter опровергла.

Также от имени Д. Медведева неизвестные подписались на Twitter Навального, «Шалтая-Болтая» и радио Anonymous.

В августе 2012 г. в Twitter от имени фальшивого аккаунта министра внутренних дел России В. Колокольцева со ссылкой на российского посла в Дамаске было размещено сообщение о смерти президента Сирии Б. Асада. Информация об этом была распространена СМИ. В результате ложного сообщения возросла цена на нефть, которая не опустилась даже после опровержения информации представителями МВД РФ.

Социальные сети являются наиболее благодатной средой для распространения дезинформации. Например, Facebook позволяет редактировать заголовок и текстовое превью новости при репосте, при этом сохраняются источник и иллюстрация, что делает подделку очень похожей на настоящую. Однако ложная информация может получить широкое распространение и через другие веб-сервисы с генерируемым пользователем контентом. Так, во время обострения вооруженного конфликта на Донбассе неоднократным правкам подвергались материалы в Wikipedia.

Еще одним примером может служить уязвимость в функции Map Maker компании Google, которая позволяет добавлять информацию на Google Maps.

Пользователи разместили через нее изображение с оскорблением в адрес конкурента, компании Apple, на территории Пакистана, чтобы продемонстрировать слабость модерации контента в Google.

Представители корпорации, разумеется, пообещали разобраться с ситуацией.

Приложения для социальных сетей и мобильные приложения, которых с каждым днем все больше и больше размещается в официальных магазинах программного обеспечения, могут стать еще одним каналом распространения ложной информации. Несмотря на достаточно строгую фильтрацию и проверку, команда модераторов, которая зачастую даже не находится в соответствующей стране, не может быть осведомлена обо всех нюансах. Таким образом, поддельное мобильное приложение, использующее чужое название и фирменное оформление, успешно может распространяться на мобильных платформах ***(Как пробелы в компьютерной безопасности становятся источником сенсаций // InternetUA (http://internetua.com/kak-probeli-v-kompuaternoi-bezopasnosti-stanovyatsya-istocsnikom-sensacii). – 2015. – 28.04).***

***

Программный механизм Facebook вводит пользователей в заблуждение, заставляя их делиться записями других людей. Об этом пишет The Daily Dot.

По словам автора издания Т. Хетмейкер, с проблемой она столкнулась, просматривая новостную ленту Facebook. Решив оставить комментарий под одним из постов, она ввела текст и нажал клавишу ввода. Однако вместо публикации комментария система «расшарила» запись в ее хронике.

«Я не собиралась делиться этим постом, поэтому мне пришлось отправиться в свой профиль и удалить оттуда запись. Ситуация повторилась еще два раза, прежде чем я поняла, в чем дело», – отмечает Т. Хетмейкер.

По ее словам, форма комментария в ленте новостей при попытке ввести текст автоматически меняется на форму для «расшаривания» поста. Теперь обозреватель The Daily Dot вынуждена открывать каждую запись, оставлять под ней комментарий, а затем возвращаться в ленту новостей.

Какое количество пользователей Facebook столкнулось с подобным поведением системы, неизвестно. Представители соцсети пока не комментировали случившееся ***(Facebook уличили в обмане пользователей // InternetUA (http://internetua.com/Facebook-ulicsili-v-obmane-polzovatelei). – 2015. – 6.05).***

***

Исследователи компании Trustwave, занимающейся вопросами безопасности в сети, зафиксировали использование вредоносного ПО в целях пророссийской пропаганды.

Неизвестные хакеры используют набор эксплоитов Angler, заражающий системы трояном Bedep, для увеличения количества просмотров пророссийских пропагандистских видеороликов.

Вирус попадает в систему, когда пользователь посещает скомпрометированный сайт, предлагающий помощь туристам. Зловред направляет жертве набор эксплоитов Angler, который загружает троян Bedep.

До недавних пор вредоносное программное обеспечение использовалось чтобы заставлять инфицированные системы посещать сайты для генерирования дохода от размещённой на них рекламы и мошеннического трафика.

Теперь же вирус занялся «накруткой» просмотров роликов политической пропаганды. В основном вирус накручивает просмотры в роликах о боевых действиях на Донбассе и о санкциях, введённых западными странами в отношении РФ.

Ранее украинские энтузиасты собственными силами запустили ресурс TrolleyBust.com, который призван отслеживать и блокировать источники антиукраинской пропаганды.

Сайт предоставляет волонтёрам простой и доступный набор инструментов для поиска в сети учётных записей пользователей, которые распространяют в социальных сетях антиукраинскую пропаганду ***(Хакеры***

начали использовать набор эксплоитов Angler для политической пропаганды // Блог Imena.UA (http://www.imena.ua/blog/angler-propaganda/). – 2015. – 5.05).

***

Издание «Зеркало недели. Украина» пишет, что Кремль использует кибератаки для вывода из строя инфраструктуры на Западе (http://zn.ua/WORLD/hakery-stali-moschneyshim-oruzhiem-rossii-newsweek-175329_.html).

В жаргоне хакеров существует понятие эффекта «от кибернетического к физическому». Это означает способность хакера влиять на реальный мир с помощью инструментов в виртуальном. И часто это влияние носит деструктивный характер.

Американцы и израильтяне были пионерами такого влияния. В 2009 г. они с помощью вируса Stuxnet обнаружили компьютерные сети Ирана и вывели из строя сотни центрифуг, которые использовались для обогащения урана. Но теперь другие крупные игроки тоже пытаются вступить в игру и использовать компьютерные сети для уничтожения инфраструктуры и влияния на человеческие жизни. И главными игроками кроме США сегодня стали Россия и Китай.

Об этом пишет журнал Newsweek, который посвятил кибернетическому оружию России следующий свой номер. Издание опубликовало обложку нового выпуска, изобразив на ней символическую «ядерную бомбу» с флагом России в виде «флешки».

В прошлом году, согласно отчету Федеральной службы информационной безопасности Германии, в неназванном городе произошел взрыв на металлургическом заводе после того, как неизвестный хакер вывел из строя систему контроля. Это же самое чуть ли не случилось в США в начале 2014 г., когда из-за кибератаки на одном из предприятий были выведены из строя системы подачи топлива и воды.

Издание пишет, что западные газеты посвящают свои материалы и первые полосы «старомодным» и отсталым хакерам, которые взламывают почтовые серверы Белого дома, Госдепартамента, Пентагона и компании Sony Pictures. Но чиновники в Вашингтоне серьезно нервничают из-за появления таких киберпреступников, которые способны добиться эффекта «от кибернетического к физическому».

«Это не предположения», – уверяет адмирал Службы национальной безопасности США М. Роджерс, добавив, что страна постоянно переживает атаки хакеров, которые «получают миллиарды долларов за это».

Эксперт из Гарвардской школы управления и главный исследователь Центра стратегических исследований в Гааге А. Климбург говорит, что кибернетическое пространство сегодня «напоминает Европу в 1914 г., когда Первая мировая война была готова разгореться, а правительства не осознавали этого».

Согласно отчетам разведки США, в 2015 г. Россия и Китай стали самыми значительными игроками-государствами в новейшем кибернетическом противостоянии. И российские хакеры имеют значительное преимущество, учитывая их изобретательность, серьезную подготовку и навыки программировать.

«Угроза от Китая велика, но деятельность России недооценена. Россияне значительно лучше подготовлены технически. Собственно, мы считаем, что российские хакеры-наемники были задействованы в атаке на компанию Sony», – сказал Д. Карр – глава компании Taia Global, которая занимается вопросами информационной безопасности.

В прошлом году японская компания стала жертвой кибератак после выхода фильма о диктаторе КНДР Ким Чен Ыне.

«Даже когда Sony потеряли 80 % потенциала своих сетей, хакеры продолжали активно действовать. Это демонстрирует очень высокий уровень технической подготовки», – сказал Д. Карр.

Причастность к таким атакам России очень беспокоит Запад, поскольку это единственная страна, которая сегодня пытается сочетать кибернетические удары с реальным наступлением танков.

«Российско-грузинская война 2008 г. замечательный пример сочетания реального наступления с кибернетическим. Никто никогда такого не делал», – добавил эксперт.

Издание пишет, что во время оккупации Крыма прошлого года наземная военная операция сопровождалась большим количеством очень технологически сложных кибератак против сетей правительств Украины и Польши, а также против систем Европарламента и Европейской комиссии. Большинство этих кибернетических нападений были попыткой взять контроль над сетями с помощью вируса Black Energy, а также DDoS-атаками.

«Вирус Black Energy широко использовался российскими хакерами для DDoS-атак на банковские системы с целью краж. Но он получил новое применение против сетей правительств и частных компаний, которые работают в разных отраслях», – пояснил эксперт Агентства по вопросам защиты сетей и информации ЕС П. Паганини.

Главной из наибольших загадок для правительства США остается то, как обнаружить личность и цель хакеров, которые устраивают новые виды атак, призванных нанести урон в реальном мире. Но роль России в современных кибернетических схватках не подлежит сомнению. Американские прокуроры называют российские и украинские группы хакеров ответственными за самые крупные киберпреступления за всю историю США. Они взламывали счета таких компаний, как J. C. Penney, JetBlue и французского ритейлера Carrefour, похитив более 300 млн дол. А в прошлом году российские хакеры похитили личные данные пользователей Apple iTunes Store, Netflix, Amazon.com, ESPN.com, а также сайта издания Wall Street Journal. Также они взломали сеть NASA.

А в феврале стало известно о том, что крупнейшая российская компания, которая занимается кибербезопасностью «Лаборатория Касперского» сама организовала атаки на 100 банков в Украине, Японии, США и по всей Европе в 2013–2014 гг.

Это привело к реальным финансовым потерям на сумму около 900 млн дол. «Это кибернетическая преступность на производственных рельсах. В одном из случаев, который произошел в Киеве, хакеры сделали так, чтобы банкомат разбрасывался деньгами. А прохожие подбирали», – рассказал изданию неназванный эксперт по информационной безопасности из Москвы, добавив, что киберпреступники стараются не выдать своих методов, чтобы жертвы не смогли залатать дыры в защите своих систем. В это же время, определить связь Кремля с хакерами, которые устраивают вредные для инфраструктуры атаки, очень сложно. Поскольку граница между преступлением ради наживы и по политическим мотивам очень тонкая.

Эксперты говорят, что для атак против правительственных и банковских систем хакеры ищут пробелы в коде популярных программ и добавляют к ним алгоритмы вирусов, которые потом откроют доступ к компьютерным сетям и дадут инструменты влияния.

Сотни «черных» хакеров в России зарабатывают на жизнь тем, что выполняют киберпреступления на заказ «банкиров в Швейцарии или украинских олигархов».

«Тех, кого в России поймали, ставят перед выбором работать на ФСБ или сесть за решетку. Кроме того, ФСБ нанимает таких экспертов по контракту», – рассказал Д. Карр.

Существуют серьезные доказательства того, что российские киберпреступники работали на правительство России во время атаки против Эстонии в 2007 г. Однако теперь существуют подозрения, что Кремль всерьез взял на вооружение такие методы воздействия, – считает директор ЦРУ Д. Карпентер.

По его мнению, правительство России финансирует исследования и разработку кибертехнологий мирового класса, вкладывая деньги в развитие специальных исследовательских центров при политехнических университетах в Санкт-Петербурге и Самаре. Издание пишет, что эксперты в Вашингтоне засекли группу российских хакеров под названием APT28, которые устроили несколько атак против США. Есть доказательства, которые указывают на связи киберпреступников с Кремлем.

В компании FireEye рассказали, что хакеры APT28 действуют исключительно в часы, когда в России рабочее время. Кроме того, их коды вирусов содержат русскоязычные эпизоды, что указывает на то, что сами хакеры, скорее всего, разговаривают на русском языке.

Главным доказательством связи APT28 с российским правительством эксперты считают то, против кого хакеры устраивают атаки. В частности, их жертвами становились сети министерства обороны Грузии, правительств

Польши и Венгрии, НАТО, ОБСЕ, Вооруженных сил Норвегии и американских военных.

«Они не занимаются кражей интеллектуальной собственности, которая бы могла иметь коммерческую выгоду, но зато собирают данные для разведки. И это наиболее выгодно именно для правительства», – пояснили в компании FireEye.

Эксперты говорят, что хакеры APT28 обладают одинаковыми знаниями и применяют похожие тактики. В их российском происхождении уже никто не сомневается.

«Их спонсирует российское государство, возможно их поддерживает российское правительство. Вероятно они работают в разных дивизиях одной кибернетической армии», – считает эксперт П. Паганини ***(Хакеры стали мощнейшим оружием России – Newsweek 7 мая в 11:03 // Зеркало недели. Украина (http://zn.ua/WORLD/hakery-stali-moschneyshim-oruzhiem-rossii-newsweek-175329_.html). – 2015. – 7.05).***

***

Почему Facebook обманывает и пользователей, и рекламодателей

Издание Pando Daily опубликовало материал, в котором выразило сомнения в достоверности недавно проведённого Facebook исследования о влиянии алгоритмов на формирование новостной ленты пользователя и призвало компанию перестать прикрываться принципом People First.

7 мая 2015 г. Facebook представила результаты внутреннего исследования компании, которое показало, что сами пользователи социальной сети изменяют свою ленту активнее, чем алгоритмы фильтрации новостей – запрещая показывать новости от конкретных пользователей или компаний или другими способами.

Исследование проводилось в преддверии выборов в Соединённых Штатах Америки и должно было показать, каким образом посетители социальной сети получают новости и насколько алгоритмы, которые применяет Facebook, ограничивают поступление сообщений в ленту пользователей. Как отмечает издание Pando Daily, это действительно важный вопрос – ведь, по данным Facebook, 88 % поколения миллениалов получают новости в основном из социальной сети.

Результаты исследования были опубликованы в научном журнале Science. Однако Pando Daily считает, что назвать это научным исследованием сложно – скорее это проплаченная PR-акция, единственная цель которой – показать Facebook в лучшем свете.

В документе, представленном аналитиками компании, сделан вывод о том, что алгоритмы формирования ленты новостей хоть и влияют на то, какие новости получает пользователь, но гораздо меньше, чем выбор самого посетителя сети.

На самом деле ответственность за то, почему пользователи получают так мало политических новостей, лежит на них самих, считают исследователи. Они,

в большинстве своём, не склонны оценивать политику – и поэтому Facebook сложно понять, какие политические новости показывать.

Социальная сеть не может предположить, что пользователю понравится какая-то заметка о консерваторах, если в его профиле указано, что он придерживается либеральных взглядов, и если он не «лайкает» записи друзей-консерваторов.

Если это действительно так, отмечает редактор Pando Daily, это говорит совсем не в пользу Facebook – социальной сети, которая стремится заменить журналы и новостные агрегаторы в традиционном понимании, взяв на себя ответственность за то, чтобы пользователь получал полное представление о картине дня. Однако компания фактически признаётся в неспособности это сделать.

Кроме того, считает автор заметки, базу исследования и многие из выводов, сделанных в его ходе, вряд ли можно назвать научными. Так, исследователи выяснили, что после запуска алгоритма формирования новостной ленты пользователи, придерживающиеся консервативных взглядов, начали получать на 5 % меньше политических новостей, а те, кто относит себя к либералам, – на 8 % меньше.

Возможно, это и не такие большие цифры, как мы ожидали. Однако они, несомненно, показывают, что алгоритмы всё же оказывают существенное влияние на формирование новостной ленты.

Но исследователи, по словам Pando Daily, предпочитают игнорировать этот факт, концентрируя внимание читателей на том, что выбор пользователя играет большую роль в формировании новостного потока.

По данным компании, друзья пользователей социальной сети, которые относят себя к либералам, оценивают лишь 24 % консервативных новостей, которые получают, а друзья консерваторов – лишь 35 % либеральных новостей. Ещё хуже, по мнению аналитиков, то, что новостями, которые учитывают взгляды обеих сторон, либералы делятся лишь в семи случаях из 100, а консерваторы – в 17 случаях из 100.

О ненаучности проведённого исследования говорят, по мнению автора, и другие факторы: «Я не очень доверяю заключениям аналитиков Facebook – как сообщает профессор одного из американских университетов К. Сэндвиг, Facebook проанализировала страницы только тех пользователей, которые в явном виде указали свои политические взгляды. Это всего лишь 4 % всех зарегистрированных в Facebook пользователей».

Для такого специфического исследования, считает Pando Daily, база должна включать в разы больше людей. Иначе оно не отражает реальное положение дел – каким бы на самом деле оно ни было.

Кроме того, по мнению редактора издания, в некоторых моментах аналитики Facebook сами себе противоречат.

Facebook не хочет признать, что контролирует ленту пользователя

Facebook, как отмечает Pando Daily, действительно могла бы стать основным местом потребления новостей для многих пользователей – если бы

отказалась от своего принципа People First и начала серьёзно контролировать новостную ленту – фильтровать спам, отсеивать повторяющиеся новости, уделять больше внимание материалам, которые отражают несколько точек зрения – а не пытаться подбирать такие, которые понравятся посетителю.

Однако для Facebook принцип People First всё ещё остаётся если не определяющей стратегией, то хорошим прикрытием от нападок – например, именно с помощью этой формулировки М. Цукерберг «обороняется» от претензий брендов по поводу уменьшения охвата публикаций, говорит автор материала на Pando Daily. Хотя на самом деле, считает он, делается это исключительно для того, чтобы вытягивать из компаний деньги на продвижение записей.

Основной доход компании приносят, говорит автор материала, рекламодатели и бренды – и каждое изменение, которое социальная сеть вносит в свои алгоритмы, невинно рассказывая об улучшении пользовательского опыта, призвано лишь увеличить заработки корпорации.

Facebook хочет выглядеть серьёзно в глазах СМИ и журналистских организаций, компании нужно, что бы те приняли её в свои круги. Однако каждый раз, когда речь заходит об изменениях в алгоритмах, Facebook забывает о главной журналистской ценности – честности.

«Facebook будет продолжать использовать неточные данные, чтобы доказать свою правоту», – говорит редактор Pando Daily. Однако методы, которые она использует, совсем не научные – это, по мнению автора, классический PR, и очень занимательно видеть, как такими вещами занимается крупнейшая корпорация, которая пытается казаться серьёзным и авторитетным источником новостей ***(Почему Facebook обманывает и пользователей, и рекламодателей // InternetUA (http://internetua.com/pocsemu-Facebook-obmanivaet-i-polzovatelei--i-reklamodatelei). – 2015. – 11.05).***

Зарубіжні спецслужби і технології «соціального контролю»

Исследователи из США и Ирландии разработали алгоритм обнаружения потенциальных массовых беспорядков на основе открытой статистики операторов мобильной связи.

Программа, разработанная учеными, рассчитывает «обычный» маршрут передвижения определенного человека по данным о его звонках и текстовых сообщениях. И если же значительное количество людей будет двигаться по «необычным» маршрутам, то это может свидетельствовать об акции протеста, забастовке, митинге или иной форме протестного поведения населения.

Эмпирическим основанием для данного исследования стала гражданская война в Кот-д'Ивуаре в 2011–2012 гг., где данных о массовых скоплениях людей было в избытке.

Отслеживать передвижение людей исключительно на основе данных операторов мобильной связи является довольно проблематичным заданием. Во-

первых, люди могут совершать общение по телефону нерегулярно, что затруднит установить их «обычный» маршрут. Во-вторых, геометка привязывается не к точке, где находится абонент, а к ближайшей вышке мобильной связи, поэтому данные о местонахождении человека сбиваются в пространственном измерении.

Однако ученым удалось решить эти проблемы путем разделения абонентов мобильной связи на определенные кластеры. И на основе «необычного» поведения таких кластеров абонентов программа и рассчитывает потенциальное протестное поведение населения ***(Протестное поведение предскажут с помощью мобильных телефонов // InternetUA (http://internetua.com/protestnoe-povedenie-predskajut-s-pomosxua-mobilnih-telefonov). – 2015. – 29.04).***

***

Многие Android-приложения, распространяющиеся на бесплатной основе, активно следят за пользователями путем скрытого взаимодействия с десятками трекинговых сайтов. Они передают самую разную информацию, начиная от текущего места дислокации и заканчивая историей интернет-серфинга.

К такому выводу пришли специалисты компании Eurecam France, протестировавшие более 2000 бесплатных приложений из официального магазина Google Play, к которому имеют доступ все Android-устройства, пишет портал PC World. Подавляющее большинство из них скрыто подключается к значительному числу веб-сайтов, количество которых в общей сложности достигает 250 тыс.

Помимо отправки информации, нечистые на руку бесплатные приложения также могут загружать навязчивую рекламу, которая не была заказана пользователям. Все это приносит выгоду разработчикам такого ПО, но наносит существенный вред владельцу мобильного гаджета.

Для начала, данные о его местоположении отправляются совершенно посторонним людям, что является нарушением целого ряда прав человекам. Но даже если закрыть на это глаза, отправка данных и прием нежелательной рекламы создают большой объем трафика, который при подключении к Интернету через сотовые сети оплачивается самим пользователем.

Специалисты Eurecam France рекомендуют пользоваться только самыми популярными приложениями в Google Play, которые получили высокие оценки от других пользователей. Они также отметили, что Google стала намного тщательнее проверять программы на такого рода скрытые угрозы прежде, чем те попадут в каталог магазина Google Play.

Впрочем, эти проверки не всегда эффективны. К примеру, довольно распространенное на Западе приложение Eurosport Player скрытно подключается к 810 трекинговым сайтам. И таких случаев немало, так что иной раз при работе с мобильным ПО следует отключать Интернет во избежание утечки информации.

Сотрудники Eurecam France в ближайшем будущем выпустят утилиту, которая покажет, какие данные и в каких объемах отправляет каждое установленное на гаджет приложение. Найти ее можно будет все в том же магазине Google Play ***(Бесплатные Android-приложения активно следят за пользователями // InternetUA (http://internetua.com/besplatnie-Android-prilojeniya-aktivno-sledyat-za-polzovatelyami). – 2015. – 6.05).***

***

Турецкая территория закрыта для доступа к интернет-ресурсам YouTube и Twitter.

Согласно имеющейся информации, причиной для принятия такого решения правоохранительными органами и провайдерами является в публикации фотоснимков, на которых запечатлён прокурор из Стамбула М. Кираз, убитый после того, как стал заложником радикалов.

К голове прокурора был приставлен пистолет. В сеть изображения попали усилиями террористов, совершивших преступление.

По словам И. Калына, являющегося представителем президента страны, кое-какие медиагруппы публиковали эти снимки, пропагандируя таким образом организацию боевиков.

Злоумышленники продолжили этим заниматься вопреки всем возражениям. И. Калына отметил, что это недопустимо.

Предполагается, что своим решением прокуратура хотела предотвратить размещение подобных материалов в эфирах и социальных сетях.

Напомним, ранее в Турции уже закрывали доступ к Twitter ***(Туркам перекрыли доступ к соцсетям // Supreme2.Ru (http://supreme2.ru/9593-turkam-perekryli-dostup-k-socsetyam/). – 2015. – 6.05).***

***

Страница главы Государственного комитета по делам межнациональных отношений и депортированных граждан Республики Крым З. Смирнова вновь удалена из сети Facebook.

Об этом рассказал председатель Госкомнаца.

По его словам, в технической службе социальной сети отказываются объяснять причины отключения страницы, несмотря на многочисленные запросы.

«В ответ тишина, никаких сообщений», – отметил З. Смирнов и добавил: «Поэтому у нас есть основания полагать, что это политический заказ, 100-процентный, чтобы лишить нас возможности влиять на информационное пространство, в данном случае, за рубежом, по вопросам освещения межнациональной проблематики в Крыму».

На странице Facebook помощницы главы Госкомнаца З. Алиевой говорится: «Известны случаи, когда создаются фейковые страницы под именем З. Смирнова, поэтому, когда будет зарегистрирован (уже третий по счету) его профиль в Facebook, мы уведомим».

Первый раз страница главы Государственного комитета по делам межнациональных отношений и депортированных граждан РК З. Смирнова была удалена из сети Facebook после опубликования перевода на турецкий язык его интервью под заголовком «Гюленовское лицо провокаций Джемилева» ***(Facebook повторно удалил аккаунт Заура Смирнова // Новости Крыма (http://news.allcrimea.net/news/2015/5/5/Facebook-povtorno-udalil-akkaunt-zaura-smirnova-36206/). – 2015. – 5.05).***

***

Facebook заблокировал пост российского журналиста С. Пархоменко про сбитый из «Бука» Boeing-777 в Донецкой области. Как сообщает Цензор.НЕТ со ссылкой на «Медузу», об этом сообщила главный редактор издательства «Корпус» В. Горностаева.

По мнению С. Пархоменко, пост заблокировали из-за многочисленных жалоб со стороны ботов. С точки зрения журналиста, публикация не нарушала правил сообщества. В социальной сети свое решение заблокировать пост никак не объяснили.

В своей записи С. Пархоменко комментировал заметку в «Новой газете» о докладе неких российских экспертов о том, что «Боинг» сбит украинским «Буком». Пархоменко критиковал Кремль, который путем такой публикации решил признать, что самолет был сбит «Буком».

«Да “Бук”. Конечно. А как же. Мы никогда и не отрицали. Кто ж мог этого не знать. Всем же давно известно. Ясно даже и ежу. И всякий – кто скажет что-нибудь иное, тот “дурак и не на своем месте”. Ну и что? Ну и что, что “Бук” – то? Зато будем теперь сражаться не на жизнь, а на смерть за признание того, что ЭТО НЕ НАШ “Бук”. То есть никаких сбивавших боинг самолетов, которые своими глазами видел М. Леонтьев, – просто не было. Вычеркиваем. Леонтьев нам всем привиделся», – писал С. Пархоменко ***(Facebook заблокировал пост российского журналиста про «Бук» // GlavPost.Com (http://glavpost.com/post/7may2015/Society/31094-facebook-zablokiroval-post-rossiyskogo-zhurnalista-pro-buk.html). – 2015. – 7.05).***

***

В Украине открыли службу экстренной помощи для владельцев заблокированных страниц и Интернете.

Таким образом, украинский кризисный медиа центр и цифровое агентство Plus One DA отреагировали на серию «банов» страниц публичных лиц в Украине. Специалисты объясняют, блокируют аккаунты российские информационные спецподразделения.

«Бан» можно получить даже за цитирование стихотворений Т. Шевченко. Поэтому владельцы заблокированных аккаунтов могут обратиться за помощью по адресу UnBan@uacrisis.org ***(Россияне больше не смогут блокировать аккаунты украинцев в соцсетях // УРА-Информ (http://ura-***

inform.com/ru/society/2015/05/07/rossijane-bolshe-ne-smogut-blokirovat-akkaunty-ukraintsev-v-sotssetjakh). – 2015. – 7.05).

***

Доверие россиян к зарубежным СМИ уменьшилось в семь раз с 2007 г.

По состоянию на май 2015 г., зарубежной прессе верит лишь 6 % россиян. Ещё 7 % ответили «скорее да», а большая часть опрошенных не доверяет им (50 %) или скорее не доверяет (19 %). Об этом пишет tjournal.ru.

Главным источником информации для жителей России является центральное телевидение: так считают 62 % опрошенных. Новостные сайты и социальные сети предпочитают лишь 16 6 % соответственно.

Информации, передаваемой по ТВ, доверяют 43 % населения. На втором месте находится радио (30 %), за ним следуют газеты (29 %), а у региональных ТВ, радио и прессы эти показатели несколько ниже. Сайтам и соцсетям полностью верят лишь 20 и 14 % аудитории.

55 % населения России больше поверят информации с телевидения, если о новости будут говорить противоречивые вещи разные СМИ одновременно. В 2013 г. этот показатель у ТВ составлял 60 %. Уменьшилась роль и новостных сайтов: с 22 % в 2013 г. до 13 % в 2015 г.

Опрос ВЦИОМ проводился 2–3 мая 2015 г. Опрошено было 1600 человек в 130 населенных пунктах в 46 областях, краях и республиках России.

По данным аналитического центра Ю. Левады за 2014 г., 70 % населения России не владели ни одним из иностранных языков. Лучше всех знание иностранных языков показала аудитория 18–24 лет с высшим образованием: среди них английским владело 20–22 % против усреднённых 11 % ***(Доверие россиян к зарубежным СМИ уменьшилось в семь раз с 2007 года // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/43326/118/lang,ru/). – 2015. – 7.05).***

***

Первый крымскотатарский телеканал ATR, прекративший свое вещание с 1 апреля из-за проблем с получением лицензии Роскомнадзора, возобновляет свою работу.

Об этом в Facebook сообщил редактор телеканала Р. Спиридонов.

По его словам, в настоящее время журналисты заканчивают работу над циклом «Дети войны» и документальными фильмами, посвященными трагическим событиям 18 мая 1944 г. – депортации крымских татар.

«Кроме этого, информационная редакция возвращается к своей привычной работе – съемкам новостных сюжетов и спецрепов», – добавил Р. Спиридонов.

Все материалы можно будет увидеть на официальном сайте телеканала.

Напомним, с 1 апреля единственный в мире крымскотатарский телеканал ATR прекратил аналоговое вещание на территории полуострова, так как ему не выдали российскую лицензию. Та же судьба постигла радиостанцию «Мейдан».

Телезрители обратились к президенту РФ В. Путину, премьер-министру России Д. Медведеву и главе Крыма С. Аксенову с просьбой оказать помощь в перерегистрации ATR и не допустить его закрытия.

Генеральный директор канала Э. Ислямова сообщила, что ATR твердо намерен добиваться получения всех необходимых разрешительных и лицензионных документов для возобновления вещания согласно законодательству Российской Федерации. Также коллектив позвал в гости главу Роскомнадзора ***(Крымскотатарский телеканал ATR возобновляет работу в Интернете // Новости Крыма (http://news.allcrimea.net/news/2015/5/7/krymskotatarskii-telekanal-ATR-vozobnovlyaet-rabotu-v-internete-36349/). – 2015. – 7.05).***

***

Необхідність реєструвати кримські ЗМІ відповідно до російського законодавства стала фільтром для виявлення лояльних до самопроголошеної влади Криму медіа. Про це в студії проекту hromadske.tv заявила заступник голови Кримської польової місії з прав людини О. Скрипник.

«Формальні вимоги для реєстрації кримських ЗМІ відповідно до російського законодавства стали певним фільтром, який дозволяє виявити медіа, лояльні до чинної влади», – зазначила вона.

За словами правозахисниці, через скорочення кількості ЗМІ та журналістів, які працюють на півострові, люди починають шукати інформацію в соціальних мережах, проте і за це може загрожувати кримінальна відповідальність.

«Російське законодавство побудовано так, щоб завжи існувала формальна причина обмежити свободу слова», – підкреслила О. Скрипник ***(Реєстрація кримських ЗМІ відповідно до російського законодавства – фільтр лояльності – правозахисниця // MediaБізнес (http://www.mediabusiness.com.ua/content/view/43335/118/lang,ru/). – 2015. – 8.05).***

***

Жителю Черкасской области грозит пять лет тюрьмы за сепаратистские призывы в соцсетях. Мужчина разметил в социальных сетях «ВКонтакте» и Facebook статью, содержащую публичные призывы к вхождению части государства в состав Российской Федерации, сообщили в прокуратуре Черкасской области.

За совершенное преступление подсудимому грозит наказание в виде лишения свободы от 2 до 5 лет ***(Жителю Черкасской области грозит пять лет тюрьмы за сепаратистские призывы в соцсетях // InternetUA***

(http://internetua.com/jitelua-cerkasskoi-oblasti-grozit-pyat-let-tuarmi-za-separatistskie-prizivi-v-socsetyah). – 2015. – 9.05).

***

Федеральный апелляционный суд США 7 мая постановил, что массовый сбор информации о входящих и исходящих звонках американцев Агентством национальной безопасности является незаконным, а объяснения правительством релевантности такой слежки несостоятельными. Об этом сообщает Wired со ссылкой на решение суда.

Панель из трёх анонимных судей постановила, что так называемый «Патриотический акт» (The Patriot Act, закон, регулирующий сбор информации о гражданах США в целях противодействия терроризму) никогда не разрешал поголовной телефонной слежки, как посчитало АНБ.

В прочтении судей «Патриотический акт» может использоваться лишь для целенаправленного расследования в особых случаях, а не для «безлимитной облавы», поясняет Wired. Однако речь идёт не о слежке в Интернете, а о метаданных звонков: например, информация об обращении по горячей линии может раскрыть суицидальные наклонности человека, опыт домашнего насилия, страдание от зависимости и другие личные данные.

Правительство указывает, что существует только одно гигантское «антитеррористическое» расследование, и что любые записи, способные оказаться полезными в развитии любого аспекта этого расследования, релевантны общему делу борьбы с терроризмом.

Требования [АНБ] касаются не только тех записей, что принадлежат подозреваемым, или тем, кто контактирует с такими субъектами, или тем, кто контактирует с тем, кто контактирует с субъектами – они простираются на все существующие записи и даже те, которые ещё не существуют.

Из решения суда

Тем не менее решение суда не означает, что программа слежки АНБ будет немедленно остановлена. Решение апелляционного суда может быть оспорено в вышестоящей инстанции судебной системы США – Верховном суде.

Иск был подан 2 сентября правозащитной организацией American Civil Liberties Union (ACLU) против ряда чиновников высшего уровня: главы АНБ, директора национальной разведки, генпрокурора, министра обороны США и директора ФБР. Он последовал за разоблачениями бывшего сотрудника ЦРУ Э. Сноудена, которые он впервые предал огласке летом 2013 г.

Впервые ACLU обратилась в нижестоящий суд в 2013 г., однако тогда их иск отклонили. Теперь суд средней инстанции признал то решение недействительным, а программу телефонной слежки – незаконной.

Решение апелляционного суда предваряет предстоящее слушание в Конгрессе США по тому, стоит ли реформировать «Патриотический акт», которое состоится 1 июня. Конгрессмены всё ещё могут в явной форме разрешить АНБ собирать массивы данных о гражданах страны и оставить всё в

прежнем виде, однако эксперты считают, что постановление суда сделало реформу практически неизбежной. Кроме того, по словам судей, многие конгрессмены даже не были в курсе существования программы слежки ***(Федеральный суд США признал массовую телефонную слежку АНБ незаконной // InternetUA (http://internetua.com/federalnii-sud-ssha-priznal-massovuua-telefonnuua-slejku-anb-nezakonnoi). – 2015. – 8.05).***

***

В сети появился сервис Transparency Toolkit, который, по словам разработчиков, содержит информацию о 27 тыс. работников разведслужб США. При этом базу набирали не благодаря каким-то утечкам информации из этих организаций. Разработчики сервиса просто детально проанализировали базу данных LinkedIn, стараясь выявлять работников разведслужб по разного рода секретным кодовым словам (правда, некоторые из них известны определенным кругам специалистов) и некоторым другим параметрам. Некоторые пользователи LinkedIn открыто публикуют название конторы, на которую они работают, сообщает IT Expert со ссылкой на Geektimes.

Авторы проекта хотели показать обычным людям, насколько много среди нас людей, которые работают на разведслужбы (естественно, не все сотрудники разведслужб являются разведчиками, тем не менее, таких сотрудников довольно много).

Сам сервис очень простой и позволяет без проблем искать нужную информацию.

Кроме LinkedIn, разработчики задействовали для своей работы и другие ресурсы, для уточнения и дополнения информации по людям, которые попали в Transparency Toolkit. Это известные социальные сети и некоторые другие источники из сети. Вся информация, которую использовали разработчики – общедоступна, и собрать нечто подобное, при желании, несложно (конечно, при наличии некоторых навыков работы с информацией и анализом данных) ***(LinkedIn «засветила» 27000 сотрудников разведслужб США // IT Expert (http://itexpert.org.ua/rubrikator/item/41846-linkedin-zasvetila-27000-sotrudnikov-razvedsluzhb-ssha.html). – 2015. – 8.05).***

Проблема захисту даних. DDOS та вірусні атаки

Неизвестные хакеры пытались похитить конфиденциальные данные высокопоставленных госслужащих украинского правительства.

Хакерскую шпионскую кампанию, получившую название Operation Armageddon, обнаружили специалисты по безопасности в сети из компании Lookingglass. Неизвестные хакеры похищали секретные данные украинского правительства. В Lookingglass отмечают, что деятельность неизвестных хакеров продолжалась не менее двух лет.

Название Operation Armageddon было взято из документов Word, которые злоумышленники использовали во время атаки. По мнению исследователей, использование фишинговых уловок лишь подтверждает, что «сами атаки не были сложными».

Первая активность Operation Armageddon была зафиксирована в середине 2013 г. Целились злоумышленники в украинское правительство, региональные отделения правоохранительных органов и некоторых высокопоставленных военнослужащих. Характер похищаемой информации не уточняется. Ранее активисты анонимной хакерской организации «Шалтай-Болтай» выложили в сеть расшифровку перехваченных записей телефонных разговоров руководящих лиц двух крупных банков РФ ***(Неизвестные хакеры 2 года шпионили за украинским правительством // Блог Imena.UA (http://www.imena.ua/blog/operation-armageddon/). – 2015. – 30.04).***

***

Как сообщают исследователи безопасности из Google, они провели полномасштабный анализ недавней DDoS-атаки на организации GreatFire и GitHub. В рамках нападения неизвестные злоумышленники прибегли к использованию китайского программного обеспечения, известного как «Великая Пушка».

Указанное ПО позволяет внедрить вредоносные пакеты в незашифрованный трафик «Великого китайского файрвола» путем осуществления MitM-атак. К примеру, во время атак на GitHub и GreatFire злоумышленники подменяли HTML и JavaScript элементы, размещенные на общественных страницах интернет-магазина Baidu.

Выяснить подробности атаки специалисты Google смогли благодаря собственной корпоративной инфраструктуре Safe Browsing, продублировавшей нападение. Такой подход позволил выяснить, что неизвестные начали вводить первые вредоносные инъекции кода еще 3 марта этого года.

Интересно также, что в первый день количество перенаправляемых запросов было ограничено, однако в период с 4 по 6 марта, это ограничение было снято.

Второй этап, по данным Google, начался 10 марта и закончился 13 марта. Во время этой фазы исследователи зафиксировали лишь один IP-адрес, связанный с sinajs.cn доменом. В течение следующих дней атакующие пытались провести аналогичные манипуляции с порталом cloudfront.net ***(Google проанализировал китайскую «Великую Пушку» для DDoS-атак // InternetUA (http://internetua.com/Google-proanalizirovaI-kitaiskuua--velikuua-pushku--dlya-DDoS-atak). – 2015. – 28.04).***

***

Конференция по цифровой безопасности RSA прошла в Сан-Франциско и принесла с собой неприятную новость. Apple стала настоящей «антизвездой»

этого мероприятия: её продукты не так хорошо защищены, как принято считать.

В презентации компании Skycure, занимающейся безопасностью мобильных устройств, её главный инженер Я. Амит и CEO А. Шарабани предоставили подробные данные об уязвимости, которую специалисты компании недавно обнаружили в iOS 8.

Я. Амит: Однажды во время исследований для демонстрации сетевой атаки мы приобрели новый роутер. После его настройки для функционирования в особом режиме и подключения к нему гаджетов, мы с нашей командой увидели, как некоторые приложения внезапно вылетают. Вскоре другие люди тоже стали замечать вылеты. Довольно быстро мы поняли, что эта ошибка воспроизводится только на iOS.

Насколько серьёзна эта проблема

Skycure копнули глубже и поняли, что это больше, чем просто вопрос качества ПО. Компания проанализировала случаи вылетов приложений и нашла источник проблемы. Ошибку удавалось воспроизвести в приложениях, которые используют при обмене данными протокол безопасности SSL: их можно было заставить «вылететь», просто сгенерировав особый SSL-сертификат. О проблеме сообщили в Apple.

Я. Амит: мы быстро написали скрипт, который использовал обнаруженную нами уязвимость по всей сети. SSL – это лучшее, что можно использовать для безопасности передачи данных, и почти все приложения из App Store его используют, поэтому возможностей для атаки оказалось очень много. Мы понимали, что любая задержка в выпуске патчей для этой уязвимости может нанести сильный удар бизнесу, ведь организованная атака на определённые сервисы приведёт к большим финансовым потерям.

Исследование Skycure показало, что уязвимость с тем же успехом действует не только в отдельных приложениях, но и на iOS в целом.

Я. Амит: при интенсивном использовании устройства, подверженного атаке, операционная система также вылетает.

Более того, команде Skycure удалось создать условия, при которых устройства отправлялись в бесконечный цикл перезагрузки, и становились совершенно непригодными к использованию.

Сложный для Apple месяц

Ситуацию прокомментировал Л. Темз, специалист по безопасности Tripwire – компании, занимающейся продвинутой защитой от подобных угроз:

«Риски, связанные с этой уязвимостью, касаются мобильных устройств, а iOS-устройства легко подключаются к небезопасным Wi-Fi-сетям при минимальном контроле со стороны пользователя. Физически обойти или покинуть зону действия точки доступа Wi-Fi – не самый изящный способ избежать последствий этой уязвимости, но возможно, единственный».

К. Янг, другой специалист по безопасности Tripwire, считает, что апрель стал «месяцем уязвимостей» для Apple. К примеру, две недели назад представители компании Е. Касперского рассказали, что специально

построенный IP-пакет может послужить причиной вылетов различных версий iOS и OS X.

Однако не стоит беспокоиться и раньше времени бить тревогу, подыскивая альтернативы любимой ОС. Проблемы iOS – наименьшие на мобильном рынке, и не идут ни в какое сравнение с тем, что творится у конкурентов ***(iOS 8 стала жертвой серьёзной уязвимости SSL // InternetUA (http://internetua.com/iOS-8-stala-jertvoi-ser-znoi-uyazvimosti-SSL). – 2015. – 28.04).***

***

Письмо, распространенное через почтовую рассылку Open Source Software Security (oss-security), которая обеспечивает сопровождение клиентского кода для работы с беспроводными сетями в ОС Android, Linux, BSD Unix и Windows, содержит срочное исправление дефекта, позволяющего «обваливать» устройства и даже вводить в их память вредоносные программы. Эти атаки производятся через специально сфабрикованное имя в одноранговой (P2P) беспроводной сети.

Дефект защиты открыт командой специалистов по информационной безопасности компании Alibaba. Он до некоторой степени напоминает Heartbleed тем, что не контролирует должным образом длину данных SSID, получаемых от однорангового устройства. Однако новая уязвимость позволяет хакеру не только считывать содержимое памяти за пределами 32 байт, отведенных для OpenSSL, но и записывать туда свои данные. В результате возникающего переполнения фиксированного буфера происходит переписывание нескольких переменных, включая указатель, и еще примерно 150 байт произвольного кода может быть размещено вне пределов резервированной памяти.

В итоге такой атаки, повреждение информации в памяти может привести к сбою в работе wpa_supplicant и сервиса Wi-Fi. Подставной SSID может использоваться для организации DDoS-атак, например, простой рассылкой ответов на запросы Wi-Fi. Он также способен извлекать содержимое памяти в ходе трехстороннего подтверждения подключения в одноранговой сети (GO negotiation) или позволять выполнять код на атакуемом устройстве.

По большей части эти дефекты трудно использовать, если целевое устройство не работает активно с беспроводными P2P-соединениями. Соответствующий патч, по всей вероятности, вскоре станет частью обновления системы Android. Однако то, как скоро его получат конечные пользователи, будет зависеть от производителей смартфонов и провайдеров сотовых сервисов ***(Программная недоработка открывает смартфоны для атак через Wi-Fi // InternetUA (http://internetua.com/programmnaya-nedorabotka-otkrivaet-smartfoni-dlya-atak-cserez-Wi-Fi). – 2015. – 28.04).***

***

Специалисты компании «Доктор Веб» обнаружили новые версии Android-троянцев семейства Android.BankBot, атакующих клиентов банков множества стран.

Некоторые модификации этих троянцев, известные также под именем Svpeng, опасны тем, что похищают деньги с банковских счетов пользователей мобильных Android-устройств и способны завершать работу целого ряда антивирусных программ.

Троянцы семейства Android.BankBot знакомы специалистам по информационной безопасности уже несколько лет. Однако широкую известность они получили лишь в начале апреля 2015 г., когда МВД России сообщило о задержании киберпреступников, использовавших несколько модификаций этих вредоносных приложений при реализации атак на клиентов ряда российских и иностранных кредитных организаций. Несмотря на то, что деятельность этих злоумышленников была пресечена, распространение данных троянцев другими вирусописателями продолжилось, о чем свидетельствует появление очередных модификаций банкеров.

Так, совсем недавно вирусные аналитики компании «Доктор Веб» обнаружили несколько подобных троянцев, среди которых – Android.BankBot.43 и Android.BankBot.45. Они распространяются под видом легального ПО, такого как игры, медиаплееры или обновления операционной системы, и благодаря применению злоумышленниками различных методов социальной инженерии опрометчиво устанавливаются на Android-смартфоны и планшеты самими же пользователями.

Запустившись в зараженной системе, троянцы Android.BankBot пытаются получить доступ к функциям администратора мобильного устройства, которые дают им расширенные возможности, включая способность препятствовать их удалению. В процессе получения необходимых прав вредоносные программы используют весьма интересный механизм. В частности, они отображают поверх стандартного системного диалогового окна собственное сообщение, которое закрывает собой настоящее уведомление операционной системы и предлагает установить некие «дополнения». Соглашаясь с предложенным действием, пользователь на самом деле добавляет троянцев в список администраторов мобильного устройства, т. к. при нажатии кнопки «Продолжить», происходит активация скрытой за мошенническим окном оригинальной функции ОС.

В то же время, при попытке удаления троянцев Android.BankBot процедура исключения их из списка администраторов пресекается демонстрацией специального сообщения, в результате чего деинсталляция вредоносных приложений стандартными средствами системы становится невозможной.

После получения необходимых полномочий данные троянцы устанавливают связь с управляющим сервером и ожидают поступления дальнейших указаний. В частности, они способны выполнить следующие действия по команде с сервера:

– позвонить на указанный в команде номер;

– использовать для связи с управляющим сервером полученный в команде веб-адрес;

– выполнить указанный в команде USSD- запрос;

– отправить на сервер все входящие и исходящие СМС-сообщения;

– выполнить сброс настроек устройства с удалением всех данных пользователя;

– отправить СМС-сообщение с заданными параметрами;

– отправить на сервер подробную информацию о зараженном устройстве;

– осуществить поиск файла в соответствии с полученным в команде именем;

– использовать заданный телефонный номер для получения дублирующих команд.

Т. к. большинство управляющих команд дублируется злоумышленниками через СМС-канал, вредоносные приложения способны выполнять многие из своих функций даже при отсутствии интернет-соединения и связи с управляющим центром, что значительно увеличивает их вредоносный потенциал ***(Android-банкеры атакуют и после ареста их распространителей // ITnews (http://itnews.com.ua/news/76815-android-bankery-atakuyut-i-posle-aresta-ikh-rasprostranitelej). – 2015. – 28.04).***

***

Согласно отчету Human Factor 2015 компании Proofpoint, менеджеры среднего звена по продажам, финансам и закупкам непреднамеренно могут стать причиной опасных кибератак на их организации.

ИБ-исследователями было установлено, что 4 %, или каждое из 25 вредоносных электронных сообщений, было открыто сотрудниками компаний. Хотя все отрасли подвержены этой опасности, подобные инциденты в финансовом и банковском деле составляют 41 % из всех случаев. Внимание злоумышленников также привлекают здравоохранение и страховые организации, строительные компании и службы доставки.

Специалисты призывают начальников управления информационной безопасности принять к сведению, что менеджеры среднего звена открывают вредоносные ссылки в два раза чаще, чем их руководители. На долю менеджеров по продажам, финансам и закупкам приходится от 50 до 80 % казусных происшествий.

Стоит отметить, что злоумышленники чаще стали использовать рассылку вредоносных сообщений, чем атаки, направленные на контроль над URL-адресами. Вторник считается самым продуктивным днем для нажатия сотрудниками на вредоносные ссылки. В этот рабочий день принимаются на 17 % больше опасных электронных сообщений, чем в любой другой.

Директор одного из филиалов Proofpoint М. Спаршотт завил, что IT-специалисты должны признать возможность вредоносных сообщений обходить межсетевые экраны ***(Менеджеры среднего звена часто становятся причиной***

кибератак на их компании // InternetUA (http://internetua.com/menedjeri-srednego-zvena-csasto-stanovyatsya-pricsinoi-kiberatak-na-ih-kompanii). – 2015. – 28.04).

***

На конференции RSA2015, специалисты FireEye Labs рассказали о множественных уязвимостях сопровождающих применение отпечатков пальцев для аутентификации личности.

Прежде всего, исследователи напомнили о способе клонирования отпечатков пальцев по фотографии, продемонстрированном в конце прошлого года. Известные личности любят помахать ручкой перед фотокамерами, тем самым раздавая всем зрителям отличную картинку своих отпечатков пальцев.

Эксперты не обошли вниманием и отпечатки пальцев на экране смартфона, которые также могут быть сфотографированы под определенным углом или сняты с нанесением пыли, а затем клонированы для проведения мошеннических действий. Но, доверие своих отпечатков устройствам и программному обеспечению, которые могут использоваться злоумышленниками для компрометации личности, также является большой ошибкой рядовых пользователей.

Особенно это касается пользователей Android-смартфонов – One Max HTC, Motorola Atrix, Samsung Galaxy Note 4 и Edge, Galaxy S6, Huawei Ascend Mate 7, а также многих других. Наиболее уязвимы смартфоны с датчиками отпечатков пальцев в ОС версии ниже Android 5.0.

Многоуровневая архитектура доступа к отпечаткам пальцев через несколько библиотек функций и интерфейсов позволяют скомпрометировать маркеры отпечатка по MItM-технологии. Samsung Galaxy S5 заслужил отдельного внимания специалистов, в нем возможность получения доступа к маркеру отпечатка пальца доступна без root-прав из специальной области смартфона.

Другим способом получения отпечатка пальцев, специалисты FireEye назвали вредоносные приложения, которые могут имитировать экран блокировки или запрос авторизации отпечатка пальца в любой момент времени. Пользователь, предоставив свой отпечаток, позволит злоумышленникам обойти ограничения двухфакторной авторизации финансовой операции или же клонировать личность пользователя.

Эксперты информационной безопасности рекомендуют отключить использование отпечатков пальцев на смартфонах, которые воспринимаются пользователями как временная безопасная игрушка, вспомнить Средневековье и приобрести столь полезный аксессуар как перчатки ***(Android-смартфоны позволяют клонировать отпечатки пальцев // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/04/28/hta-f01-to-swipe-or-not-to-swipe-a-challenge-for-your-fingers.html). – 2015. – 28.04).***

***

Настоящие хакеры работают не только через Интернет, но интересуются и другими, самыми необычными способами, как заставить окружающие объекты делать то, что им не положено. Передают новости ИТ.

Вот почему бывший офицер ВМС США С. Уэйл, а ныне инженер компании APA Wireless, экспериментирует с биоимплантатом, который можно использовать для взлома мобильных гаджетов и обхода сканеров безопасности.

Небольшой NFC-чип в стеклянной капсуле (россыпь таких показана на фото вверху) с 888 байтами памяти имплантирован в мякоть ладони между большим и указательным пальцами. Поскольку такие операции на людях не проводятся, хакеру пришлось купить шприц производства Freevision для пометки крупного рогатого скота ***(Хакер внедрил чип NFC в руку и взламывает смартфоны прохожих // Новости ИТ (http://www.novostiit.net/haker-vnedril-chip-nfc-v-ruku-i-vzlamyivaet-smartfonyi-prohozhih-00020314). – 2015. – 29.04).***

***

Число пользователей, столкнувшихся с попытками кражи денег с банковских онлайн-счетов, за первые три месяца этого года увеличилось на 64 %. Такие данные озвучили эксперты KasperskyLab на основе анализа киберугроз в I квартале 2015 г., сообщает IT Expert.

Всего же в период с января по март решения KasperskyLab заблокировали более 5 млн попыток заражения компьютеров пользователей зловредами, предназначенными для опустошения счетов в системах онлайн-банкинга.

В последнее время злоумышленники наиболее активно стремятся всеми возможными способами внедрить функции перехвата конфиденциальной информации для доступа к банковским счетам и платежным системам в любое вредоносное ПО. Наиболее ярко эта тенденция проявилась среди угроз для мобильных устройств.

Так, все больше SMS-троянцев и троянцев-шпионов модифицируются и обзаводятся инструментами атаки на банковские счета пользователей. К примеру, популярный среди злоумышленников SMS-троянец Opfake, который два года назад похищал деньги лишь со счетов мобильных телефонов, сегодня умеет атаковать около 30 банковских и финансовых приложений. Некоторые из SMS-троянцев также начинают вести себя как программы-вымогатели. Возможно, во многом из-за этого в I квартале произошел серьезный спад количества «чистых» банковских троянцев – их доля по сравнению с предыдущим аналогичным периодом уменьшилась более чем в четыре раза и составила всего 1,1 %. При этом доля одних только SMS-троянцев достигла 21 %.

Однако финансовые атаки в I квартале были нацелены не только на пользователей персональных гаджетов. Киберпреступники научились красть деньги напрямую из банков. Именно так, например, был похищен почти 1 млрд дол. в рамках нашумевшей кампании Carbanak.

В общей сложности в I квартале 2015 г. продуктами Kaspersky Lab было предотвращено более 2 млрд попыток совершения атак на компьютеры и мобильные устройства пользователей. При этом 40 % всех зарегистрированных веб-атак были проведены с интернет-ресурсов, размещенных в России.

Украинские пользователи входят в число тех, кто чаще других сталкивается с попытками заражения в сети: на долю нашей страны приходится около 37 % уникальных пользователей, чьи устройства подверглись интернет-атакам.

«Киберпреступники все чаще создают и используют многофункциональные инструменты для атак. Они постоянно изменяют и расширяют функциональность уже запущенных “в оборот” зловредов, и это помогает им быстрее достигать своей цели – заполучить данные доступа для управления денежными счетами своих жертв. Именно поэтому пользователям стоит проявлять внимание и осмотрительность при работе с онлайн-банкингом и электронными устройствами и, безусловно, обеспечить их надлежащую защиту при помощи специальных программных решений», – рассказывает Д. Макрушин, антивирусный эксперт Kaspersky Lab ***(Зловреды все активнее охотятся за деньгами пользователей // InternetUA (http://internetua.com/zlovredi-vse-aktivnee-ohotyatsya-za-dengami-polzovatelei). – 2015. – 30.04).***

***

Очередной доклад Internet Security Threat от компании Symantec называет 17 % приложений на мобильной операционной системе Android вредоносными. Специалисты нашли на платформе от Google 700 тыс. вредоносных программ, из них целью более чем трети было распространение рекламы.

Исследователи не уточняют, сколько из общего числа вредоносных приложений были найдены в магазине Google Play Store, однако они уверены, что это число не слишком велико. В Symantec считают, что Google делает хорошую работу по предотвращению попадания вредоносных приложений в магазин и по нахождению всё же сумевших проникнуть туда программ.

Зато сторонние магазины похвастаться такой же ответственностью не могут; также небезопасно скачивание приложений с сайтов производителей, через ссылки в электронной почте и на торрентах.

Для анализа в Symantec использовали программное обеспечение Norton Mobile Insight, которое исследовало более 200 магазинов, скачивая и анализируя более чем 50 тыс. приложений и их обновлений каждый день на протяжении 2014 г. Большая часть вредоносного ПО нацелена на кражу конфиденциальных данных, вроде номеров телефонов и списков контактов, которые затем продаются ***(Доклад Internet Security Threat говорит об угрозах ОС Android // InternetUA (http://internetua.com/doklad-Internet-Security-Threat-govorit-ob-ugrozah-os-Android). – 2015. – 30.04).***

***

Google защитит пользователей от фишинговых атак

Google постоянно стремится сделать жизнь владельцев Android-устройств проще. В настоящее время компания решила сосредоточить свои усилия на улучшении безопасности пользователей и представила новое расширение для браузера Chrome под названием Password Alert, которое направлено на защиту пользователей от фишинговых атак. Расширение работает на аккаунтах Google и Google Apps for Work и разработано для того, чтобы предупредить пользователей о том, что их пароль используется где-то ещё.

По словам Google, расширение также должно сподвигнуть пользователей на использование разных паролей для разных сайтов, что, как правило, очень положительно сказывается на защите персональных данных. Ведь использование одной и той же комбинации электронной почты и пароля может поставить под угрозу сохранность личной информации.

После установки Password Alert в Chrome, Google будет хранить хешированную версию пароля к аккаунту Google. Компания заявила, что эта информация будет использоваться только в целях предотвращения возможных фишинговых атак.

«Наиболее эффективные фишинговые атаки заканчиваются успехом злоумышленников в 45 % случаев, а порядка 2 % писем, получаемых Gmail, разработаны специально, чтобы выманить у людей их пароли. Различные сетевые сервисы рассылают миллионы таких писем ежедневно», – сообщили представители Google ***(Google защитит пользователей от фишинговых атак // InternetUA (http://internetua.com/Google-zasxitit-polzovatelei-ot-fishingovih-atak). – 2015. – 2.05).***

***

Хакеры впервые атаковали робота-хирурга

В истории впервые произошел случай постороннего вмешательства в хирургическую операцию путем перехвата управления медицинским роботом. Это происшествие подняло вопрос безопасности проведения удаленных хирургических операций.

Во время исследования был осуществлен ряд успешных кибератак на робота-хирурга под названием Raven II, пишет Computerworld. Для начала специалистами были перехвачены пакеты данных, отправленные роботу, и изменен порядок их передачи. В результате «киберхирург» начал выполнять хаотичные движения, а затем, получив контроль над манипуляторами, специалисты изменили углы их поворота и диапазон перемещения, перехватив управление роботом окончательно.

В итоге медик-оператор полностью утратил контроль над роботом-хирургом и не смог осуществить даже удаленную перезагрузку аппарата. Было решено сделать применение шифрования данных в подобных операциях обязательным, иначе развитие телехирургии окажется под вопросом ***(Хакеры***

впервые атаковали робота-хирурга // InternetUA (http://internetua.com/hakeri-vpervie-atakovali-robota-hirurga). – 2015. – 2.05).

***

Експерти, що стежать за комп'ютерною безпекою, опублікували попередження про загрозу вірусу, який може вкрасти ваш аккаунт в Facebook.

За словами експертів, вірус набуває поширення за допомогою повідомлень від друзів, які нібито передають посилання зі своєю аватаркою та написом «Privat V1DEO», передає joinfo.ua.

Якщо перейти за посиланням, то вірус розішле його по всіх ваших друзях.

Потім у вас на стіні з'явиться аватарка одного з написом імені та прізвища користувача і вказівкою «Privat V1DEO» з тисячами переглядів. Клік по посиланню призведе до нового зараження, що дасть змогу вірусу розповсюджуватися з величезною швидкістю ***(У Facebook масово поширюється вірус «Privat V1DEO» // PINU.com.ua (http://pinu.com.ua/novyny/it/3-05-15/u-facebook-masovo-poshyryuyetsya-virus-privat-v1deo). – 2015. – 3.05).***

***

Исследователи безопасности компании Core Security выявили бреши в сетевых проекторах InFocus, позволяющих неавторизованному пользователю получить доступ к конфигурационным файлам и веб-интерфейсу устройств. Хотя специалисты протестировали только модель InFocus IN3128HD с версией прошивки 0.26, не исключено, что уязвимости затрагивают и другие версии.

Одна из брешей (CVE-2014-8383) позволяет обойти аутентификацию. Как поясняют эксперты, обычно конфигурационные изменения выполняются при помощи веб-интерфейса устройства, который защищен паролем. Однако в этом случае при входе пользователя в систему идентификационный механизм только проводит проверку правильности пароля без генерации сеансовых файлов cookie. Таким образом злоумышленник может обойти страницу авторизации и получить доступ к веб-интерфейсу напрямую. В результате в руках неавторизованного пользователя может оказаться приватная информация, в том числе сведения о конфигурациях сети и Wi-Fi (включая пароль). При этом права администратора позволяют преступнику модифицировать любой из параметров.

Вторая уязвимость (CVE-2014-8384) связана с ошибкой аутентификации при доступе к конфигурационному файлу webctrl.cgi.elf. Получив доступ к этому файлу, злоумышленник может выполнить конфигурационные изменения на устройстве, в том числе подкорректировать параметры DHCP-сервера, IP-конфигурации, удаленно произвести перезагрузку девайса или изменить его имя.

Эксперты Core Security уведомили компанию-производителя о наличии брешей, однако та пока не предприняла никаких действий для исправления уязвимостей. Как заявил представитель InFocus в письме изданию

SecurityWeek, злоумышленник сможет получить доступ только ко встроенным настройкам и функционалу включения/выключения устройства. Компания заверяет, что в будущем в ее продуктах будут реализованы дополнительные функции защиты ***(В проекторах InFocus обнаружены бреши, позволяющие обойти аутентификацию // InternetUA (http://internetua.com/v-proektorah-InFocus-obnarujeni-breshi--pozvolyauasxie-oboiti-autentifikaciua). – 2015. – 4.05).***

***

30 квітня сайт інформаційного агентства «Мост-Днепр» піддався серії хакерських атак, внаслідок чого в стрічці новин цього медіа з'явився ряд публікацій провокаційного характеру. Про це повідомило саме агентство.

Редакція ІА офіційно заявила, що не має відношення і не несе відповідальності за появу в подібних новин.

«Керівництво та колектив ІА "Мост-Днепр" розцінюють інцидент, як умисне перешкоджання журналістській діяльності, у зв'язку з чим у правоохоронні органи будуть направлені відповідні звернення і заяви», – ідеться у повідомленні агентства.

30 квітня розпочалася технічна службова перевірка за участю правоохоронних органів.

Нагадаємо, у квітні невідомі організували DDoS-атаки на два кримські опозиційні видання, «Новости Севастополя» та «Меридиан Севастополь», унаслідок чого ресурси певний час були недоступні для інтернет-користувачів ***(Сайт іформагентства «Мост-Днепр» атакували хакери // Телекритика (http://www.telekritika.ua/pravo/2015-05-04/106718). – 2015. – 4.05).***

***

Хакерам и подобным им злоумышленникам приходится жить с мыслью о том, что однажды их может застать врасплох полиция, а их настольные компьютеры и ноутбуки в этом случае будут использоваться против них самих же. Поэтому теперь в арсенале «злых компьютерных гениев» появилось новое вредоносное программное обеспечение под названием USBKill. Оно мгновенно выводит из строя ноутбук хакера при попытке незапланированного подключения или отключения от него USB-накопителя.

С помощью этого ПО хакеры смогут защитить себя от собственного же орудия для преступлений: USBKill «убивает» компьютер еще до того момента, как он может быть изучен следователями. Другими словами, ПО приходит хакерам на выручку тогда, когда война в онлайне переходит в реальную плоскость. Инструмент не идеален, и для его полноценного функционирования необходимо несколько условий: к примеру, шифрование на жестком диске.

USBKill поможет предотвратить повторение сценария с Р. Ульбрихтом, который является создателем подпольного сервиса по продаже наркотиков Silk Road. Ноутбук Р. Ульбрихта был изъят правоохранительными органами и стал главным источником доказательств его противозаконной деятельности

(Простой компьютерный код превращает флэшку в «убийцу ноутбуков» // InternetUA (http://internetua.com/prostoi-kompuaternii-kod-prevrasxaet-fleshku-v--ubiicu-noutbukov). – 2015. – 6.05).

***

Новый троянский вирус FakeInst атакует Android-смартфоны. Маскируясь под официальный магазин приложений Google Play и приложение Google Wallet, вирус собирает реквизиты банковских карт пользователей.

Распознавание вредоноса усложняет тот факт, что вирус не только имитирует внешний вид платёжного клиента Google Wallet, но и может взаимодействовать со многими легитимным онлайн-сервисами.

Троянец распространяется посредством SMS-спама с предложением установить обновление Google Play. Сразу после запуска вирус запрашивает права администратора, блокируя возможность работы с устройством до их получения.

После получения прав вредоносная программа отображает окно с требованием ввода реквизитов банковской карты якобы для её авторизации в системе Google Wallet.

Все вводимые пользователем данные о карте сверяются с форматом BIN и на принадлежность к большому списку платёжных систем. Получив корректную информацию, троянец закрывает окна и отсылает собранные сведения на сервер злоумышленников.

Получив данные, вредоносная программа, не подавая внешних признаков, продолжает функционировать на мобильном устройстве, собирая информацию о его владельце. Права администратора позволяют вирусу надёжно укорениться в системе.

Недавно аналитики антивирусной компании «Доктор Веб» обнаружили в сети приложение-фонарик, которое может полностью скомпрометировать любое устройство под управлением операционной системы Android ***(Android-вирус маскируется под кошелёк Google Wallet // Блог Imena.UA (http://www.imena.ua/blog/android-google-wallet/). – 2015. – 5.05).***

***

Федеральное управление гражданской авиации США обнаружило в программном обеспечении новейшего широкофюзеляжного самолёта Boeing 787 Dreamliner уязвимость, подвергающую опасности пассажиров.

Уязвимость позволяет вызвать серьёзный сбой в системе электроснабжения самолёта, тем самым провоцируя полную потерю контроля за воздушным судном. Проблема кроется в электрогенераторах на борту Boeing, которые могут выйти из строя по истечении восьми месяцев эксплуатации.

Непрерывная работа в течение 248 дней вызывает сбой в системах управления генераторами, которые одновременно переходят в

отказоустойчивый режим работы. Потеря тока приводит к потере контроля за самолётом Boeing, чем могут воспользоваться сторонние злоумышленники.

Инженеры Boeing осведомлены о существовании проблемы и уже провели перезапуск систем на всех самолётах 787 Dreamliner, которые в настоящее время находятся в эксплуатации.

Тем не менее, пока что проблема не устранена – всё ещё разрабатывается обновление для устранения данной ошибки. Впрочем, сроки выхода этого исправления производитель пока не озвучивает.

Недавно Международная организация гражданской авиации запустила онлайн-сервис, который позволяет обмениваться информацией о зонах, опасных для полётов гражданской авиации ***(В электросистемах самолётов Boeing обнаружена опасная уязвимость // Блог Imena.UA (http://www.imena.ua/blog/boeing-787-dreamliner/). – 2015. – 5.05).***

***

Чтобы помочь сохранить конфиденциальность участников своей социальной сети, Facebook внедрил функцию «Анонимный логин», чтобы пользователи могли не предоставлять личные данные.

Ранее новые пользователи должны были соглашаться с тем, что личная информация на Facebook становятся доступны в сторонних приложениях. Теперь участники могут на свое усмотрение делиться только теми данными, которыми хотят поделиться. Это станет возможным благодаря «Анонимному логину», говорили представители социальной сети еще в 2014 г. Разработчикам дали окно на один год, чтобы подготовиться к таким изменениям.

И сегодня Facebook выполняет свое обещание. Пользователи, которые хотят зайти в какое-либо стороннее приложение, используя функцию «Войти с помощью Facebook», получили возможность выбора данных, которыми они готовы поделиться. Например, можно выбрать категории только дня рождения и места ***(Facebook внедрил анонимный вход // IT новости (http://itnovosti.org.ua/2015/05/internet/socialnye-seti/facebook-vnedril-anonimnyj-vxod.html). – 2015. – 5.05).***

***

Спустя всего три месяца после того, как Lenovo была уличена в установке на свои новые компьютеры опасного программного обеспечения, крупнейшего в мире производителя ПК вновь обвинили в недостаточно серьезном подходе к защите пользователей. Специалисты из компании IOActive сообщают о том, что обнаружили в системе безопасности Lenovo серьезные уязвимости, с помощью которых злоумышленники могут легко получать управление компьютером жертвы.

К примеру, используя бреши в системе обновления, хакеры без особого труда могут обойти системы проверки программного обеспечения, заменить фирменное ПО Lenovo на вредоносное, после чего запускать на компьютере жертвы почти любые команды. Подготовленные хакеры могут провернуть

операцию по незаметной смене ПО даже в кафе, в котором владелец ноутбука Lenovo решит обновить систему.

Подобные схемы являются классическими, поэтому китайский производитель должен был предусмотреть наличие подобных уязвимостей в своей продукции. Как отмечают специалисты из IOActive, данная «дыра» в безопасности (как и некоторые другие) обнаружена ими в обновлении Lenovo System Update 5.6.0.27 и более ранних версиях.

В начале этого года Lenovo обвинили в распространении предустановленного вредоносного ПО, позволяющего шпионить за пользователями ***(На ноутбуках Lenovo вновь обнаружили серьезные уязвимости // InternetUA (http://internetua.com/na-noutbukah-Lenovo-vnov-obnarujili-sereznie-uyazvimosti). – 2015. – 7.05).***

***

Компания Arbor Networks опубликовала отчет о DDoS-атаках по итогам первого квартала, отметив, что в этот период по ее клиентской базе был зафиксирован новый рекорд по мощности – 334 Гб/с. Эта атака была проведена против одного из индийских сетевых операторов, ее продолжительность составила 6 минут.

В целом за квартал Arbor насчитала 940 тыс. DDoS-инцидентов в сетях пользователей информационно-аналитической платформы ATLAS, которая в настоящее время мониторит до 120 ТБ трафика, обслуживая 330+ интернет-провайдеров. При этом 17,7 % атак по мощности превышали 1 ГБ, а 25 показали на пике более 100 ГБ. Потолок другого важного показателя мощности DDoS, pps (число пакетов в секунду), за квартал снизился почти в два раза, с 112,5 до 65,15 Mpps.

«Атаки, значительно превышающие 200 Гб/с, очень опасны для операторов сетей и могут также причинить ущерб сервис-провайдеру, веб-серверам и корпоративным сетям, – отметил Д. Энсти, архитектор защитных решений Arbor. – DDoS-атаки продолжают эволюционировать. За последние полтора года не только повысились их мощность и частота, но возросло также число атак на веб-приложения. Чтобы успешно противостоять современной DDoS-угрозе во всех ее аспектах, мы настоятельно рекомендуем использовать многоуровневую систему обороны, которая сочетает защиту от атак прикладного уровня на местах и облачные решения, способные отражать более мощные атаки».

Большинство атак, зафиксированных Arbor в отчетный период, использовали технику отражения и усиления мусорного трафика. В качестве посредников в таких DDoS злоумышленники обычно задействовали устройства, работающие по протоколу NTP, SSDP или DNS. Техника атаки с плечом (DrDoS) до сих пор актуальна, сетуют эксперты, потому что многие сервис-провайдеры так и не удосужились установить на границах своих сетей фильтры, которые бы блокировали пакеты с поддельным IP-адресом источника. В то же время в сетях все еще много плохо сконфигурированных и

незащищенных устройств, использующих UDP и способных возвращать объемный ответ на короткий запрос.

Количество SSDP-атак, согласно Arbor, за квартал увеличилось с 83 тыс. до 126 тыс., их максимальная мощность тоже возросла – до рекордной отметки 137,88 ГБ. Из всех DrDoS 43,3 % проводились на порту 80 (HTTP); эксперты отметили, что в целом этот порт все чаще фигурирует в атаках, в течение квартала его использовали инициаторы 25,8 % DDoS.

Средняя продолжительность DDoS-инцидентов несколько увеличилась против IV квартала 2014 г. и составила 1 час 14 минут, однако в 90 % случаев ресурс подвергался атаке менее часа. Злоумышленники зачастую выбирали мишень с американской, китайской или французской пропиской (16,2; 16 и 7,5 % атак соответственно). Источники мусорного трафика в 40 % случаев определить не удалось, анализ остальных DDoS показал, что злоумышленники предпочитали проводить атаки с территории США (11,3 % инцидентов), Южной Кореи (8,5 %) и Китая (5,3 %) ***(В первом квартале зафиксирована DDoS-атака рекордной мощностью 334 Гб/с // InternetUA (http://internetua.com/v-pervom-kvartale-zafiksirovana-DDoS-ataka-rekordnoi-mosxnostua-334-gb-s). – 2015. – 7.05).***

***

Новый представитель вредоносного ПО пытается повредить компьютер при попытках его обнаружения антивирусными приложениям. Вирус получил от специалистов из Cisco Systems название Rombertik и предназначен для перехвата вводимого в окно браузера текста. Он распространяется через спам и фишинговые ссылки.

Вирус проводит на Windows-компьютерах несколько проверок на предмет того, не был ли он обнаружен. Зафиксировав определённые атрибуты связанного с анализом вредоносного ПО кода вирус начинает вести разрушительную деятельность. В этом он похож на аналог 2013 г. в атаке против Южной Корее и на прошлогодний, применённый против Sony.

Вирус вычисляет 32-битный хеш ресурса в памяти; если этот ресурс или дата компиляции были изменены, начинается процедура самоуничтожения вируса. Сначала атака идёт на главную загрузочную запись (Master Boot Record, MBR); если тут доступ не получен, вирус уничтожает файлы в домашней папке пользователя, шифруя их случайным ключом RC4. Далее компьютер перезагружается и MBR попадает в бесконечный цикл, не дающий системе загрузиться. На экране отображается сообщение Carbon crack attempt, failed.

При попадании на компьютер вирус распаковывает себя, на 97 % состоя из файлов-«обманок», имея 75 изображений и 8000 отвлекающих функций, в действительности никогда не используемых. Они призваны отвлечь внимание антивирусных приложений. Также вирус старается избежать попадания в «песочницу» – карантин на время его проверки. Rombertik начинает записывать в память один байт данных 960 млн раз, и если антивирус попытается зафиксировать все циклы записи, размер файла превысит 100 Гб ***(Новый вирус***

при обнаружении пытается уничтожить систему // InternetUA (http://internetua.com/novii-virus-pri-obnarujenii-pitaetsya-unicstojit-sistemu). – 2015. – 7.05).

***

В то время как развлекательные компании и официальные власти стараются всеми силами пресечь интернет-пиратство, методы, применяемые ими, зачастую ставят под угрозу безопасность пользователей. Блокировка пиратских сайтов, конфискация оборудования, снижение поискового ранга – все это способствует созданию менее безопасной онлайн-среды, говорится в публикации издания The Torrent Freak.

Как правило, блокировка файлообменников, распространяющих противоправный контент, приводит к появлению множества «дочерних» торрент-сайтов. К примеру, в Великобритании крупные пиратские ресурсы блокируются операторами связи, однако эти ограничения достаточно легко обойти через VPN. Подобные блокировки касаются только основных веб-сайтов, никак не затрагивая мгновенно появляющиеся десятки клонов, двойников или зеркал The Pirate Bay и KickassTorrents. Зачастую, такие ресурсы-имитаторы распространяют агрессивную или откровенно вредоносную рекламу, которая отсутствует на оригинальных порталах. Более того, по свидетельствам читателей The Torrent Freak, некоторые фальшивые Kickass-сайты не только требуют регистрации, но и запрашивают кредитную информацию пользователей.

В течение долгого времени правообладатели требовали от Google удалить пиратские ресурсы из поисковой выдачи. В итоге компания пошла на уступки и изменила алгоритм поискового движка. Однако эти действия привели к тому, что теперь при вводе запроса KickassTorrents поисковик выдает список мошеннических сайтов, которые не имеют никакого отношения к оригинальному ресурсу.

Насколько действенными окажутся анти-пиратские меры в долгосрочной перспективе – вопрос спорный. Тем не менее, факт остается фактом: каждая новая блокировка, конфискация оборудования и дезактивация пиратских ресурсов создает широкое поле деятельности для мошенников и увеличивает риск инфицирования вредоносным ПО, которое распространяется подложными сайтами ***(Борьба с пиратством в сети ставит под угрозу безопасность пользователей // InternetUA (http://internetua.com/borba-s-piratstvom-v-seti-stavit-pod-ugrozu-bezopasnost-polzovatelei). – 2015. – 6.05).***

***

9 роковых ошибок в Интернете, которые делают вас легкой добычей для хакеров

Каждый день в Интернете случаются взломы. Иногда это серьезные кибер-нападения с тысячами строк кода, способного свалить защиту Пентагона, но чаще – обыкновенные мошенничества. Как правило, к краже личных данных

и утечке информации виноват ни кто иной, как сам пользователь. Тут никакие антивирусы не помогут, единственный способ помешать хакерам до вас добраться – сохранять бдительность. Журналисты Business Insider назвали 9 вещей, которые вы каждый день делаете в Интернете, тем самым превращаясь в идеальную мишень для хакеров, пишет // AIN.UA (http://ain.ua/2015/05/07/579426).

Очевидные пароли

Люди – ленивые создания. Когда речь заходит о безопасности устройств, подключенных к Интернету, они, почему-то, выбирают самые простые и очевидные пароли. Каждый год SplashData публикует отчет по мировым паролям, и результаты удручают. Так, самый популярный в мире пароль, согласно данным сервиса, какой бы вы думали? Вот такой: «123456». На втором месте «password», то есть пароль – «пароль»! Серьезно, люди, пора бы начать использовать более сложные пароли.

Пароль должен содержать цифры, пунктуационные символы, если это дозволяется, большие и маленькие буквы. И бога ради, пусть он не будет простым словом, в особенности, таким, которое ассоциируется с вами. Хакеры ищут людей с простыми паролями, а когда находят – набрасываются, словно стая волков на заблудшую овцу.

Двухшаговая идентификация

Даже самые сложные пароли можно подобрать или попросту украсть. На такой случай лучше перестраховаться. Двухшаговая идентификация затрудняет несанкционированное проникновение в аккаунт, поскольку требует подтвердить личность владельца дважды. Например, после того, как вы вводите пароль от аккаунта, сервис перенаправит вас на новую страницу, которая затребует ввести код подтверждения, предварительно высланный вам на мобильный телефон.

Такой вот, казалось бы, элементарный прием обеспечивает куда большую степень защищенности в современных реалиях с избытком 13-летних компьютерных гениев, мошенников и воришек.

Бесплатный Wi-Fi

Конечно, использование открытых хотспотов в кафе и ресторанах очень удобно и, казалось бы, что в этом плохого? А то, что тем самым вы становитесь мишенью потенциальных атак. Охранная компания Cylance ранее обнаружила огромную уязвимость, зияющую в роутерах одной из крупнейших отельных сетей. Фактически, она предоставляла хакерам безлимитный доступ к веб-серфингу пользователей.

Помимо прочего, бесплатный Wi-Fi давно стал основным инструментом для DDoS-атак. Знающий человек никогда в жизни не проверит почту или банковский счет с использованием публичной Wi-Fi сети. Потому что это – прогулка по тонкому льду.

Незащищеное соединение

Это происходит постоянно. Вы видите что-то, что хотите купить, заходите на сайт, вам выдает форму с запросом данных вашей банковской

карты, вы все добросовестно вводите и совершаете транзакцию. Но есть один момент, на который вы едва ли обращаете внимание: использует ли данный сайт протокол HTTPS?

Это легко проверить. Просто посмотрите, есть ли слева от URL значок с замочком. Если такового нет, хакеры смогут легко проследить, на какие сайты вы заходите, и скопировать данные, которые вы вводите, чтобы потом воспользоваться ими в собственных целях.

Сомнительные сделки на онлайн-аукционах

Казалось бы, кто вообще станет таким заниматься? На самом деле, многие. Однажды, возможно, соблазнитесь и вы. Когда кто-то обращается к таким сайтам как eBay, Aukro и прочим онлайн-аукционам, первое средство безопасности – это проверка отзывов.

Остерегайтесь подозрительно выгодных сделок на таких сайтах, потому как часто они оказываются обыкновенным мошенничеством.

Подозрительные вложения

Социальный инжиниринг – самый распространенный прием проникновения хакеров в аккаунты беспечных пользователей. Таким образом они заставляют ничего не подозревающих пользователей выполнять за них всю работу. Вместо того, чтобы писать код, который пробьет брешь в защите сервиса, некоторые мошенники просто пришлют письмо с вирусом, открыв который, пользователь сам вручит управление своим компьютером ленивому хакеру.

Такие вредоносы часто содержатся во вложениях к письму и замаскированы под pdf и другие форматы. На самом деле, это злые троянцы, которые неведомо чего натворят, когда попадут на ваш компьютер.

Подозрительные ссылки

По аналогии с нездоровыми вложениями, люди постоянно ведутся на фишинговые кампании. Например, в письме содержится ссылка на сайт, замаскированный под популярный ресурс. Он вроде заслуживает доверия, но на самом деле нет.

Очень часто людям присылают письма с предложением сменить пароль или настройки для пущей безопасности. При переходе по ссылке у пользователя запрашивают драгоценные полномочия, и горе тем, кто их предоставит. Это самый простой способ получить вашу информацию. Избежать утечки очень просто – проверяйте ссылки, прежде чем по ним переходить.

Для разных сервисов – одинаковые пароли

Одинаковые или даже похожие пароли для всех ваших аккаунтов – это самоубийство. Конечно, в эпоху Интернета очень раздражает необходимость каждый раз придумывать новый пароль и не дай бог его запоминать. Поэтому часто люди везде вводят один и тот же набор символов. Если однажды каким-то непостижимым образом этот пароль утечет в сеть, хакеры получат доступ ко всей вашей информации сразу.

Не пренебрегайте своей безопасностью. Тем более, для самых ленивых даже существуют генераторы уникальных паролей, например 1Password и LastPass.

Человеческий фактор

Чаще всего взломы становятся результатом обыкновенного человеческого фактора. Если роковая ошибка допущена, не спешите посыпать голову пеплом – от этого толку чуть. А лучше подготовьтесь к тому, что будет дальше. Например, неплохо в таких случаях уметь быстро поменять все свои пароли, защитить счета и провести аудит своих аккаунтов ***(9 роковых ошибок в Интернете, которые делают вас легкой добычей для хакеров // AIN.UA (http://ain.ua/2015/05/07/579426). – 2015. – 7.05).***

***

7 мая исследователь безопасности под псевдонимом BruteLogic сообщил о еще одной XSS-бреши на веб-сайте linkedin.com.

На момент написания новости уязвимость оставалась неисправленной, что ставит под угрозу компрометации злоумышленниками данные пользователей, посетителей и администраторов сайта. За все время существования портала это уже пятая брешь, обнаруженная специалистами. XSS – это возможность злоумышленника определенным образом интегрировать в страницу сайта-жертвы скрипт, который будет выполнен при ее посещении.

Также XSS-уязвимость на популярных ресурсах может быть использована для проведения DDoS-атаки. Похищение cookie-файлов, персональной информации, учетных данных, а также просмотр истории браузера – пожалуй, наименее опасные последствия XSS-атак. С каждым днем подобные атаки становятся более сложными и опасными и, зачастую, используются в паре с фишингом, социальной инженерией и атаками drive-by ***(На сайте linkedin.com обнаружена XSS-уязвимость // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/05/08/linkedin-flaw.html). – 2015. – 8.05).***

***

Исследователи FireEye уверены, что ряд вредоносных приложений, анализом которых они занимались с декабря 2014 г., был разработан при помощи набора инструментов Microsoft Word Intruder без вмешательства человека.

Сам инструмент, как сообщается на сайте антивирусной компании, вероятнее всего, разработали российские хакеры. Программа распространялась на русскоязычных подпольных форумах, в связи с чем в настоящее время она не пользуется широкой популярностью среди злоумышленников всего мира.

Автор Microsoft Word Intruder, скрывающийся под псевдонимом Objekt, просит за свою разработку 2–3,5 тыс. дол. и позиционирует ее, как «наиболее надежный и универсальный набор экплоитов для .doc».

В FireEye, в свою очередь, отмечают, что созданные таким образом документы Word могут умещать в себе сразу несколько эксплоитов, поочередно предпринимающих попытки скомпрометировать целевую систему. При этом соответствующие модули и вся работа над формированием вредоноса производится автоматически без вмешательства человека ***(Обнаружен набор инструментов, создающий вирусы в автоматическом режиме // InternetUA (http://internetua.com/obnarujen-nabor-instrumentov--sozdauasxii-virusi-v-avtomaticseskom-rejime). – 2015. – 10.05).***

***

Apple Mac уязвимы к различным видам вредоносного ПО

По словам бывшего сотрудника АНБ и интерна НАСА, а ныне руководителя исследовательского отдела ИБ-компании Synack П. Уордла, обойти традиционные средства защиты операционной системы OS X – проще простого.

В частности, он обнаружил, что защитная технология Gatekeeper позволяет выполнение неподписанного кода. Утилита Gatekeeper используется для проверки кода и является предустановленной на всех Mac под управлением OS X. Инструмент сконструирован таким образом, что по умолчанию позволяет либо выполнение подписанного кода, либо, в зависимости от настроек, принимает пакеты только от Mac App Store.

П. Уордл отметил, что встроенные Apple защитные механизмы – Gatekeeper, Xprotect, требования к сертификатам цифровой подписи – достаточно легко обойти и проэксплуатировать.

До недавнего времени все обновления безопасности Mac загружались через незащищенное HTTP-соединение, полагаясь на Gatekeeper для верификации кода. Однако обнаружение способа обхода утилиты предоставляет злоумышленникам возможность осуществления атак «человек посередине».

«Хорошо подготовленные атакующие, такие как национальные государства, смогут мониторить процесс загрузки, прежде чем внедрить код в легитимные загрузки», – пояснил П. Уордл в интервью изданию The Register.

Еще одна проблема заключается в том, что десктопная операционная система Apple позволяет работу неподписанных локальных приложений. Таким образом, скомпрометировав машину, злоумышленники могут добавить свой собственный код в уже подписанный. При этом OS X не заметит, что прежде подписанное приложение не является таковым, и позволит ему работать дальше ***(Apple Mac уязвимы к различным видам вредоносного ПО // InternetUA (http://internetua.com/Apple-Mac-uyazvimi-k-razlicsnim-vidam-vredonosnogo-po). – 2015. – 10.05).***