СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(19–31.05)

2014 № 10

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(19–31.05)
№ 10

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

Головний редактор
В. Горовий, д-р іст. наук, проф.

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Соцсеть «ВКонтакте» планирует выпустить обновлённую версию клиента для iPad с дизайном, соответствующим iOS 7. Об этом объявил руководитель отдела разработки «ВКонтакте» А. Рогозов.

А. Рогозов официально подтвердил, что клиенты «ВКонтакте» под iPhone и iPad были удалены из App Store за порнографический контент. По словам ведущего разработчика соцсети, с ростом интереса Apple к российскому рынку жёсткость соблюдения правил магазина приложений только росла.

А. Рогозов отметил, что компания делает всё возможное, чтобы вернуть мобильные клиенты в App Store. В комментарии TJournal он отметил, что разработчикам «приходится скрывать много взрослого контента».

Вместе с тем, по словам А. Рогозова, в итоге пользователям станут доступны обновлённые приложения. Клиент для iPad наконец получит редизайн в «плоском» стиле операционной системы iOS 7.

Система вышла в сентябре 2013 г., и многие пользователи критиковали «ВКонтакте» за затягивание с обновлением приложения ***(«ВКонтакте» выпустит iPad-клиент под iOS 7 // IT Expert (http://itexpert.org.ua/rubrikator/item/35805-vkontakte-vypustit-ipad-klient-pod-ios-7.html). – 2014. – 18.05).***

***

Социальная сеть Facebook создает видеомессенджер в стиле программы Snapchat, пишет The Financial Times со ссылкой на источники. Утверждается, что новое приложение называется Slingshot. По имеющейся информации, разработка программы продолжается уже несколько месяцев.

Как отмечают источники, у Slingshot будет простой и быстрый пользовательский интерфейс. Не исключено, что приложение выйдет в этом месяце, однако Facebook все еще может отказаться от этого проекта, добавляет газета.

В Facebook решили разработать Slingshot после того, как не смогли купить Snapchat за 3 млрд дол. в прошлом году, говорится в статье.

В настоящее время у социальной сети есть собственное приложение для обмена текстовыми сообщениями Facebook Messenger. Кроме того, компания приобрела мессенджер WhatsApp ***(Facebook создает видеомессенджер // Marketing Media Review (http://mmr.ua/news/id/facebook-sozdaet-videomessendzher-39698/). – 2014. – 19.05).***

***

«Лаборатория Касперского» запустила сервис FriendOrFoe для пользователей социальной сети Facebook, пишет AIN.UA (http://ain.ua/2014/05/19/524681).

Новинка позволяет оценить характер поведения друзей и то, как пользователь выглядит с точки зрения окружающих. Приложение также выявляет географическое распределение друзей. Похоже, сервис удобным инструментом для тех россиян, которые хотят выявить в своих рядах «бандеровцев», а также для украинцев, которые хотят избавиться от пророссийских активистов «во френдах». Сервис анализирует всю информацию, которую собирает о пользователях Facebook: типы публикуемых постов, поисковые запросы, используемые приложения, временные интервалы активности и другое. Для того, чтобы запустить процесс, нужно зайти на сайт сервиса через свой аккаунт в Facebook.

Анализ происходит за пару минут, хотя создатели предупреждают, что иногда этот процесс может затянуться на полчаса. Вероятно, скорость анализа зависит от активности пользователя на Facebook и количества у него таких же активных друзей.

На основе полученных данных формируется инфографика о ваших друзьях: кто чем занимается в сети, кто самый активный, у кого с вами общие интересы, а кто вам враг. Вы узнаете, кто из ваших друзей является вашим преданным читателем, кого предпочитаете читать вы, кто из них лидеры мнений, а кто и вовсе звезды Facebook.

Однако основной акцент сервиса все-таки сделан на выявление врагов. Особого внимания заслуживают подрубрики, на которые сервис разбивает ваших друзей из «группы риска»:

«чужаки» – в первых рядах у некоторых украинцев здесь внезапно российские пользователи;

«молчание ягнят» – сюда попадают те, кто редко постит в Facebook;

«говорящие со стеной» – их посты никто не лайкает;

«любители публиковать ссылки» – название говорит само за себя ***(«Лаборатория Касперского» создала сервис поиска врагов среди Facebook-френдов // AIN.UA (http://ain.ua/2014/05/19/524681). – 2014. – 19.05).***

***

В начале 2014 г. наибольшая доля мобильного трафика принадлежала Facebook и YouTube. Это связано с тем, что все больше пользователей используют мобильные устройства во время веб-браузинга, общения в соцсетях и просмотра видео.

Совокупная доля мобильного трафика сервисов в Северной Америке в пиковое время в начале текущего года составила 32 %, утверждают эксперты Sandvine. При этом Facebook принадлежит 26,9 % исходящего трафика, в то время как показатель входящего трафика равен 14 %. Что касается YouTube, то его исходящий трафик – 3,7 %, а входящий – 17,6 %.

Судя по высокому показателю исходящего трафика Facebook, пользователи стали еще чаще загружать в соцсети гораздо больше фотографий и видео с мобильных устройств. При этом доля входящего трафика YouTube подчеркивают стабильность активности интернет-пользователей, ведь в прошлом году, по данным Sandvine, этот показатель составлял 17,7 %.

Выше представлен список, созданный компанией Statista. В нем содержатся 10 веб-сервисов, захвативших основную часть мобильного трафика. В перечень ресурсов, помимо Facebook и YouTube, попали Pandora, Netflix, Instagram, Google Play и iTunes ***(YouTube и Facebook – лидеры мобильного интернет-трафика // InternetUA (http://internetua.com/YouTube-i-Facebook---lideri-mobilnogo-internet-trafika). – 2014. – 19.05).***

***

Крупнейшая российская соцсеть «ВКонтакте» решила частично легализовать музыкальный контент, поставив в официальном клиенте ссылки на песни из iTunes Store. Правда, само приложение пока заблокировано Apple.

«В ближайшем обновлении наших iOS-приложений среди прочего мы интегрируем поддержку iTunes, – заявил представитель «ВКонтакте» Г. Лобушкин. – То есть всю музыку, которой пользователи обмениваются в приложении социальной сети для iPad, можно будет приобрести в несколько кликов в музыкальном магазине». О том, что «ВКонтакте» интегрирует iTunes, рассказал источник, близкий к крупным звукозаписывающим студиям.

Как отмечают «Ведомости» со ссылкой на гендиректора Национальной федерации музыкальной индустрии (НФМИ, представляет интересы звукозаписывающих компаний Sony Music, Universal Music, Warner Music и др.) Л. Агронова, разрешение правообладателей требуется на распространение музыки по любой модели – будь то скачивание за деньги по модели iTunes или стриминг. «Пока этого нет, любое распространение является пиратским», – сказал он.

Но бесплатный стриминг музыки, которую во «ВКонтакте» закачивают пользователи, в соцсети останется. Сейчас представители соцсети ведут переговоры с правообладателями о том, каким образом будет монетизироваться этот контент. Как сообщается, компании быстрее удается найти общий язык с российскими правообладателями, нежели с западными ***(«ВКонтакте» интегрируют с iTunes // InternetUA (http://internetua.com/vkontakte--integriruuat-s-iTunes). – 2014. – 19.05).***

***

В Google Play появилось приложение популярной анонимной социальной сети Secret, пользователи которой без стеснения делятся друг с другом самым сокровенным.

Для полноценного использования Secret нужно привести в приложение как минимум трех друзей. Все пользователи и даже друзья сохраняют полную анонимность – читать их откровения можно, а узнать, кто именно оставил запись, нельзя. В общую ленту сообщение попадает только в том случае, если его прочли друзья и друзья друзей. В версии Secret для Android есть эксклюзивная функция – публикация сообщений, которые могут быть видны только друзьям. На iOS такой возможности нет, но она скоро появится. Русскоязычных пользователей в Secret пока мало, общение в основном ведется на английском ***(На Android вышло приложение Secret // InternetUA (http://internetua.com/na-Android-vishlo-prilojenie-Secret). – 2014. – 23.05).***

***

В мобильном приложении Facebook появилось два интересных нововведения: 1. Социальная сеть запустила функцию, которая будет автоматически определять для последующего указания в статусе, какое видео смотрит пользователь в конкретный момент времени, или какую музыкальную композицию прослушивает. 2. Возможность отображения на публичных страницах меню ресторанов.

Предоставив приложению доступ к микрофону, пользователь сможет мгновенно поделиться информацией о контенте с друзьями. При этом ему не придется печатать название песни, фильма или ТВ-шоу, – приложение введет текст самостоятельно и предложит владельцу устройства опубликовать свой статус в один клик. В статусе также будет указываться номер сезона и название эпизода. «При активации функции вы увидите на экране своего устройства подвижную иконку, в случае, если композиция распознана – вам сразу же будет предложено обновить свой статус и поделиться им с желаемой группой пользователей», – сообщают в Facebook .

Если же пользователь делится информацией о просмотре музыкального клипа, пользователя или аудиокомпозиции, окружающим будет предложено посмотреть 30-секундное превью. Таким образом, музыкальное произведение можно будет обсудить с друзьями.

В ближайшие несколько недель владельцы устройств на iOS и Android смогут оценить новинку.

Еще одной заметной функцией, появившейся в мобильном приложении Facebook, стала возможность отображения на публичных страницах меню ресторанов. Нововведение будет запущено в ближайшие месяцы по всему миру.

«В поисках хорошего ресторанного заведения пользователи не редко обращаются к Facebook-приложению. Они ищут в социальной сети

расположение ресторанов, часы работы и меню. Вот почему, начиная с сегодняшнего дня, мы позволим ресторанам публиковать информацию о главных блюдах меню на публичных страницах Facebook», – заявляют представители социальной сети.

Владельцы ресторанов из Канады и США уже могут загрузить информацию о меню в Faceboo, используя возможности SinglePlatform. Рестораторы за пределами этих стран совсем скоро смогут загрузить файл с информацией о меню в формате PDF, используя настройки публичной страницы (Settings – Page Info – Menus) ***(Мобильное приложение Facebook распознает музыку, кино, ТВ-контент и покажет меню ресторанов // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/mobilnoe_prilozhenie_facebook_raspoznaet_muzyku_kino_tv_kontent_i_pokazhet_menyu_restoranov). – 2014. – 27.05).***

***

Facebook начинает массовый запуск нового дизайна для публичных страниц. Администраторы уже получили возможность увидеть, как именно страница их компании будет отображаться в обновлённом интерфейсе. Об этом сообщает searchengines.ru.

Автоматический перевод на новый дизайн всех страниц брендов состоится к 6 июня 2014 г. Паблики в новом интерфейсе, как и ранее, будут двухколоночными. В новой версии лента сообщений будет отображаться в основной части экрана справа и располагаться в одну колонку. Слева от нее разместился блок с основной информацией и контактами компании. В старом интерфейсе обе упомянутые колонки были частью «Хроники».

Информация о ключевых показателях страницы, включая количество подписчиков, оповещения, настройки, перенесена в правый верхний угол и расположилась в правой колонке. Блок является статичным и открывается для просмотра, когда ленту прокручивают вниз.

Что касается функционала новых публичных страниц, то теперь администраторы получили возможность создавать списки похожих страниц, а впоследствии сопоставлять их ключевые показатели пользовательской активности со своими. Функция будет доступна в разделе статистики страницы.

Впервые о запуске публичных страниц в новом дизайне представители Facebook сообщили в начале марта 2014 г. Практически тогда же состоялся запуск новой версии оформления «Ленты новостей» ***(Facebook представит новый дизайн для всех публичных страниц // Marketing Media Review (http://mmr.ua/news/id/facebook-predstavit-novyj-dizajn-dlja-vseh-publichnyh-stranic-39809/). – 2014. – 27.05).***

***

Важность мнения почти любого пользователя Twitter трудно переоценить. Она, несомненно, очень велика, особенно когда дело касается какой-нибудь очень значимой новости. Но как сделать так, чтобы самый важный твит на свете увидели все? Для этого есть сервис Super Important Tweet.

Пользоваться им в Twitter очень просто: просто введите текст, который должен быть замеченным, и твит будет снабжён цветастой картинкой, на коей и расположится этот текст.

Конечно, к этому сервису стоит обращаться с осторожностью, если не хотите растерять всех подписчиков. Если же вы агрессивный бот – пользуйтесь на здоровье ***(Super Important Tweet поможет подчеркнуть важность твита // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/super_important_tweet_pomozhet_podcherknut_vazhnost_tvita). – 2014. – 28.05).***

***

Украинские инвесторы и ученые теперь имею свою социальную сеть http://industriya.com.

Новая сеть предлагает возможность объединяться в группы по интересам и по роду своей трудовой деятельности. В сети можно будет публиковать собственные научные статьи и новости техники. Каждый пользователь при желании может создавать свои блоги и размещать свою коллекцию фотографий. По мере становления нового проекта, в нем появятся и другие опции ***(Украинская социальная сеть для инвесторов и ученых // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/ukrainskaya_sotsialnaya_set_dlya_investorov_i_uchenyh). – 2014. – 29.05).***

***

К концу 2014 г. численность пользовательской аудитории Twitter по всему миру увеличится на 24,4 %. При этом наибольший рост числа пользователей наметится в странах Азиатско-Тихоокеанского региона. В целом, к 2018 г. темп роста аудитории Twitter замедлится, но все же прирост окажется существенным.

Такие прогнозы относительно дальнейшего развития сервиса микроблогов приводит агентство аналитики eMarketer.

Если говорить о региональной распределённости аудитории сервиса микроблогов, то к концу 2014 г. наибольший прирост (32,8 %) наметится в странах Азиатско-Тихоокеанского региона. Следом идёт Северная Америка – к концу 2014 г. численность пользователей Twitter в этом регионе может увеличиться на 23,7 %. Третью строчку занимают страны Западной Европы – для них данный показатель на конец года может составить 16,8 %.

Наиболее заметный рост численности пользовательской аудитории Twitter наблюдается в таких странах как Индонезия и Индия (61,7 и 56,9 % к концу 2014 г., соответственно). Далее идут страны Латинской Америки: Аргентина, Мексика и Бразилия. Россия занимает шестую строчку рейтинга. Прогнозируемый прирост аудитории Twitter в этой стране к концу 2014 г. составит 31,4 %, а к концу 2018 г. – 15,2 %.

В целом, по данным eMarketer, к 2018 г. объём пользовательской аудитории Twitter по всему миру увеличится на 10,7 % и составит 400 млн человек ***(eMarketer: к 2018 году общая численность аудитории Twitter'а составит 400 млн. человек // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/emarketer_k_2018_godu_obschaya_chislennost_auditorii_twitter_a_sostavit_400_mln_chelovek). – 2014. – 30.05).***

***

Нью-йоркский стартап Dropp.fm стремится создать новую социальную сеть для людей, которые любят музыку.

Вообразите ленту новостей, заполненную музыкальными треками, которыми делятся с вами ваши друзья, а вы, в свою очередь, с ними. Возможность прослушивать свои плейлисты и плейлисты друзей. Понравившуюся композицию можно разместить у себя на странице. Все это содержит в себе Dropp.fm.

Проект все еще находится на ранних стадиях разработки, но основатель Dropp.fm П. Либерман уверен, что данный его детище перевернет восприятие музыки через Интернет и образ взаимодействия с ней.

«Dropp.fm – удивительная новая социальная сеть, которая дает возможность пользователям обмениваться, находить и собирать новую музыку с сотни сайтов, – прокомментировал П. Либерман. – Сочетание новейшей музыки в Интернете и взаимодействия с друзьями – вот, что делает Dropp.fm настолько уникальным».

П. Либерман – меломан до корней волос, который с любовью относится к созданию музыки, да и ко всему, что с ней связано. Даже при том, что уже существуют всевозможные приложения и тонны музыки на различных сайтах, П. Либерман считает их не достаточно социальными. Он намеревается сделать свою собственную социальную сеть, для создания которой потрачено немало времени на изучение, уже существующих, музыкальных сервисов.

Чтобы получить доступ к Dropp.fm, следует просто зайти на главную страницу сайта, зарегистрироваться через Facebook.

В настоящее время для вашей ленты новостей могут быть предложены только YouTube и SoundCloud ссылки, но в будущем, П. Либерман надеется добавить еще множество медиа порталов для обмена контентом, таких как Vimeo ***(DROPP.FM – первая социальная сеть для меломанов // ProstoWeb***

(http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/dropp_fm_pervaya_sotsialnaya_set_dlya_melomanov). – 2014. – 30.05).

***

Facebook повідомив про суттєве скорочення кількості постів, які автоматично публікуються сторонніми додатками в стрічках користувачів. Такий тип публікацій найчастіше позначається як спам і є небажаним для користувачів. Користувачі відчують на собі новацію в ближчі кілька місяців.

Facebook обіцяє дотримуватись свого принципу, який озвучувався вже не раз – пріоритет надаватиметься публікаціям, які генерують чи якими діляться користувачі самостійно.

Користувачі також отримають можливість приватно ділитися з друзями постами, що зацікавили їх, використовуючи сервіс Messenger.

У найближчі тижні в мобільній версії соціальної мережі також з'явиться можливість додаткового налаштування користувачем даних, які Facebook автоматично передаватиме додаткам. Встановивши налаштування приватності один раз, людині не доведеться турбуватися про те, яку інформацію про нього Facebook передасть стороннім додаткам ***(Facebook зменшить кількість спам-публікацій в стрічці новин // UkrainianWatcher (http://watcher.com.ua/2014/05/30/facebook-zmenshyt-kilkist-spam-publikatsiy-v-strichtsi-novyn/). – 2014. – 30.05).***

***

Как сообщает CNet, клиент Twitter для Android начал переводить твиты с одного языка на другой. Переводы осуществляются автоматически с помощью сервиса Bing Translator.

Обнаружить это нововведение не так просто, поскольку переводятся далеко не все твиты на незнакомых языках и не у всех пользователей. Однако то, что в приложении Twitter на Android все же появится автопереводчик, можно не сомневаться, ведь он уже есть на Windows Phone 8 и веб-версии сервиса ***(Twitter тестирует перевод твитов с одного языка на другой в приложении для Android // InternetUA (http://internetua.com/Twitter-testiruet-perevod-tvitov-s-odnogo-yazika-na-drugoi-v-prilojenii-dlya-Android). – 2014. – 31.05).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Несколько десятков пользователей, которые по тем или иным причинам не смогли принять участие в выборах Президента, решили

продемонстрировать свой выбор в социальных сетях. Для этого они написали на листочке имя своего кандидата в Президенты, год и город, в котором проживают, сфотографировали и выставили фото в соцсети, сообщают «Новости Мариуполя», пишет «Обозреватель» (http://obozrevatel.com/politics/14960-ukraintsyi-massovo-golosuyut-v-sotssetyah--fotofakt.htm).

Большинство участников побоялись показать всей стране свои лица, поэтому скрыли их на фотографии. Были же и те, кто отважно продемонстрировал в соцсети свой паспорт.

Среди «проголосовавших» в основном люди из восточных городов Украины: Донецк, Мариуполь, Макеевка, Горловка ***(Украинцы массово голосуют в соцсетях // Обозреватель (http://obozrevatel.com/politics/14960-ukraintsyi-massovo-golosuyut-v-sotssetyah--fotofakt.htm). – 2014. – 24.05).***

***

Facebook під вибори запускає кнопку I'm A Voter

Facebook уперше презентував кнопку I'm A Voter (я виборець) ще під час виборів 2012 р. у США. Наступний раз ця можливість використовувалась вже у 2014 р. під час виборів в Індії. А з цього тижня ініціатива стала глобальною і поширилася майже на 10 країн, у яких ближчим часом будуть вибори.

Кнопка I'm A Voter буде присутня у жителів Європи під час виборів до Європейського парламенту наступного тижня, а також на найближчих виборах у Колумбії, Південній Кореї, Індонезії, Швеції, Шотландії, Новій Зеландії та Бразилії.

На жаль, у переліку країн України поки що нема.

У Facebook також розповіли в коментарі агенції Reuters, що понад 4 млн користувачів клікнули на кнопку I'm A Voter під час останніх виборів в Індії. Коли люди бачать у Facebook, що їхні друзі проголосували, це мотивує прийти на вибори та піднімає явку ***(Facebook під вибори запускає кнопку «I'm A Voter» // UkrainianWatcher (http://watcher.com.ua/2014/05/20/facebook-pid-vybory-zapuskaye-knopku-im-a-voter/). – 2014. – 20.05).***

***

Понтифик Франциск есть в Twitter, но его нет в Facebook. Почему? Недавно представители крупнейшей в мире соцсети посетили Ватикан и попытались убедить представителей папского престола в том, что завести профиль в Facebook необходимо, однако К. М. Селли, архиепископ, занимающийся медиастратегией папы, сообщил, что папа Франциск не хочет присоединяться к соцсети, ибо не желает получать оскорбительные комментарии.

Это довольно странно, ведь Ватикан в последнее время активно использовал социальные сети, а сам папа даже назвал Интернет «даром

Божьим». Предшественник Франциска, Бенедикт XVI, завёл аккаунт в Twitter в 2012 г., и это рассматривалось как весьма умный ход для расширения влияния католической церкви. Затем эта учётная запись перешла к Франциску.

Но некоторые кардиналы беспокоились о бранных ответах, которые аккаунт получал на свои записи. По словам К. М. Селли, это стало виной настоящего кризиса в Ватикане после создания учётной записи @Pontifex.

В Twitter, как считает архиепископ, бранные записи проще игнорировать, чем комментарии в Facebook. Он рассказывает, что и без того уходит много времени на то, чтобы удалять ругательные послания со страницы новостного агентства Ватикана News.va (при этом администрация оставляет конструктивную критику) ***(Стало известно, почему папа римский не заводит себе аккаунт в Facebook // InternetUA (http://internetua.com/stalo-izvestno--pocsemu-papa-rimskii-ne-zavodit-sebe-akkaunt-v-Facebook). – 2014. – 24.05).***

***

Днями запрацював новий інформаційний ресурс із назвою «КіберОборона». Він має стати майданчиком для дискусій на тему кібербезпеки в Україні, розповів mediasapiens.ua ініціатор проекту О. Пилипенко. Проект запрацював 26 травня у вигляді сторінки в соціальній мережі Facebook.

«Завдання групи в Facebook під назвою “КіберОборона”: привернути увагу до кібербезпеки країни. Це питання, котрим повинна займатися влада, але наразі не займається в достатньому обсязі, – пояснює О. Пилипенко. – Ми будемо намагатися запросити до участі експертів, журналістів, політологів, громадськість. Думаю, що сьогодні ніхто не сумнівається, що кібербезпека – надзвичайно важливий виклик для держави».

За словами координатора, ідея такого ресурсу визрівала вже давно, однак саме президентські вибори стали каталізатором до прискорення її реалізації. О. Пилипенко нагадує, що 22–25 травня хакери ледь не зірвали проведення виборів. «Те, що раніше вважалося фантастикою – коли за допомогою віруса-трояна та дій кіберзлочинців можна активно впливати на фізичне середовище – раптом стало реальністю», – додає він.

Наразі активісти планують активно просувати сторінку у Facebook. Сайт, націлений на тих, хто не є користувачем соцмережі, мають намір створити пізніше ***(Активісти запустили інтернет-проект «КіберОборона» // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/39516/126/lang,ru/). – 2014. – 29.05).***

***

Пользователи Facebook за несколько часов нашли женщину, похитившую младенца из клиники в пригороде канадского Квебека. Об этом сообщает CNN.

27 мая новорождённая Виктория была похищена из больницы в Квебеке женщиной, одетой в костюм медсестры. Похитительница взяла ребёнка якобы на взвешивание, а в действительности увезла его на красной Toyota Yaris с наклейкой «Ребёнок на борту».

Вскоре после совершения преступления кадры с портретом неизвестной, обнаруженные на записях с камер наблюдения, оказались в Интернете и были показаны местным телевидением.

Четверо двадцатилетних местных жителей увидели сообщение о похищении на Facebook и по собственной инициативе отправились на поиски красной «Тойоты». По дороге к больнице они загрузили фото преступницы на телефон, и одна из участниц стихийной спасательной операции узнала в ней свою соседку по многоквартирному дому.

Прежде чем вызвать полицию, добровольные спасатели отправились к дому, где, по их предположениям, жила похитительница, и нашли на стоянке Toyota Yaris с наклейкой. В окнах квартиры горел свет, а из-за двери слышался шум проточной воды из крана. Полицейским пришлось взломать дверь, чтобы попасть внутрь, но с ребёнком всё было в порядке.

Уже через три часа после исчезновения маленькая Виктория при помощи полиции была возвращена родителям. Вскоре после этого мать и отец малышки встретились с её спасителями и поблагодарили их лично. Позже мать Виктории написала пост с благодарностями на Facebook.

Тысячи людей поделились фотографией этой женщины в социальных медиа. Именно это и спасло нашу маленькую Викторию. Каждый клик, каждый шер повлиял на ситуацию – М. МакМэхон, мать Виктории

Похитительницей оказалась 21-летняя В. Пулин-Коллинз, которую несколько раз задерживали за кражу детских товаров в магазинах и обвиняли в хранении наркотиков.

Власти Квебека обратились к администрации больниц в городе и пригородах, попросив их пересмотреть процедуры безопасности. В качестве меры предосторожности в роддомах предложили делать для новорождённых специальные электронные браслеты, чтобы можно было отслеживать их перемещение в крайних случаях ***(Пользователи Facebook спасли новорожденного ребёнка от похитительницы // InternetUA (http://internetua.com/polzovateli-Facebook-spasli-novorojdennogo-reb-nka-ot-pohititelnici). – 2014. – 29.05).***

***

Силу социальных сетей не стоит недооценивать. Правильный хештег и несколько фото в Instagram смогли обратить внимание известного международного космического консорциума Sea Launch на работу

шестиклассников из донецкой школы, пишет AIN.UA (http://ain.ua/2014/05/30/526555).

В апреле в Украине проходил финал Robotica – всеукраинского конкурс по робототехнике для детей и подростков. Школьники из Донецкого лицея информационных технологий № 61 делали для конкурса архитектурный проект на тему «космическое пространство». И выбрали создание плавучего космодрома Sea Launch. Это реально существующий космодром в экваториальных водах Тихого океана, с которого уже 15 лет на орбиту выводят спутники. Макет, собранный из 8000 лего-блоков, попал в пятерку победителей. Но история – не совсем об этом.

Во время создания макета (с января по апрель) один из кураторов донецкой команды И. Шихат-Саркисов делал фото макета и выкладывал его в Instagram, подписывая хештегами #robotica2014, #lego #legography и #sealaunch.

«Каково же было мое удивление, когда недавно кто-то начал лайкать эти, уже достаточно старые фотки», – рассказывает он. Лайки были от официального Instagram консорциума Sea Launch. Кстати, платформа Sea Launch выводит на орбиту спутники с помощью, в том числе, ракет украинского производства – Zenit 3SL.

Почти сразу после лайков и комментариев вышел на связь директор по маркетингу и продажам Sea Launch с предложением обсудить эти фото. В результате пресс-служба консорциума подготовила статью и фоторепортаж о работе украинских школьников, и вывесила у себя на сайте. «Мы аплодируем этим школьникам за их интерес к науке, технике, робототехнике, «Морскому старту» и поздравляем их с победой! Для нас большая честь, что студенты выбрали для своего проекта именно платформу Odyssey», – пишут в компании. Лицею пообещали прислать поздравление с победой в конкурсе.

Напомним, ранее И. Шихат-Саркисову с помощью Facebook и «ВКонтакте» удалось собрать деньги на открытие робототехнического клуба в Донецке ***(Как Instagram свел донецких школьников с топами глобальной космической компании // AIN.UA (http://ain.ua/2014/05/30/526555). – 2014. – 30.05).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Facebook и Publicis Groupe заключили широкое соглашение, в рамках которого французский холдинг потратит сотни миллионов долларов на рекламу.

Instagram также является частью сделки. Как отметил представитель Facebook, соглашение «фокусируется на сферах digital-маркетинга, которые включают данные, сторителлинг и онлайн-видео рекламу, предоставляя клиентам агентств новые возможности».

Соглашение делает уникальным тот факт, что Facebook смог предоставить доступ к новым рекламным продуктам и инсайтам об аудитории, которые ранее были недоступны.

Publicis должен разработать рекламные инструменты для интеграции с Facebook Audience Network, которая была запущена на мобильных девайсах в прошлом месяце. У Publicis также будет доступ к видеорекламе Instagram и Facebook. Facebook отметил, что будет сотрудничать с Publicis для создания рекламы для автоматически проигрываемого видео, которое расположено справа в ленте пользователей. Как отмечают источники Ad Age стоимость сделки около 500 млн дол. ***(Facebook и Publicis Groupe заключили многомиллионную рекламную сіделку // Marketing Media Review (http://mmr.ua/news/id/facebook-i-publicis-groupe-zakljuchili-mnogomillionnuju-reklamnuju-sdelku-39704/). – 2014. – 20.05).***

***

Принадлежащий Google YouTube достиг договоренности о покупке популярного сервиса Twitch, ведущего видеотрансляцию компьютерных игр, пишет Variety со ссылкой на неназванный источник. Сумма сделки, по сведениям Variety, превысит 1 млрд дол. О ней может быть объявлено в ближайшее время. Представители компаний информацию не комментируют.

The Wall Street Journal (WSJ) со ссылкой на свои источники написала, что переговоры о сделке, действительно, ведутся, но находятся на ранней стадии. Газета напоминает, что у YouTube есть встроенный сервис видеотрансляции, но он не пользуется такой популярностью, как Twitch. По данным сетевой видеокомпании Qwilt, на которую ссылается WSJ, месяц назад через Twitch шло 44 % трафика потоковых трансляций США.

Покупка Twitch может стать самой значительной сделкой в истории YouTube, купленного в 2006 г. Google за 1,65 млрд дол.

Аудитория Twitch, по данным самой компании, насчитывает 45 млн человек в месяц. Функция видеотрансляции компьютерных игр используется на видеоприставках последнего поколения – Xbox One и Playstation 4 ***(YouTube покупает популярный сервис видеоигр за $1 млрд // Версии.com (http://www.versii.com.ua/news/303932/). – 2014. – 20.05).***

***

Facebook запускает систему видеорекламы за пределами США. Согласно анонсу компании, данная инициатива увеличивает потенциальную аудиторию 15-секундных роликов, которые пользователи видят автоматически в новостных лентах, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-videoreklamu-za-predelami-ssha-39723/).

Видеореклама впервые начала появляться в американской версии Facebook в декабре этого года. Для Facebook она является дополнительным источником дохода. Изначально в видеорекламе количество роликов было

существенно ограничено, но сейчас в Facebook говорят, что компания заключила соглашения с большим количеством рекламодателей, в том числе и тех, что ранее выбирали телевизионную рекламу.

Со вторника Facebook начала продавать рекламу на семи рынках за пределами США, в том числе на рынках Австралии, Бразилии, Канады, Франции, Германии, Японии и Великобритании ***(Facebook запускает видеорекламу за пределами США // Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-videoreklamu-za-predelami-ssha-39723/). – 2014. – 21.05).***

***

Почему не стоит публиковать посты в Facebook, когда ваши поклонники в сети

Сервис Facebook Insights предлагает администраторам страниц много возможностей анализа, в том числе и функцию, позволяющую узнать, когда ваши поклонники находятся онлайн, пишет Marketing Media Review (http://mmr.ua/news/id/pochemu-ne-stoit-publikovat-posty-v-facebook-kogda-vashi-poklonniki-v-seti-39751/). Звучит, на первый взгляд, неплохо. Давно известно, что время публикации поста имеет первостепенное значение. Каким же образом это знание может помочь в выборе времени публикации постов?

Вывод специалистов ресурса Wisemetrics довольно неожиданный: планирование публикации на время, когда большинство поклонников находятся в сети, – это стратегия с низкой эффективностью. На самом деле, когда в сети много пользователей, каждый из них старается поделиться контентом, от чего интенсивность обмена растет. Вместе с интенсивностью растет и конкуренция между сообщениями в новостной ленте, что в свою очередь уменьшает шансы сообщений брендов быть замеченными.

Резюме: публикация постов в периоды, когда наибольшее число поклонников страницы находятся онлайн, означает усиление конкуренции и – с высокой вероятностью – значительное уменьшение охвата.

Давайте ознакомимся с результатами исследования и в конце сделаем главный вывод.

Сначала заметим, что статистика «когда ваши поклонники в сети» показывает не время чтения ваших постов подписчиками страницы, а любое присутствие их в Facebook – на сайте или в мобильных приложениях.

Специалисты Wisemetrics проанализировали 5 тыс. страниц различного размера. Для каждой из них они определили оптимальный день и час публикаций, а также установили, сколько поклонников находится онлайн в это оптимальное время.

Дневная статистика

Результаты оказались неутешительными: количество поклонников онлайн в понедельник, во вторник и в любой другой день недели остается приблизительно неизменным. Так что день недели не влияет на количество

поклонников онлайн. Максимальное количество поклонников онлайн отличается от среднего значения всего на 1,6 %.

И что интересно, для 52 % страниц, оптимальным днем публикации оказался четверг, когда конкуренция самая высокая.

Обратите внимание, что эти выводы справедливы для всех страниц, независимо от их размера: в оптимальный день поклонников онлайн только на 2 % больше, чем обычно, даже для страниц с количеством подписчиков менее 1 тыс.

В среднем, для любой страницы ежедневное количество поклонников онлайн составляет 84 %. Это намного выше, чем ежедневное присутствие пользователей Facebook, которое, по данным социальной сети, составляет 61 %. Причина в том, что из 39 % пользователей Facebook, которые не заходят в Facebook каждый день, лишь немногие являются подписчиками на страницы ввиду своей низкой активности в соцсети.

Резюме: ежедневно Facebook посещают 61 % пользователей социального сервиса, в то время как дневная аудитория последователей страниц достигает 84 %.

Почасовая статистика

Почасовая статистика весьма динамична: присутствие пользователей Facebook онлайн неравномерно в течении суток. Однако проблема в том, что пик посещений соцсети подписчиками страниц совпадает с пиком присутствия в Интернете всех пользователей Facebook: почти 30 % присутствия приходится на период между 21:00 и 22:00.

И в этом нет большой пользы для продвижения поста: если поклонники всех страниц находятся онлайн в одно и то же время, они получают контент от всех своих друзей, находящихся онлайн, в одно и то же время (в том числе и контент от конкурирующих страниц, которые также знают, когда их поклонники онлайн).

Оптимальное время публикации влияет на эффективность постов

Важно не то, когда ваши поклонники находятся онлайн, а то, когда в их лентах новостей есть свободное пространство для ваших сообщений. Для оценки оптимального времени публикации, эксперты Wisemetrics измерили охват аудитории в зависимости от времени дня и дня недели для каждой из 5 тыс. страниц.

Дневная статистика

Время публикации действительно влияет на эффективность постов, и разница в количестве охваченных пользователей Facebook составляет не 1,6 % (как в случае с учетом статистики присутствия поклонников онлайн), а все 30 %. И, кстати, оптимальным днем по наибольшему охвату в более половины случаев является не четверг – каждый день имеет свой потенциал.

Резюме: в среднем, выбирая оптимальный день для публикации поста, можно увеличить охват аудитории на 30 %.

Обратите внимание, что воскресенье является лучшим днем для многих страниц, в то время, как с точки зрения присутствия поклонников онлайн это самый неподходящий день для публикаций.

Почасовая статистика

Оптимальным временем является не 21:00 – исследователи отметили много пиков, которые могут быть использованы для привлечения внимания аудитории.

Резюме: публикация постов в Facebook во время наибольшего присутствия онлайн ваших поклонников, как правило, является не очень хорошей идеей.

Главный вывод

Необходимо установить оптимальное время для публикации постов в соцсетях. При правильном подходе к определению этого времени можно увеличить органический охват в среднем на 30 % (по данным авторов описанного выше исследования).

Не стоит полагаться только на статистику присутствия ваших поклонников онлайн. Публикации в такие периоды могут наоборот привести к уменьшению охвата из-за высокой конкуренции в лентах новостей пользователей. При определении наилучшего времени для публикаций нужно учитывать статистику охвата постов в разное время суток и в разные дни недели ***(Почему не стоит публиковать посты в Facebook, когда ваши поклонники в сети // Marketing Media Review (http://mmr.ua/news/id/pochemu-ne-stoit-publikovat-posty-v-facebook-kogda-vashi-poklonniki-v-seti-39751/). – 2014. – 22.05).***

***

Социальные сети – будущее для нативной рекламы

В рамках фестиваля Internet Week в Нью-Йорке, который состоялся на прошлой неделе, издание издательская компания MediaPost провела конференцию OMMA Social, пишет Marketing Media Review (http://mmr.ua/news/id/socialnye-seti-buduschee-dlja-nativnoj-reklamy-39792/).

Конференция началась с вопроса об уменьшении органического охвата в Facebook – вплоть до однозначных цифр, согласно отчету Social@Ogilvy, и стоило ли платить за охват в Facebook.

Все участники дискуссии были единодушны в том, что в результате существующего положения вещей их клиенты, рекламодатели брендов, достигли более высокого уровня, по сравнению со старыми добрыми временами, когда бесплатно пользовались органическим охватом, покупая лайки для увеличения армии фанатов и нацеливаясь на охват и частоту. Теперь, они больше внимания уделяют вовлечению и результатам для бизнеса. Фактически, некоторые из них отвергли большой охват, назвав его неэффективным, если фанаты не предпринимают действий.

Кроме того, бренды не собираются исключать Facebook из своего маркетингового микса. Скорее наоборот, готовы увеличить его использование.

Масс-медиа с новыми возможностями

Большое количество пользовательского контента и взаимодействий, которые произошли на платформе за все годы ее существования, вместе с географической, демографической информацией о пользователях, означает, что у Facebook есть возможность таргетировать аудиторию очень детально.

Кроме того, с запуском видеорекламы на Facebook, рекламодатели могут достичь предполагаемых 90 млн уникальных пользователей каждый день.

Значение для агентств и клиентов

Так как Facebook все больше продает рекламу напрямую брендам, медиа агентства, которые раньше занимались размещением рекламы, оказались под риском, что их услуги больше не понадобятся. Кроме того, интерфейсы для самообслуживания Facebook, Twitter, YouTube, LinkedIn, означают, что менеджера по маркетингу сами могут управлять или оптимизировать свою кампанию.

И, наконец, блестящий пример от Л. Хендерсон, Mondelez, о том, как корпоративная команда установила студию по видео-продакшену в режиме реального времени. Студия будет производить короткие брендированные видео в ответ на новости, которые оказываются в тренде в определенное время – чтобы бренд мог принять участие в диалогах или в актуальных темах.

Как получить преимущество от естественной рекламы в сетях?

Рекламодатели теперь активно стараются создать контент и комментарии, которые фанаты найдут ценными для того, чтобы поделиться ими или быть вовлеченными. Большинство брендов новички в таком виде рекламы. Чтобы позволить себе стать участником диалога между реальными пользователями, который происходит в Facebook, им нужно предоставить нечто актуальное, полезное и развлекательное. «Если естественная реклама является подлинной и полезной, оставьте ее, если она предполагает, что реклама должна стать контентом, забудьте о ней».

CEO Shareablee Т. Юкки дает несколько практических советов:

– бренды должны размещать посты чаще, а не реже, чтобы расти каждый месяц;

– бренды должны платить за спонсируемые посты, чтобы достичь менее активных фанатов, но не слишком полагаться на оплату в охвате;

– бренды должны сосредоточиться на качестве развлечения – для бренда ценным является не лайк, а расшаривание. Взаимодействие с брендом более одного раза.

Социальные сети – будущее для естественной рекламы

Вместо того, чтобы рассматривать социальные сети как рекламу – какое количество бренд может показать и какому количеству пользователей –

рекламодатели могут использовать сети для достижения потенциала естественной рекламы. Лучше всего, если пользователи сами будут говорить о вас и рекомендовать вас своим друзьям. Поэтому дело не в количестве рекламных сообщений, органических или спонсируемых, а в том, хотят ли пользователи взаимодействовать с вами и вовлекать своих друзей ***(Социальные сети – будущее для нативной рекламы // Marketing Media Review (http://mmr.ua/news/id/socialnye-seti-buduschee-dlja-nativnoj-reklamy-39792/). – 2014. – 26.05).***

***

Портал Social Media Examiner представил результаты 6-го ежегодного исследования соцмедиа индустрии 2014 г. Social Media Marketing Industry Report. В ходе исследования был проведен опрос более 2800 представителей отрасли, которые ответили на самые разные вопросы о своей работе.

Преимущества использования SMM

92 % маркетологов отметили, что работа в социальных сетях увеличивает узнаваемость бренда. 80 % также назвали увеличение трафика. 72 % респондентов утверждают, что SMM помогает развивать лояльность подписчиков. 71 % заявили, что благодаря соцмедиа получают маркетинговые инсайты, а 66 % – генерируют лиды.

Социальные платформы

Как и следовало ожидать, самая популярная социальная медиаплатформа для работы – Facebook. Также респонденты отметили Twitter, LinkedIn, YouTube, платформы для блоггинга, Google+, Pinterest и Instagram.

Примечательно, что Facebook, YouTube, Pinterest и Instagram используют в основном B2C-компании, а LinkedIn, Google+ и блоггинг – B2B.

Эффективность использования

Только 43 % маркетологов считают, что их усилия в Facebook приносят результат.

Время на работу

64 % респондентов тратят на социальные медиа 6 часов в неделю и более, 37 % – 11 и более часов в неделю, 19 % маркетологов – более 20 часов в неделю. Причем специалисты SocialMediaExaminer отметили интересный факт – чем моложе маркетолог, тем больше времени на SMM он тратит.

Планы на будущее

Респонденты планируют увеличить затраты на использование блогов (68 %), YouTube (67 %), Twitter (67 %), LinkedIn (64 %) и Facebook (64 %). Несмотря на популярность сервиса Snapchat, 85 % опрошенных заявили, что не собираются использовать его в работе. 68 % маркетологов также отметили, что использование геолокации не входит в их планы.

Платформы, о которых хотелось бы узнать больше

Несмотря на то что Google+ считается платформой-призраком, 65 % респондентов хотели бы узнать о ней больше. Более 50 % маркетологов также отметили LinkedIn, Facebook, Twitter и YouTube.

Реклама в социальных сетях

Практически все респонденты используют рекламу в Facebook – 90 %. Также участники опроса отметили рекламу в LinkedIn и Twitter – 20 % и 17 % соответственно.

Аутсорсинг

27 % респондентов заявили, что используют в своей работе аутсорсинг: дизайн/разработка (14 %), создание контента (12 %), аналитика (10 %), мониторинг (7 %), исследования (6 %).

Контент

94 % респондентов самостоятельно создают письменный контент, 73 % – курируют чужой, 60 % работают с собственным визуальным и видеоконтентом, 22 % с собственным аудиоконтентом.

Более 60 % маркетологов хотели бы узнать больше о том, как создавать хороший визуальный и видеоконтент.

ROI

Только 37 % респондентов заявили, что измеряют социальную активность.

Другие форматы маркетинга

Помимо социальных сетей, маркетологи также активно используют email-маркетинг (85 %) и поисковое продвижение (65 %) ***(50 % маркетологов не уверены в эффективности своих действий на Facebook // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/50_marketologov_ne_uvereny_v_effektivnosti_svoih_deystviy_na_facebook). – 2014. – 28.05).***

***

Twitter и Omnicom заключили партнёрство в области автоматизированной закупки мобильной рекламы, пишет Marketing Media Review (http://mmr.ua/news/id/twitter-i-omnicom-zakljuchili-reklamnuju-sdelku-na-230-mln-dollarov-39821/).

В рамках соглашения сеть автоматизированной закупки рекламы Accuen, принадлежащая Omnicom, интегрируется с мобильной рекламной платформой MoPub, приобретённой сервисом микроблогов в сентябре 2013 г. На первом этапе продолжительность сотрудничества компаний составит два года.

«Это наше первое соглашение с холдинговой компанией, которое мы подписываем в сегменте мобильной рекламы. И этот шаг является для нас очень важным и ценным, поскольку позволит нам заполучить первоклассных рекламодателей. Мы не делали специального заявления по поводу предоставления Twitter возможностей автоматизированной закупки рекламы.

Тем не менее, это вполне логичный и естественный шаг», – комментирует ситуацию А. Бейн директор Twitter по глобальным доходам.

«Наше соглашение с Twitter демонстрирует серьёзность взглядов на медиа-партнёрство. Мы предоставляем существенные преимущества всем своим клиентам: от уникальных возможностей размещения контента до удобных инструментов измерения эффективности рекламных стратегий», – сообщается в заявлении пресс-службы Omnicom.

Напомним, что в апреле 2014 г. Twitter запустил полноценный рекламный функционал для разработчиков мобильных приложений на базе существующей рекламной платформы. Инструмент разработан на основе технологии MoPub.

Впервые информация о том, что Twitter готовится представить новый формат рекламы мобильных приложений – App-install Ads – появилась в отраслевых СМИ начале марта 2014 г. Планировалось, что новинка привлечёт дополнительное количество рекламодателей из числа представителей e-commerce и лидеров игровой индустрии ***(Twitter и Omnicom заключили рекламную сделку на 230 млн долларов // Marketing Media Review (http://mmr.ua/news/id/twitter-i-omnicom-zakljuchili-reklamnuju-sdelku-na-230-mln-dollarov-39821/). – 2014. – 28.05).***

***

Федеральное агентство по туризму (Ростуризм) разместило заявку на популяризацию отдыха в Крыму в социальных сетях. Как сообщает BuisinessFM, на продвижение крымских пляжей через Facebook, Twitter и «ВКонтакте» для начала потратят 500 000 р. (170 910 грн).

За эту сумму Ростуризм хочет получить специальные группы в соцсетях. Например, в Facebook должно появиться две группы: для бизнеса и для простых туристов. От исполнителя работ требуется наполнить каждую группу 20–50 видеороликами и фотографиями, а также поддерживать общение с подписчиками.

Контракт рассчитан на период 1 июня – 30 сентября 2014 г. Будет ли дальше кто-то поддерживать созданные в соцсетях группы, неизвестно.

BuisinessFM напоминает, ранее Министерство туризма России констатировало, что поток отдыхающих в 2014 г. упал в 2–2,5 раза по сравнению с прошлым годом. Отели и санатории заполнены всего на 28–30 % ***(Ростуризм попробует спасти крымский сезон через Twitter // rusNEWS.info (http://rusnewsinfo.ru/ekonomika/24471-rosturizm-poprobuet-spasti-krymskiy-sezon-cherez-twitter.html). – 2014. – 30.05).***

***

Соцсеть «ВКонтакте» покажет записи матчей чемпионата мира по футболу в Бразилии, а также другой связанный с турниром фото- и

видеоконтент. Об этом lenta.ru сообщил исполнительный директор соцсети Д. Сергеев.

По его словам, в настоящее время соцсеть пытается договориться о показе прямых трансляций игр ЧМ-2014. «Вопрос с правами (на прямые трансляции) пока до конца не решен, но мы рассчитываем и на них», – сказал Д. Сергеев.

«ВКонтакте» в случае достижения договоренности о прямых трансляциях будет показывать их через видеоплеер сайта Sportb~~ox~~.ru спортивного портала, входящего в состав холдинга ВГТРК.

Чемпионат мира по футболу пройдет с 12 июня по 13 июля в 12 городах Бразилии ***(«ВКонтакте» покажет матчи чемпионата мира по футболу // Media бізнес (http://www.mediabusiness.com.ua/content/view/39511/126/lang,ru/). – 2014. – 29.05).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Исследователи Университета Квинсленда, Австралия, установили, что пользователи социальных сетей могут впадать в депрессию, если их очередная заметка не вызывает бурных обсуждений.

Причиной тому, утверждают специалисты, является подсознательное желание любого человека быть популярнее других людей и всегда находиться в центре внимания.

Более того, в отдельных случаях не только настроение, но и физическое самочувствие автора может напрямую зависеть от популярности его записей в социальной сети.

Чтобы установить взаимосвязь между настроением и популярностью в социальной сети, исследователи попросили группу активных пользователей Facebook разделиться на две команды. Первая группа активно пользовалась соцсетью, пока вторая должна была лишь пассивно наблюдать.

Через два дня участники второй группы начали испытывать проблемы с самоощущением: им начало казаться, что они стали незаметными для остальных, и исключёны из общества.

Это, в свою очередь, послужило для участников эксперимента источником проблем с самооценкой и они стали хуже себя контролировать ***(Пользователи соцсетей впадают в депрессию, если их записи***

непопулярны // InternetUA (http://internetua.com/polzovateli-socsetei-vpadauat-v-depressiua--esli-ih-zapisi-nepopulyarni). – 2014. – 18.05).

***

Австралийские специалисты нашли способ отслеживать настроения людей со всего мира, используя сеть микроблогов Twitter.

Инструмент под названием We Feel сканирует 32 тыс. Twitter-постов в минуту, что составляет около 10 % всех англоязычных записей. Система ищет 600 ключевых слов, связанных с такими эмоциями, как любовь, радость, удивление, гнев, печаль и страх.

Собранные данные можно использовать для отслеживания эмоций отдельных пользователей и целых общин в разных регионах. На основе такой выборки можно довольно точно установить целесообразное место для размещения, к примеру, спасательных служб.

Аналитики отмечают, что нельзя недооценивать значение подобной информации – исследователи психического здоровья сегодня ориентируются на программы здравоохранения с использованием устаревших данных о населении, которым иногда даже больше 5 лет.

Мониторинг социальных сетей, в свою очередь, предоставляет более актуальную картину ментального состояния масс.

Пока что программа анализирует только англоязычные записи и не собирает информацию о гендерной идентичности и местоположении пользователей социальной сети – эти недостатки учёные планируют исправить в ближайшее время ***(В Twitter можно наблюдать за ментальным здоровьем пользователей // InternetUA (http://internetua.com/v-Twitter-mojno-nabluadat-za-mentalnim-zdorovem-polzovatelei). – 2014. – 22.05).***

***

У США жінки є значно активнішими користувачами соціальних медіа, ніж чоловіки. Такого висновку дійшли журналісти видання Financesonline.com, проаналізувавши дані Pew Research Center та Burst Media.

За результатами аналізу спеціалісти Financesonline підготували інфографіку, яка демонструє порівняння активності у соціальних мережах чоловіків та жінок. Порівнювалися дані за п’ятьма найбільш популярними ресурсами – Facebook, Tumblr, Pinterest, Instagram, Twitter та LinkedIn.

Більше за жінок чоловіки користуються лише соціальною мережею для працівників та роботодавців LinkedIn.

З’ясувалося, що жінки більш активно взаємодіють із брендами у соціальних мережах, а також отримують новини на цих ресурсах частіше за чоловіків. Крім того, жінки активніше, ніж чоловіки, користуються соціальними мережами на мобільних пристроях – смартфонах та планшетах.

Візуальними соціальними медіа, такими як Tumblr, Pinterest, Instagram також активніше користуються жінки ***(У США жінки користуються***

соціальними мережами активніше за чоловіків // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/30965). – 2014. – 26.05).

Маніпулятивні технології

Боты в соцсетях: сделать ложь ярче правды

Тот, кто говорит, что деньги не могут купить друзей, видимо, не сталкивался с социальными сетями. Ведь там по цене чашки кофе можно купить несколько тысяч новых знакомых в Twitter. А если добавить еще пару долларов, тогда можно добавить столько же друзей и в Facebook. Конечно, это будут не люди, а боты, но свою главную задачу – поднять популярность любого желающего – они выполняют. А реальный пользователь не отличит, что тысячи виртуальных друзей его любимого кумира – это купленный за 5 дол. набор программ.

Подобной методикой раскрутки часто пользуются звезды и другие публичные люди. Таким способом они могут показать себя на виртуальном пространстве ярче, чем они есть на самом деле. Ведь поисковая выдача соцсетей в первую очередь учитывает число друзей, последователей, читателей и тому подобное.

Чтобы обзавестись 4 тыс. новых последователей в Twitter, понадобится всего 5 дол. Такое же количество друзей в Facebook стоит столько же. А если надо, чтобы они проявили активность, например, поставили лайк, тогда придется доплатить сверху несколько долларов. За 3700 дол. компьютерные эксперты обещают добавить в Instagram целый миллион друзей. А если к этой сумме прибавить 40 дол., тогда 10 тыс. из этих новых подписчиков полюбят одно фото заказчика и поставят ему лайк.

В Интернете есть много площадок, где можно купить друзей дешево. Среди самых популярных – Swenzi и Fiverr. Большинство новых виртуальных знакомых проживают в Индии, Бангладеш, Румынии, России и других отдаленных от США и Европы странах. Но это не мешает им выглядеть очень натурально, чтобы реальные пользователи верили.

Умный бот – доверчивый пользователь

Программы выдают себя за реальных юзеров уже много лет, и их было сравнительно легко отличить. У таких ботов были случайные аватарки (чаще всего – женское фото) и сгенерированные компьютером имена вроде Инна2841.

Сегодня же роботы значительно поумнели и маскируются практически идеально. Они называют себя реальными именами, работают только днем, а посреди ночи «отдыхают». Более того, они обмениваются фотографиями и другим контентом между собой и даже затевают разговоры. Отличить такого бота от действительно живого пользователя Интернета с первого взгляда практически нереально.

Этим воображаемым гражданам Интернета удалось стать довольно мощной силой в виртуальном пространстве. Они легко делают звезд и компании популярней, чем те есть на самом деле. Они также могут манипулировать общественным мнением благодаря различным дискуссиям, которые ведут в нужную заказчику сторону.

«Я работал с ботами для соцсетей довольно долгое время, и теперь они не отличаются от реальных живых пользователей, хотя на самом деле таковыми не являются», – отмечает Т. Вонг. Он работает главным исследователем в группе Pacific Social Architecting Corporation, которая изучает, как боты и технологии формируют социальное поведение.

Как рождаются боты

Для создания виртуальных роботов используют различные методики. Одна из самых популярных – это использование готового инструментария под названием Zeus. Его можно купить примерно за 700 дол. и с помощью сравнительно простой панели управления контролировать армию ботов. В качестве последних выступают миллионы зараженных ПК пользователей.

Боты уже много лет используются не только для увеличения популярности звезд, но и для более глобальных заданий. Например, во время президентских выборов 2012 г. в Мексике партию Institutional Revolutionary Party обвинили в использовании ботов с целью «утопить» сообщения политических оппонентов в Twitter и Facebook. Еще одна большая группа ботов работала в Сирии, где угрожала каждому, кто писал в соцсетях о протестах или лидерах оппозиции. А один из самых недавних случаев использования роботов случился в Турции. Расследование показало, что каждая политическая партия управляла своей армией ботов, которые выводили в топ обсуждения нужные им темы и тенденции.

Боты под прицелом

Компаниям, которые владеют соцсетями, не нравится, что их сервисы наводнили роботы, которые фактически умеют руководить реальными пользователями. Google, Facebook, Twitter и другие тратят много усилий на очистку своего виртуального пространства от ботов. Например, Twitter провела масштабную работу по чистке перед публичным размещением акций, удалив миллионы аккаунтов. А Google убрал сотни миллионов просмотров на YouTube, которые сделали боты. В это же время киберзлоумышленники придумывают новые способы обхода – они уже даже используют искусственный интеллект, чтобы оставаться впереди.

«Это эволюционный процесс, – говорит Т. Вонг. – Компании придумывают совершенные фильтры, которые ведут к улучшенным ботам». Один из примеров подобного – программное обеспечение Simon Z. Оно покупает у реальных людей информацию: аватары, фотографии и разговоры. Этим удается эмулировать поведение человека, и примерно 100 тыс. таких сегодня активно трудятся в YouTube, Facebook, Twitter, Vine, Instagram и SoundCloud.

«Это все ради власти и контроля – то же самое, что можно наблюдать в реальном мире, – говорит исполнительный директор компании по безопасности Support Intelligence Р. Вессон. – Теперь разница только в том, что все в цифровой форме и можно сделать намного больше».

Боты развиваются

Сегодня боты в социальных сетях просто обманывают людей, поднимают популярность звездам, компаниям или манипулируют общественным мнением. Все это происходит в виртуальном пространстве. Но боты становятся изощренней и уже научились влиять на повседневную жизнь, например, на направление движения при поездках.

В марте студенты израильского Института технологий создали новый тип ботов, который научился обманывать навигацию Google. Последний владеет сервисом Waze – это соцсеть для водителей, которая благодаря их отзывам помогает другим прокладывать оптимальные маршруты.

Созданные студентами боты оказались очень продвинутыми: они имитировали смартфоны Android, которые получали фальшивые сигналы GPS в фальшивых машинах с такими же водителями. Программное обеспечение Waze не распознало обман и поверило, что эти боты действительно едут по дороге в пробке. Из-за этого реальные живые водители вынуждены были по совету соцсети объехать несуществующее препятствие по другому маршруту ***(Боты в соцсетях: сделать ложь ярче правды // InternetUA (http://internetua.com/boti-v-socsetyah--sdelat-loj-yarcse-pravdi). – 2014. – 18.05).***

***

Російська влада готується до масованої маніпуляції громадською думкою в закордонних інтернет-ЗМІ та соціальних мережах, вдавшись до використання ботів та тролінгу.

Як пишуть Ведомости, у Кремлі почали розробляти цю програму ще восени 2013 р., а куратором цього проекту називають В. Володіна, заступника голови адміністрації президента Росії. Нова стратегія була створена після того, як взимку 2011 р. у багатьох містах Росії пройшли масові опозиційні мітинги та акції протесту, які самоорганізувались у соціальних мережах та за сприяння онлайн-ЗМІ. Діджитал-пропаганда В. Суркова не подіяла, і його було звільнено.

Роботу В. Володіна на внутрішньому ринку визнали настільки ефективною, що було вирішено спрямувати сили й на закордонні медіа. Ефект від такої стратегії став помітний уже тепер: всього кілька тижнів тому британські журналісти з The Guardian заявили про масовану атаку проросійськи налаштованих ботів, які в коментарях до новин та статей возвеличували політику Росії та В. Путіна. Аналогічне зростання кількості проросійських повідомлень показав і контент-аналіз німецьких онлайн-ЗМІ.

У мережу виклали документи, які є своєрідними гайдлайнами для роботи «проросійських» тролів. І, що цікаво, команди підрядників, що є

безпосередніми виконавцями пропаганди Кремля, розташовані по всьому світу – у США, Німеччині, Індії, Таїланді та інших країнах. Переважно виконавці – це вихідці з Росії. З документів стало зрозуміло, що онлайн-пропаганда Кремля детально проаналізувала більшість медіа, соцмереж та навіть окремих спільнот і готується активно «обробляти» їх на користь Росії ***(Кремль готує масовану атаку онлайн-пропаганди в західних ЗМІ і соцмережах // UkrainianWatcher (http://watcher.com.ua/2014/05/21/kreml-hotuye-masovanu-ataku-onlayn-propahandy-v-zahidnyh-zmi-i-sotsmerezhah/). – 2014. – 21.05).***

***

Група компаній «1+1 Медіа» звернулася до керівників офісів соціальних мереж Facebook, Twitter, «Одноклассники», «ВКонтакте», а також до Секретаря РНБО стосовно фактів постійного поширення в соціальних мережах закликів до порушення територіальної цілісності України, сепаратизму і тероризму на території самопроголошених усупереч Конституції України Донецької та Луганської «народних республік», які створюють істотні загрози національній безпеці України. Про це повідомляє прес-служба групи.

«1+1 Медіа» у своєму зверненні закликає керівників офісів соціальних мереж вжити заходів із блокування груп та сторінок, які системно допускають відкриті заклики до сепаратизму, тероризму та схвалення дій протизаконних збройних формувань сепаратистів та інших військових спецпідрозділів, що ведуть військові дії проти легальних українських спецпідрозділів та Національної гвардії на території самопроголошених Донецької та Луганської «народних республік»; заклики до екстремістської діяльності всупереч як українському, так і міжнародному законодавству; опублікування списків громадян з фотографіями, адресами, номерами телефонів із закликами до вчинення над ними «самосуду» та насилля; розпалювання міжнаціональної ворожнечі, висловлювання дискримінаційного характеру за ознаками національності, громадянства, політичних уподобань; оприлюднення інформації, що не відповідає дійсності та направлена на маніпулювання свідомістю громадян. Перелік основних таких груп у соціальних мережах додані до звернення.

«Ми не виступаємо проти свободи слова та вільного висловлення своїх думок і не підтримуємо введення державної цензури. Ми розуміємо як це, бо саме канали нашої медіа-групи відключила самопроголошена влада Донецької та Луганської “народних республік”. Ми розуміємо, що на даний час нормативне регулювання порядку створення, використання чи закриття доступу до таких інтернет-ресурсів в Україні відсутнє. Ми впевнені, що подібні проблеми у демократичній країні цілком можуть вирішуватись за допомогою механізмів саморегулювання. Тим більше, що діяльність подібних груп не тільки суперечить законодавству, але й грубо порушує

умови та правила самих соціальних мереж», – ідеться у зверненні «1+1 Медіа».

У зверненні до Ради національної безпеки та оборони «1+1 Медіа» пропонує створити робочу групу, яка об'єднає спеціалістів у галузі інформаційної безпеки, для розробки загального плану дій щодо боротьби з інформаційними проявами сепаратизму, тероризму, що поширюються через соціальні мережі. А також у разі доцільності розробити законодавчий процес врегулювання цієї проблеми та визначити державні органи, які мають фіксувати подібні порушення.

Зі свого боку «1+1 Медіа» висловлює готовність взяти активну участь в опрацюванні зазначених питань у складі робочої групи ***(«1+1 Медіа» закликала керівників соцмереж заблокувати групи сепаратистів // «Телекритика» (http://www.telekritika.ua/kontekst/2014-05-22/93940). – 2014. – 22.05).***

***

Днями Росія вдалася до чергового витка пропагандистської війни. Цього разу у Twitter. 27–28 травня великою групою російських ботів було запущено акцію #savedonbasspeople та #savedonbaspeople. Головне повідомлення акції – «врятуйте жителів Донбасу від української армії». Акція стартувала у Twitter, але досить швидко поширилась і в інших соцмережах.

Як це вже стало звично, цинічність російської пропаганди не має меж. В акції використовуються фотографії вбитих дітей, які не мають жодного відношення до нинішніх подій в Україні. Наприклад, росіяни поширюють у Twitter фото дитини, нібито вбитої українськими військовими. Хоча це фото 4-річної давнини вбитого хлопчика якимось божевільним у Криму.

Не гребують підробляти фотографії М. Обами, дружини президента США (хоча не факт, що вони знають, хто вона така) та речника Держдепартаменту США.

Досить дивно виглядають шахтарі, які спустились у забій і фотографуються з зображеннями поліграфічної якості.

Ну і, звісно, спалені українцями церкви на Донбасі, виявились спаленими церквами в Росії.

Українці досить швидко зорієнтувались і розпочали свою контрпропагандистську кампанію з тими самими хештегами ***(#savedonbasspeople: протистояння українських активістів організованій російській пропаганді в Твітері // UkrainianWatcher (http://watcher.com.ua/2014/05/30/savedonbasspeople-protystoyannya-ukrayinskyh-aktyvistiv-orhanizovaniy-rosiyskiy-propahandi-v-tviteri/). – 2014. – 30.05).***

Сеть Tor не может защитить интернет-пользователей от программ слежения спецслужб. Об этом сообщило издание The Inquirer со ссылкой на эксперта Microsoft, основателя Cyber Crime Security Forum Э. Мэлоуна. По его словам, несмотря на устойчивую и надежную природу Tor, использование сетью сторонних дополнений означает, что существуют способы слежения и похищения пользовательской информации. Напомним, ранее сообщалось о том, что Агентству национальной безопасности США не удалось взломать Tor.

«В Интернете нет возможности быть по-настоящему анонимным. Если ты нужен им (хакерам или спецслужбам), они тебя достанут», – заявил Э. Мэлоун. Он подтвердил, что до настоящего времени информация о том, что Tor когда-либо был взломан, отсутствует, однако в сети есть уязвимости, которые можно эксплуатировать.

По словам эксперта, утечки в Tor могут происходить через сторонние приложения и дополнения, такие как Flash. «Если бы я проводил экспертизу вашей активности и знал, что вы используете Tor, я бы не атаковал саму сеть, а только слабые места вокруг», – пояснил он.

Э. Мэлоун рассказал о нескольких способах, с помощью которых хакеры или правительственные ведомства могут следить за пользователями. Они способны осуществлять атаки по времени, перехватывая трафик между узлами сети, мониторить авторизацию и выход из Tor, эксплуатировать уязвимости нулевого дня и т. д. Более того, правительственные ведомства активно работают над созданием более прямых путей осуществления атак на сеть для слежения за его пользователями ***(Tor не способен остановить слежение за пользователями // InternetUA (http://internetua.com/Tor-ne-sposoben-ostanovit-slejenie-za-polzovatelyami). – 2014. – 17.05).***

***

Согласно информации, опубликованной канадской управляющей широкополосной компанией Sandvine, объем зашифрованного интернет-трафика растет по всему миру. Действия Э. Сноудена, в результате которых было открыто огромное количество секретной информации, стали причиной того, что пропускная способность, потребляемая зашифрованным трафиком, выросла в два раза в Северной Америке, а в Европе и Латинской Америке – в четыре раза.

В новом отчете, опубликованным Sandvine, указывается что BitTorrent теряет свою популярность в США, продолжая свой рост в Европе. По сравнению с прошлым годом, в 2014 г. зафиксирован рост зашифрованного трафика.

Изменения наиболее ярко выражены в Европе, где процент зашифрованного интернет-трафика в периоды пикового времени увеличился за год в четыре раза – с 1,47 до 6,10 %. В Северной Америке процент

зашифрованного интернет-трафика в час пик возрос в текущем году с 2,29 до 3,80 %. В среднем абсолютный интернет-трафик увеличивается на 20–40 % каждый год, пропускная способность, потребляемая зашифрованным трафиком удваивается в этот период.

Рост объема зашифрованного трафика является глобальным явлением. В Латинской Америке доля SSL увеличилась с 1,8 до 10,37 % за год. Кроме того, подобную ситуацию можно наблюдать в сетях мобильной связи, где зашифрованный трафик также растет.

Изменения зашифрованного трафика можно связать с наблюдениями Э. Сноудена. В результате, число пользователей VPN-сервиса резко возросло. Кроме того, Google вместе с другими веб-сервисами перешли по умолчанию на SSL ***(Объем зашифрованного интернет-трафика растет по всему миру // InternetUA (http://internetua.com/obem-zashifrovannogo-internet-trafika-rastet-po-vsemu-miru). – 2014. – 17.05).***

***

Один из «отцов-основателей» Рунета, известный блоггер А. Носик в статье для американского журнала The New Republic рассказывает об истории Интернета в России, которая, по его мнению, может завершиться уже этим летом, а то и раньше.

Как передает InoPressa.ru, начинается статья с воспоминаний о встрече группы интернет-деятелей с В. Путиным в декабре 1999 г., незадолго до того, как он впервые приступил к исполнению обязанностей президента России. «Теперь в это трудно поверить», пишет А. Носик, но в тот день он «торжественно пообещал уважать и охранять сетевую свободу слова и коммерческой деятельности», отдельно упомянув о том, что китайская и вьетнамская модели представляются ему неприемлемыми.

Слова В. Путина вызвали у присутствующих «озадаченность и недоверие», вспоминает автор, поскольку «всем было известно о том, как в 1980-х он, будучи оперативником КГБ, гонялся в Ленинграде за диссидентами. Честно сказать, многие из нас подумали, что сказанное В. Путиным – это скорее дымовая завеса, чем подтверждение серьезных намерений. Мы опасались правительства и ждали худшего. К счастью, мы ошибались».

В. Путин «держал слово на протяжении следующих 13 лет», говорится в статье. «С 2000 по 2012 год направленные на регулирование Интернета законопроекты, которые кто только не вносил, начиная от мэра Москвы Ю. Лужкова до министров правительства... немедленно хоронились и забывались, так как их не поддерживал президент. В результате Интернет в России превратился в единственную конкурентоспособную отрасль... Кроме того, Интернет стал единственной в России территорией ничем не скованной свободы слова».

Какова же была причина такой политики? Тому есть несколько объяснений, полагает автор: «Либо президент был уверен, что российский

сегмент Интернета (так называемый Рунет) всегда будет слишком мал, чтобы быть значимым, или же он просто не хотел позориться перед «большой восьмеркой» чересчур китайским поведением. А может быть, был искренне уверен в действенности стратегии его советников, в соответствии с которой следовало не закрывать антиправительственные сайты, а создавать проправительственные... Так или иначе, дав обещание не вмешиваться, В. Путин действовал в соответствии с ним почти 13 лет. К сожалению, сейчас эти счастливые 13 лет позади, и мы наблюдаем быстрое и беспощадное уничтожение сетевой свободы».

Как В. Путин в одночасье превратился в «параноидального ненавистника Интернета»

«Никто не может сказать, что заставило В. Путина впоследствии изменить свое мнение об опасности сетевой свободы. Кто-то говорит, что на него произвела впечатление революция в Молдавии, в результате которой в 2009 г. было смещено пророссийское коммунистическое правительство, ведь ее катализатором явился Twitter. Я сильно сомневаюсь в истинности этого предположения, поскольку В. Путин не стал бы выжидать три года после кишиневских событий, прежде чем на них отреагировать. Другие указывают на «арабскую весну», видя в ней поворотную точку... С этой гипотезой я тоже не согласен. Мубарак не был другом В. Путина, а парня, который им был (Муаммара Каддафи), свергли и убили воинствующие племена, на которых Интернет никакого видимого влияния не оказывал. В том, что В. Путин вдруг в одночасье превратился в параноидального ненавистника Интернета, повинны московские акции протеста 2011–2012 годов», – убежден А. Носик.

Перечисляя недавно принятые Госдумой законы, которыми фактически вводится цензура Интернета, он отдельно останавливается на правовой норме, обязывающей интернет-компании хранить информацию на серверах, физически расположенных на территории России, и без всяких дополнительных санкций передавать ее российским правоохранительным органам.

«5 мая 2014 г. этот законодательный шедевр в духе Д. Оруэлла был подписан В. Путиным. 1 августа 2014 г. он вступает в силу. Станет ли этот день последним для российского Интернета? – задается вопросом А. Носик. – Может, и так. Если какой-нибудь новый закон не убьет его еще раньше» ***(А. Носик: Путин 13 лет держал слово охранять сетевую свободу, но летом Рунету может прийти конец // InternetUA (http://internetua.com/anton-nosik--putin-13-let-derjal-slovo-ohranyat-setevuua-svobodu--no-letom-runetu-mojet-priiti-konec). – 2014. – 18.05).***

***

Сервіс мікроблогів Twitter заблокував у Росії акаунт «Правого сектора». Доступ до облікового запису @PravyjSektorRus, згідно з повідомленням на сторінці, закритий для користувачів мережі в Росії.

Найцікавіше, що акаунт не оновлюється із 17 квітня. Та й раніше він не був надто активним. На нього підписано трохи більше 3 тис. фоловерів.

Наразі офіційної причини заборони ніде немає, але ймовірно, що блокування акаунта пов'язане з нещодавними заявами Роскомнадзора, який вимагав від Twitter та Facebook блокування сторінок, які в Росії визнано екстремістськими. Тобто Twitter пішов на зустріч вимогам російської влади.

Напевно настав вже час і українській владі взятись за екстремістсько-фашистські російські групи в соцмережах «ВКонтакте» та «Одноклассники». Українська влада має достатньо важелів впливу на адміністрації цих соцмереж. Наприклад, «ВКонтакте» тримає в Україні свої сервери для кешування даних. І у «ВКонтакте» є вже технологія для обмеження доступу до окремих акаунтів у соцмережі за регіональним принципом – росіяни не мають доступу до більшості популярних українських групп, пов'язаних з «Євромайданом» та «Правим Сектором».

Як ви ставитесь до блокування доступу в Україні до російських нацистських спільнот, що пропагують ненависть до українців? ***(Twitter заблокував доступ росіян до Правого сектора. Пора українській владі братись за російські соцмережі // UkrainianWatcher (http://watcher.com.ua/2014/05/19/twitter-zablokuvav-dostup-rosiyan-do-pravoho-sektora-pora-ukrayinskiy-vladi-bratys-za-rosiyski-sotsmerezhi/). – 2014. – 19.05).***

***

По решению Генпрокуратуры оказались заблокированными несколько роликов YouTube и записей в блогах, призывающих к участию в митинге против В. Путина, который должен был пройти 18 мая. Об этом сообщается на сайте Antizapret.info.

По решению Генпрокуратуры 18 мая был ограничен доступ к серии роликов на видеохостинге YouTube и некоторым записям в блогах, содержащих призывы к несанкционированному митингу. Он должен был состояться в 9 часов вечера на Манежной площади в Москве и в других городах по всей России.

В реестр запрещённых сайтов были также внесены сайт manezka2014.com, публиковавший новости об аналогичных митингах, и несколько блогов на платформах LiveJournal и Blogspot, публиковавших анонсы будущего митинга. По состоянию на 14:00 19 мая ни одиз из 17 заблокированных ресурсов не был доступен, а вместо страниц отображалось сообщение о блокировке.

Судя по фотографиям, опубликованным в соцсетях 18 мая неподалёку от Манежной площади, акция так и не состоялась.

Как сообщала «Независимая газета», на 18 мая был запланирован несанкционированный митинг с лозунгом «Долой Путина из Кремля». Его организаторы остались неизвестными, а информация об акции распространялась через соцсети и блоги.

Представители официальных протестных групп (например, «Солидарность» и РПР-ПАРНАС) открестились от участия в акции, назвав её провокацией националистов, и заявили, что отговаривали своих членов идти на этот митинг. Предполагается, что 18 число было неслучайно, так как цифры 1 и 8 являются шифром имени Адольфа Гитлера, замечает «Независимая газета».

Информацию о готовящемся митинге 16 мая якобы прокомментировал (в контексте «Правого сектора») министр обороны Донецкой народной республики И. Стрелков ***(Генпрокуратура РФ заблокировала серию блогов и роликов YouTube за призывы к митингу против Путина // InternetUA (http://internetua.com/genprokuratura-rf-zablokirovala-seriua-blogov-i-rolikov-YouTube-za-prizivi-k-mitingu-protiv-putina). – 2014. – 19.05).***

***

Спецслужби США і ЄС провели одну з наймасштабніших операцій за останні роки: під час розслідування було затримано 97 хакерів у всьому світі, які підозрюються у прихованому стеженні за людьми через веб-камери.

Як пише The Telegraph, стеження проводилося за допомогою шпигунського ПЗ Blackshades Remote Access Tool, яке втручалося в роботу вашої ОС та активовувало веб-камеру без вашого відома. Зазвичай жертвами шпигунів ставали люди, які клікали на шахрайське посилання, що прийшло їм на пошту або через соціальні мережі.

Скандал почався із США, де хакер таким чином зняв оголені фото переможниці конкурсу Miss Teen USA і був ув'язнений на 18 місяців. Окрім того, зловмисники часто вимагали у жертв гроші в обмін на не-публікацію приватних чи компроментуючих фото, знятих на вебкамеру.

Ураження хакерським програмним забезпеченням зазнали понад 700 тис. користувачів ***(Спецслужби арештували 97 хакерів, які приховано стежили за людьми через веб-камери // UkrainianWatcher (http://watcher.com.ua/2014/05/20/spetssluzhby-areshtuvaly-97-hakeriv-yaki-pryhovano-stezhyly-za-lyudmy-cherez-veb-kamery/). – 2014. – 20.05).***

***

Соединенные Штаты планируют выдвинуть против нескольких китайских военнослужащих обвинения в экономическом шпионаже против американских компаний. В 19 мая генеральный прокурор США Э. Холдер провел пресс-конференцию, на которой рассказал подробнее об этих обвинениях. Этот случай станет первым в истории, когда правительство США возбуждает уголовные дела против официальных лиц иностранной державы по обвинениям в кибер-преступлениях.

Судебный процесс по данному делу ознаменует столкновение интересов двух крупнейших экономик мира. По объему производства США в два раза опережает Китай. Однако некоторые аналитики считают, что по

ряду других показателей Китай может уже в течение года обойти США, став самой крупной экономикой мира.

В 2013 г. издания The New York Times и The Wall Street Journal сообщили о кибернападении со стороны китайских хакеров на их компьютерные системы. Ранее американские эксперты выступали с заявлениями о том, что Китай занимается взломом сетей в США и других странах для того, чтобы определить источники утечек информации в своем правительстве.

Пресс-секретарь Министерства иностранных дела Китая назвал «безответственным» заявление американского Минюста.

Китайские власти в свою очередь требуют от американских спецслужб разъяснений относительно слежки за деятельностью компании Huawei, в компьютерную систему которой якобы внедрилось Агентство национальной безопасности США. Кроме того, как следует из доклада о развитии Интернета в Китае, в 2013 г. китайские веб-сайты и компьютеры подверглись множественным зарубежным кибератакам. Кроме того, более 10,9 млн компьютеров в Китае попали под контроль зарубежных серверов, 30 % которых находились в США ***(США выдвигают официальные обвинения против хакеров из Китая // InternetUA (http://internetua.com/ssha-vidvigauat-oficialnie-obvineniya-protiv-hakerov-iz-kitaya). – 2014. – 19.05).***

***

Соединенные Штаты готовятся опубликовать список российских чиновников, причастных к кибершпионажу в отношении американского государства. Об этом пишет The Wall Street Journal со ссылкой на собственные источники в американском правительстве. О каких именно персонах идет речь, не сообщается… ***(США обвинят Россию в кибершпионаже вслед за Китаем // InternetUA (http://internetua.com/ssha-obvinyat-rossiua-v-kibershpionaje-vsled-za-kitaem). – 2014. – 21.05).***

***

Созданное интернет-предпринимателем П. Омидьяром издание The Intercept приводит новые данные, компрометирующие АНБ США. Согласно данным издания, американское разведведомство без каких-либо санкций и уведомлений перехватывало «виртуально все» сотовые звонки на Багамских островах. Правительство островного государства ничего не знало о данных действиях американского ведомства.

Данная разведывательная операция АНБ носила название SOMALGET и была инициирована по просьбе американского антинаркотического ведомства. Сообщается, что разведчики смогли выявить уязвимости в багамской сотовой инфраструктуре и получили доступ к звонкам пользователей. По данным, переданным Э. Сноуденом, АНБ перехватывало и записывало данные, а также серверные журналы багамских сотовых операторов. В статье за авторством Л. Поитрас, Г. Гринвальда и Р. Деверо

говорится, что на Багамах АНБ применяло достаточно продвинутые инструменты шпионажа, которые предоставляли информацию не только о метаданных, но и о самих звонках.

SOMALGET – это часть более широкой шпионской программы Mystic, которая предусматривала мониторинг со стороны АНБ США телекоммуникационных систем не только на Багамах, но и в Мексике, Филиппинах, Кении и других странах. Всего у АНБ в рамках Mistic были технические возможности по мониторингу звонков примерно 250 млн человек. В случае с Багамами, АНБ интересовали, в основном, переговоры наркоторговцев, но в других странах интересы прослушки были шире.

В статье говорится, что программы SOMALGET и Mistic являются иллюстрацией американской внешней разведдеятельности. Также авторы публикации говорят, что руководство АНБ лжет, когда говорит, что вело прослушку только выборочную и данные утечки говорят о массовых прослушках людей, которые ни к политике, ни к криминалу отношения не имеют. Кроме того, в официальных документах США Багамы декларируются как «государство стабильной демократии» и не представляющее террористической угрозы для США ***(Опубликованы новые данные о шпионаже АНБ США на Багамах // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/04/21/bahamas-nsa-espionage.html). – 2014. – 21.05).***

***

Використання органами державної влади України «Антивіруса Касперського» є небезпечним, оскільки він може віддалено блокувати роботу комп’ютерів та передавати дані користувачів російським спецслужбам. Про це йдеться в результатах дослідження на замовлення українського уряду, частина якого опинилася у розпорядженні видання AIN.UA.

Експерти виявили, що використання антивірусних продуктів «Лабораторії Касперського» є ризикованим. Причиною цьому, зокрема, є безконтрольна передача інформації від комп’ютера до серверів компанії з можливістю подальшого використання нею цих даних. Може йтися, у тому числі про передачу відомостей правоохоронним органам Російської Федерації.

Зазначається також, що засновник компанії Є. Касперський закінчив Вищу школу КДБ (сьогодні Інститут криптографії, зв’язку та інформатики Академії ФСБ Росії). Крім того, «Лабораторія Касперського», як зауважують автори дослідження, постійно співпрацює із ФСБ РФ щодо надання інформації, аналізу та розслідування інцидентів, консультацій у сфері інформаційної безпеки.

Видання AIN.UA звернулося про «Лабораторії Касперського» за коментарями, однак у прес-службі заявили, що вважають аналітичний документ не є дослідженням, а спробою маніпуляцій на тлі загострення ситуації в Україні.

«Всі наші продукти регулярно перевіряються та сертифікуються, в тому числі на предмет відсутності “закладок”. Kaspersky Lab не упереджена в питанні забезпечення інформаційної безпеки незалежно від політичної ситуації. Ми впевнені, що клієнти вибирають продукти безпеки з точки зору об’єктивних критеріїв, поділяють нашу позицію і не стануть жертвами подібних провокацій», – відповіли в прес-службі «Лабораторії Касперського».

Напередодні виборів зловмисники на деякий час вивели з ладу ІТ-інфраструктуру Центрвиборчкому, у результаті чого в Інтернет потрапили паролі доступу та структура комп’ютерної мережі організації, нагадує AIN.UA. Тоді голова Держспецзв’язку В. Звєрєв пояснив, що зловмисники змогли дістатися до серверів організації через те, що встановлений на комп’ютері адміністратора ЦВК антивірус «Касперського» не працював. У «Лабораторії Касперського» на це відповіли, що їхній антивірус не міг запобігти такого виду атакам ***(«Антивірус Касперського» може передавати дані держустанов України російським спецслужбам – ЗМІ // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/31040). – 2014. – 28.05).***

***

Китайским банкам предписано отказаться от серверов американской корпорации IBM. Власти Китая считают, что это оборудование может использоваться американскими властями для шпионажа. Поднебесная продолжает отказываться от продуктов и услуг компаний из США в ответ на претензии, предъявляемые Вашингтоном.

Китайское правительство потребовало от местных банков отказаться от серверов, выпущенных американской корпорацией IBM, и заменить их аналогами китайских производителей, сообщает Bloomberg со ссылкой на осведомленные источники.

Государственные организации, включая Народный банк Китая и министерство финансов, в настоящее время выясняют, угрожает ли использование серверов IBM финансовой безопасности государства. Расследование пока сохраняется в тайне.

Новое указание китайских властей последовало после того, как Министерство юстиции США опубликовало имена и фотографии пяти китайских хакеров, обвинив их в промышленном шпионаже в пользу азиатского государства.

«Безопасность – превыше всего, – прокомментировал председатель пекинской консалтинговой компании BDA China Д. Кларк. – Сегодня Китай не нуждается в американских поставщиках, как это было в последние несколько десятков лет».

В случае отказа китайских финансовых учреждений от оборудования IBM, продажи компании в этой стране упадут еще сильнее. По итогам I квартала 2014 г. выручка IBM в Китае сократилась на 20 % в сравнении год

к году – в большей степени по сравнению с любым другим государством в группе BRIC (Бразилия, Россия, Индия, Китай). Объемы продаж IBM во всей группе в указанный период снизились на 11 %.

В общей сложности в I квартале на Китай пришлось около 5 % всей выручки IBM. Несмотря на столь малое значение, этот регион является важным для IBM. В начале года гендиректор IBM Д. Рометти дважды посещала Поднебесную для того, чтобы восстановить доверие местных заказчиков к американскому поставщику. Оно было подорвано после того, как бывший сотрудник АНБ и ЦРУ Э. Сноуден раскрыл информацию о деятельности американской разведки. Из документов выяснилось, что спецслужбы США устанавливают жучки в том числе в оборудование китайских вендоров.

Отношения между Китаем и США накалились после того, как в 2012 г. американские власти обвинили в шпионаже крупнейших китайских производителей оборудования связи Huawei и ZTE. В марте 2014 г. выяснилось, что США сами использовали оборудование Huawei для шпионажа. Китайские власти назвали обвинения США необоснованными и приостановили сотрудничество с ними в области кибер-безопасности.

На прошлой неделе регуляторы Китая запретили использование в правительственных структурах новых ПК на платформе Microsoft Windows 8, объяснив этот шаг нежеланием сохранять зависимость от иностранного поставщика программного обеспечения.

Накануне стало известно, что Пекин предписал государственным компаниям сократить свои связи с американскими консалтинговыми агентствами, такими как McKinsey, Boston Consulting Group, Bain и другими известными игроками консалтингового рынка в связи с подозрениями в шпионаже в пользу американского правительства ***(Китай отказывается от серверов IBM из-за подозрений в шпионаже // InternetUA (http://internetua.com/kitai-otkazivaetsya-ot-serverov-IBM-iz-za-podozrenii-v-shpionaje). – 2014. – 28.05).***

***

Национальный совет по поддержанию мира и порядка Таиланда заблокировал доступ интернет-пользователей к ряду аккаунтов в социальной сети Facebook, сообщила 28 мая таиландская газета The Phuket News.

Как заявил представитель временных властей Таиланда, речь идет лишь о блокировке ряда политически ориентированных страниц социальной сети. Эта мера не должна препятствовать доступу пользователей к их личным аккаунтам, говорится в сообщении.

Между тем, по данным издания, интернет-пользователи в ряде районов Таиланда испытывают трудности с доступом к Facebook, размещая об этом твиты в Twitter. Phuket News, ссылаясь на неназванные источники, отмечает, что речь может идти о блокировке около 30 млн аккаунтов Facebook на территории Таиланда.

Агентство Reuters позже в среду днем сообщило со ссылкой на тайских пользователей, что они снова могут нормально заходить на Facebook. Кроме того, по данным Reuters, некий представитель военных опроверг факт блокировки соцсети.

А еще чуть позже официальный представитель Министерства информации и коммуникационных технологий заявил Reuters, что Facebook действительно был временно заблокирован. Кроме того, 29 мая временные власти Таиланда намерены встретиться с представителями компаний Twitter и Instagram, чтобы попросить их о сотрудничестве – пресекать распространение в соцсетях призывов к протестам против армии ***(Из Таиланда сообщили о блокировке соцсети Facebook // InternetUA (http://internetua.com/iz-tailanda-soobsxili-o-blokirovke-socseti-Facebook). – 2014. – 28.05).***

***

Российская телекоммуникационная компания «Ростелеком» заблокировала на территории РФ доступ к сайту популярного мобильного приложения для обмена анонимными сообщениями Secret.ly.

Сайт был добавлен в Единый реестр запрещённых ресурсов и заблокирован. При этом само мобильное приложение на момент написания статьи работает.

В Secret.ly можно писать анонимные сообщения, которые видят друзья пользователя и друзья его друзей. Контакты друзей приложение берёт из телефонной книги, социальных сетей Twitter, Facebook и прочих.

В свою очередь представители «Ростелекома» уточняют, что сайт Secret.ly стал «заложником обстоятельств»: решением суда был закрыт доступ к одному из ресурсов с противоправными материалами.

Так как доступ к сайтам с информацией, запрещённой в России, блокируется только по его IP-адресу, ресурс Secret.ly попал под блокировку, поскольку его адрес совпал с адресом сайта с противоправными материалами ***(В России заблокировали сайт анонимной социальной сети Secret // Блог Imena.UA (http://www.imena.ua/blog/rostelekom-zablokiroval-sajt). – 2014. – 29.05).***

***

Украинские клиенты МТС – под колпаком? Дело о возможной прослушке абонентов расследует СБУ, изучает вопрос и Нацкомиссия по регулированию связи. Кстати, основной владелец МТС, российский бизнесмен – В. Евтушенков. Именно с ним якобы встречался В. Янукович, накануне вильнюского саммита, где должны были подписать Соглашение об Ассоциации.

МТС – расскажи об Украине ФСБ. Такие фотожабы в последнее время появляются в Интернете. И, возможно, не случайно. В апреле Нацкомиссия

по вопросам регулирования связи установила: Россия вмешивалась в работу МТС. По сути – велась прослушка.

И. Сиротенко, бывший член национальной комиссии по вопросам регулирования связи и информации:

«Подтверждено, что есть возможность узнать местонахождение абонента и возможность прослушивать разговоры абонента. Например, если солдат в танке с мобильным телефоном находиться в каком-то месте, можно примерно определить, где это. В этой ситуации МТС должна была обеспечить все условия, чтобы вмешательства в их сеть не было».

Проверка показала – данные о звонках перенаправлялись на узел связи в Санкт-Петербурге. В МТС этого не отрицают. Но говорят – о вмешательстве они сами сообщили, после чего и началась проверка.

В. Рубан, пресс-секретарь МТС:

«Наши технические специалисты отследили нехарактерную последовательность сигналов. Мы естественно об этих случаях проинформировали. Эта проблема, которая имеет вообще отношение вообще к технологии GSM. Это не нарушение со стороны МТС. Это угроза для всех сетей всех абонентов».

С выводами комиссии в МТС не согласны, и пошли в суд. Говорят – защититься от вмешательства не могут. Мол, государство должно утвердить новые нормы сертификации оборудования.

Проверяли МТС по обращению СБУ, говорит нацрегулятор. В мае комиссия готовила акт о повторном нарушении, поскольку компания не защитила свое оборудование. Но выдать документ – не успела. На следующий день руководство и состав нацкомисиии сменили.

А. Семенченко, председатель национальной комиссии по вопросам регулирования связи и информации:

«Комісія тільки приступила до своєї роботи, ми вивчаємо. Справа знаходиться в суді, є там питання такі, які не можна виносити на загал».

В закрытом режиме рабочая группа по МТС заседала уже дважды. А в состав комиссии, к слову, вошел бывший работник МТС. А. Довгий еще в мае работал в компании.

Т. Попова, председатель правления интернет-ассоциации Украины:

«Все, что происходило в комиссии, все совещания, они проходили за закрытыми дверями, нас как общественность, на них не приглашали, поэтому мне сложно сейчас сказать о том, какое у этой комиссии мнение».

Впрочем, вопрос завис не только в Нацкомиссии. В суде тоже. Первое заседание должно было быть 6 мая. Его перенесли – на середину июня. А на время судебных перипетий решать судьбу оператора регулятор не может.

Л. Ошеров, председатель совета Украинской ассоциации операторов связи «Телас»:

«Могут лишить лицензии, придется им по новому покупать лицензию, но это все зависит от того, что там будет выяснено в ходе работы».

Д. Тымчук, руководитель Центра военно-политических исследований:

«Действительно очень многие представители различных структур коммерческих и некоммерческих, и в государственных структурах были случаи, когда работают на другую сторону. СБУ эти факты выявляет».

В СБУ пока молчат. Телеканал «Интер» ждет ответа на официальный запрос. Россия же и дальше может спокойно использовать отработанную схему прослушки.

И. Сиротенко, бывший член национальной комиссии по вопросам регулирования связи и информации:

«Не хотите, чтобы знали ваше местонахождение – выключите мобильный телефон, не хотите, чтобы вас прослушивали – не ведите по этому телефону такие разговоры».

К слову, контрольный пакет акций МТС Украина – принадлежит российской компании МТС ***(Лысенко Е. Клиенты МТС могут оказаться под колпаком у российских спецслужб // InternetUA (http://internetua.com/klienti-mts-mogut-okazatsya-pod-kolpakom-u-rossiiskih-specslujb). – 2014. – 29.05).***

***

Китайские власти начали кампанию по искоренению злоупотреблений при использовании мобильных приложений для обмена сообщениями.

Власти обеспокоены тем, что подобные приложения используют с «целью распространения запрещенной и вредной информации, которая противоречит общественным интересам».

Как заявляет руководство страны, арестованные по подозрению в террористической деятельности признались, что делились информацией об изготовлении взрывчатых веществ через мобильные приложения.

В Китае, где действует ряд ограничений на пользование социальными сетями, большую популярность приобрели мобильные приложения для обмена сообщениями.

Например, приложением WeChat в стране пользуются более 800 млн человек ***(Власти Китая обратили внимание на мобильные приложения // InternetUA (http://internetua.com/vlasti-kitaya-obratili-vnimanie-na-mobilnie-prilojeniya). – 2014. – 29.05).***

***

Иранские хакеры уже три года собирают разведданные о высокопоставленных чиновниках США и других стран при помощи социальных сетей.

Аналитики отмечают, что хакеры из Ирана установили контакты с чиновниками через различные социальные сети, в частности, Facebook и Linkedln. Созданные ими фальшивые личности на собственных страницах постепенно наладили контакты с работниками из интересующих их сфер.

Специалисты по безопасности обнаружили 14 виртуальных профилей людей, никогда не существовавших в реальности. Шестеро из них якобы

были сотрудниками новостного сайта, который размещал материалы новостных агентств. Остальные «работали» в оборонных компаниях.

Заручившись доверием своих «друзей», шпионы постепенно получили доступ к секретной информации: им точно удалось собрать сведения об экономических санкциях в отношении Ирана, а также, о шагах, направленных на предотвращение распространения ядерного оружия.

Среди пострадавших оказались американский адмирал, конгрессмены, члены произраильского лобби AIPAC.

Информацию подтверждает и руководство социальной сети Facebook – корпорация давно обратила внимание на этих хакеров, расследуя жалобы на подозрительные попытки записаться в друзья. В настоящее время все 14 профилей удалены.

В свою очередь американские спецслужбы следили за пользователями, внедряя своих агентов в популярные онлайн-игры. По долгу службы блюстителям национальной безопасности пришлось играть в World of Warcraft и Second Life ***(Иранские хакеры выведывали информацию у американских чиновников через соцсети // Блог Imena.UA (http://www.imena.ua/blog/iran-based-cyberspies/). – 2014. – 30.05).***

***

Кремлёвские комментаторы оптом

Оригинал взят у a_nikonov в «Попалили кремлевскую мразоту»

Собщает normhaa59:

«Сегодня появилось подтверждение тому, что в сети действует команда платных прокремлевских комментаторов.

“Анонимным интернационалом” разоблачена деятельность “Агентства интернет исследований” – кормящейся бюджетными деньгами организации, создающей с помощью заказных комментариев иллюзию поддержки кремлёвского режима в Интернете.

Интересно, что владельцем агентства является основатель холдинга “Конкорд” Е. Пригожин, известный как “повар Путина”, а непосредственное руководство компанией осуществляет М. Купрашевич, известная тем, что устраивалась на работу в либеральные СМИ с целью шпионажа.

Вот сайт, на котором можно подробнее прочесть о случившемся – http://b0ltai.wordpress.com.

А вот сами архивы переписок:

https://mega.co.nz/#!XpgUXIYa!XcjPKUZC7322tKKpls8VPRzB1QkgcAYbhhbNWfag8vE;

https://mega.co.nz/#!X5gSBBBZ!W9Iw2Q_sdkxBbFKR-yhnykQd8V4RQ9tcPt5Gdt128HA

Было выяснено, что существует целый штат людей, работающих в режиме строгой отчетности перед кураторами, и пишущих в Интернете платные проправительственные комментарии.

Средняя з. п. такого “комментатора”, пишущего “политически верные” посты – от 30 до 40 тыс. р. Пропаганда ведется на два фронта – как в российском интернете, так и в заграничном.

Каждый отдел имеет своих “специалистов”, общие траты на которых за прошлый месяц составили 33 млн р.

В качестве подтверждения реальности вышеизложенного, достаточно сравнить сканы паспортов, обнаруженные во взломанной почте с реальными аккаунтами людей в соц. сетях». Материалы представлены в статье на сайте ***(Кремлёвские комментаторы оптом // InternetUA (http://internetua.com/kreml-vskie-kommentatori-optom). – 2014. – 31.05).***

Проблема захисту даних. DDOS та вірусні атаки

В мае 2014 г. специалисты компании «Доктор Веб» выявили и исследовали рекордное по сравнению с предыдущими месяцами количество троянов для ОС Linux, значительная часть которых предназначена для организации DDoS-атак. Об этом CNews сообщили в «Доктор Веб».

По словам экспертов компании, эти вредоносные программы объединяют общие черты. Во-первых, они предназначены для организации DDoS-атак с использованием различных протоколов, а во-вторых, по косвенным признакам можно сделать вывод о том, что большинство исследованных DDoS-троянов создано одним и тем же автором, считают они.

Так, вредоносная программа, добавленная в вирусные базы Dr.Web под именем Linux.DDoS.3, обладает достаточно широким спектром функциональных возможностей. После своего запуска троян определяет адрес командного сервера и отправляет на него информацию об инфицированной системе, а затем ожидает получения конфигурационных данных с параметрами текущей задачи (отчет о ее выполнении также впоследствии отправляется злоумышленникам). Linux.DDoS.3 позволяет осуществлять DDoS-атаки на заданный сервер с использованием протоколов TCP/IP (TCP flood), UDP (UDP flood) и отправляет запросы на серверы DNS для усиления эффективности атак (DNS Amplification).

Еще одна модификация данной угрозы, получившая наименование Linux.DDoS.22, ориентирована на работу с дистрибутивами Linux для процессоров ARM, а Linux.DDoS.24 способен инфицировать серверы и рабочие станции, на которых используются 32-разрядные версии Ubuntu и CentOS. Так, троян Linux.DDoS.24 устанавливается в систему под именем pktmake и автоматически регистрирует себя в параметрах автозагрузки ОС. После запуска он также собирает сведения об аппаратной конфигурации инфицированного компьютера – в том числе о типе процессора и объеме памяти – и отправляет их в зашифрованном виде на принадлежащий киберпреступникам управляющий сервер. Основное предназначение этой

вредоносной программы заключается в выполнении DDoS-атак по команде с удаленного узла.

Следующая группа угроз для ОС Linux, исследованных специалистами «Доктор Веб» в текущем месяце, включает троянов Linux.DnsAmp.1, Linux.DnsAmp.2, Linux.DnsAmp.3, Linux.DnsAmp.4 и Linux.DnsAmp.5. Некоторые вредоносные программы семейства Linux.DnsAmp используют сразу два управляющих сервера и способны инфицировать как 32-разрядные (Linux.DnsAmp.1, Linux.DnsAmp.3, Linux.DnsAmp.5), так и 64-разрядные (Linux.DnsAmp.2, Linux.DnsAmp.4) версии Linux. Подобно другим представителям данного класса DDoS-троянов, Linux.DnsAmp регистрирует себя в автозагрузке, собирает и отправляет на удаленный сервер сведения о конфигурации инфицированной машины (версия ОС, частота процессора, объем свободной памяти и Swap-кэша, и т. д.), после чего ожидает поступления управляющих команд.

Среди возможностей данного класса троянов «Доктор Веб» выделили следующие: SYN Flood (отправка специально сформированного пакета на атакуемый узел до тех пор, пока тот не перестанет отвечать на запросы); UDP Flood (устанавливается соединение с атакуемым узлом по протоколу UDP, после чего троян пытается отправить жертве 1000 сообщений); Ping Flood (с использованием протокола ICMP формируется эхо-запрос, в котором в качестве идентификатора используется PID процесса, а данные представляют собой hex-значение 0xA1B0A1B0); отправка запросов на серверы DNS (DNS Amplification); отправка запросов на серверы NTP (NTP Amplification – в ранних версиях трояна функция реализована, но не используется). Также по команде с удаленного сервера Linux.DnsAmp может записать информацию в файл журнала, повторить атаку или обновиться.

Трояны Linux.DnsAmp.3 (для 32-разрядных версий Linux) и Linux.DnsAmp.4 (для 64-разрядных Linux-дистрибутивов) представляют собой модификации первой версии Linux.DnsAmp с предельно упрощенной системой команд, рассказали в компании. Фактически, эти реализации трояна могут выполнять только три поступающих с управляющего сервера директивы: начать DDoS-атаку, остановить атаку и записать данные в файл журнала. Примечательно, что многие из перечисленных выше вредоносных программ используют одни и те же управляющие серверы.

Наконец, в «Доктор Веб» упомянули о вредоносной программе для ARM-совместимых дистрибутивов Linux, получившей наименование Linux.Mrblack. Этот троян также предназначен для выполнения DDoS-атак с использованием протоколов TCP/IP и HTTP. Он имеет довольно примитивную архитектуру и, подобно другим аналогичным угрозам, действует по команде с управляющего сервера.

Как удалось выяснить компании, командные центры, с использованием которых осуществляется управление упомянутыми троянскими программами, располагаются преимущественно на территории Китая, и реализованные с их помощью DDoS-атаки направлены, в основном, против

китайских интернет-ресурсов ***(DDoS-трояны атакуют Linux // InternetUA (http://internetua.com/DDoS-troyani-atakuuat-Linux). – 2014. – 17.05).***

***

Киберпреступники постоянно обнаруживают новые способы осуществления успешных атак на компании для кражи финансовых данных. Об этом сообщается в отчет ИБ-компании Trend Micro об угрозах в I квартале 2014 г. «Киберпреступники атакуют неожиданные цели».

Жажда наживы мотивирует киберпреступников искать нетрадиционные подходы в выборе маловероятных, порой неожиданных целей, например, осуществляя чрезвычайно сложные атаки на POS-терминалы. Несмотря на то, что эти системы являются хорошо защищенными, злоумышленники ищут различные хитроумные способы обхода защиты.

По данным экспертов, в I квартале текущего года продолжает активно использоваться вредоносное ПО для online-банкинга. Более того, появились его новые разновидности и семейства, предназначенные для разных целей и использующие разнообразные способы обхода обнаружения.

Также эксперты отметили рост мобильных угроз. Так, по их данным, количество вредоносного ПО достигло 2 млн с тех пор, как появилась платформа Android. «Для того чтобы оставаться защищенными от этих постоянно меняющихся киберугроз, пользователи должны исправно использовать передовой опыт для работы с Интернетом, особенно при проведении финансовых транзакций», – отметил главный технический директор Trend Micro.

В отчете говорится, что в I квартале нынешнего года появилось большое количество эксплоитов нового поколения. Эти приложения позволяют анонимно обмениваться контентом и отправлять сообщения без возможности перехвата. Кроме того, возросло количество атак с использованием социальной инженерии ***(В поисках наживы киберпреступники атакуют неожиданные цели // InternetUA (http://internetua.com/v-poiskah-najivi-kiberprestupniki-atakuuat-neojidannie-celi). – 2014. – 17.05).***

***

Google и Facebook объявили, что они недавно удалили 4000 подозрительных учетных записей рекламодателей, связанных с более чем 2400 сайтами технической поддержки. Этот шаг объяснился заявлением, что Google и Facebook объединились вместе с AOL, Twitter и Yahoo для того, чтобы повысить осведомленность пользователей на тему вредоносной рекламы.

Фальшивая техническая поддержка дает советы жертвам, которые считают, что они общаются с представителями техподдержки от легальных компаний. Получив несколько жалоб, Google и Facebook начали

расследование технологий веб-сайтов по факту обмана пользователей, и, как следствие, их жалоб.

Как оказалось, мошенники стали больше изощряться для обмана жертвы через рекламу, которая появляется, когда пользователь выполняет поиск в Интернете. Когда потенциальная жертва набирает номер технической поддержки, указанный в объявлении или на веб-сайте, фальшивые представители call-центра пытаются убедить абонентов загрузить файл на свой компьютер. Если пользователь делает это, на его компьютер пользователя загружаются вредоносные программы, которые могут быть использованы для кражи его личных данных: информации о счетах, логины, пароли, номера кредитных карт и прочее.

Эксперты советуют пользователям никогда не соглашаться предоставлять кому-либо свои пароли по телефону, и никогда не предоставлять доступ к своему компьютеру. Лучше всего сразу обратиться на оригинальный веб-сайт производителя или к доверенным лицам ***(Google и Facebook удалили подозрительные учетные записи рекламодателей // InternetUA (http://internetua.com/Google-i-Facebook-udalili-podozritelnie-ucsetnie-zapisi-reklamodatelei). – 2014. – 18.05).***

***

Создание национальной операционной системы не только повысит уровень защиты государственных информационных ресурсов и информационно-коммуникационных сетей, но и уменьшит зависимость госорганов от иностранных вендоров программного обеспечения, уменьшит затраты государства на поддержку этого ПО, считает программист, доцент Кафедры вычислительной техники НТУУ «КПИ» С. Стиренко. Это важная задача государственного масштаба, сказал он в эксклюзивном интервью журналистам телеканала БТБ.

«В целом большинство развитых стран имеют такую операционную систему. Она есть в России, во Франции и во многих других странах», – сказал С. Стиренко. Эксперт отметил, что создание такой системы избавит государство от необходимости платить лицензионные отчисления разработчикам ПО.

«Есть смысл на базе открытых операционных систем, например, GNU/Linux, сделать разработку на базе уже готового ядра, дописать какие-то сервисы с подключением своих драйверов и подготовить специальный пакет прикладных программ, также открытых, для того, чтобы как минимум государственные учреждения могли использовать это программное обеспечение для своих целей, – считает эксперт. – Технически это сложная задача, однако она под силу украинским специалистам».

«Кроме того, чтобы просто разработать эту ОС, нам понадобится создать для нее центр технической поддержки. Это должна быть группа разработчиков и технических специалистов, которые будут отслеживать новые тенденции, мониторить существующую ситуацию и, возможно,

дописывать какие-то модули, приобретают актуальность. Однако мы получаем в этом случае видимые преимущества. Современное открытое программное обеспечение является достаточно качественным и защищенным, с открытыми кодами. Это позволит нам самим дорабатывать продукт, чтобы он был максимально приспособленным к нашим украинским реалиям. И центр компетенции, который должен находиться у нас. То есть мы никогда не будем зависеть от какого-то иностранного вендора, который обычно закрывает коды. Также в этой операционной системе не будет никаких зловредных программ, которые могут красть информацию. Это очень важно для наших специальных служб, защиты и сохранения персональных данных», – рассказал С. Стиренко ***(Что может усилить кибербезопасность Украины? // InternetUA (http://internetua.com/cto-mojet-usilit-kiberbezopasnost-ukraini). – 2014. – 18.05).***

***

Журналисты Reuters, со ссылкой на свои источники в Google, заявили, что веб-гигант уже начал получать запросы на удаление данных в соответствии с «правом быть забытым». Согласно недавнему постановлению Европарламента, жители Евросоюза имеют право потребовать от Google удалить из поисковой выдачи ссылки на недействительную или устаревшую информацию.

Решение было принято 13 мая, и с тех пор интернет-гигант получил огромное количество запросов от людей, желающих стереть данные о себе из сети. В настоящее время в компании думают над тем, как технически наладить механизм удаления, введя автоматизированную систему.

Согласно новому закону Европейского Союза, каждый гражданин может обратиться к администратору любого веб-сайта с просьбой удалить информацию, касающуюся этого человека, если эта информация отображается в поисковой выдаче. Если администрация не удалит эту информацию, веб-сайт может быть оштрафован в соответствии с европейскими законами.

На сегодняшний день Интернет работает, как агрегатов информации, и, если в него попадают какие-либо данные, вывести их из сети практически невозможно. Вероятно, постановление Евросоюза сможет запустить механизмы обратного процесса, позволяющего пользователям не только добавлять информацию, но и удалять ее ***(Пользователи интернета хотят удалить в Google информацию о себе // InternetUA (http://internetua.com/polzovateli-interneta-hotyat-udalit-v-Google-informaciua-o-sebe). – 2014. – 17.05).***

***

Пользователи социальной сети «ВКонтакте» сообщают о новом трояне, ориентированном на русскоязычных пользователей смартфонов.

Вредоносное приложение получает доступ к мобильному устройству и пытается заразить телефоны других абонентов из адресной книги.

На смартфон приходит SMS следующего содержания: «Привет Тебе фото: https://materzoptom. ru/rzxf/868329010990269» или «Здравствуйте, позвоните мне срочно 0025229724044». Отправителем может быть как абонент из адресной книги, так и неизвестный номер. При переходе по ссылке предлагается установить вредоносное приложение, что многие пользователи и делают не задумываясь.

Установленная на смартфон программа рассылает аналогичные SMS всем людям из списка контактов в телефоне. Соответственно, за каждое сообщение снимаются деньги. Предположительно, вирус опасен только для смартфонов под управлением Android, так как на iPhone, при переходе по ссылке, ничего установить не предлагается.

Злоумышленники зарабатывают с помощью трояна, контролируя функции Android-аппарата. Зараженный гаджет может совершать звонки или отправлять SMS-сообщения на платные номера, спровоцировав огромные телефонные счета для пользователя. Так как журнал очищается, человек не может узнать об отправке данных.

Эксперты советуют ни в коем случае не проходить по присланной ссылке и не звонить, а просто удалить это сообщение со смартфона. Также при получении такого SMS со знакомого вам номера телефона постарайтесь сообщить владельцу номера о заражении его телефона вирусом ***(В соцсети «ВКонтакте» сообщили о рассылке Android-трояна посредством SMS // InternetUA (http://internetua.com/v-socseti--vkontakte--soobsxili-o-rassilke-Android-troyana-posredstvom-SMS). – 2014. – 19.05).***

***

Хакеры, причисляющие себя к группировке «Анонимный интернационал», выложили в сеть архив объемом 1,35 Гб с перепиской командующего вооруженными силами самопровозглашенной «Донецкой Народной Республики» И. Стрелкова (Гиркина). В архиве находится переписка И. Стрелкова за последние пять лет и много интересной информации о личности «Стрелка» и его роли во всплеске украинского сепаратизма, пишет AIN.UA (http://ain.ua/2014/05/19/524631).

Как следует из переписки, И. Стрелков – отставной российский военный, который в начале этого года был командирован в Украину для выполнения особо ответственного задания. Подробности командировки в переписке не упоминаются, но в ряде писем И. Стрелков рассказывает о своей работы в Украине.

До этого И. Стрелков уже участвовал в военных конфликтах – он консультировал добровольцев, желающих принять участие в боевых действиях в Сирии и тесно общался с вербовщиками наемников. Кроме этого, он занимался PR-кампанией по «отбеливанию имиджа» засветившейся в Сирии ЧВК «Славянский корпус».

Также из переписки следует, что «Стрелок» занимал пост руководителя службы безопасности компании «Маршал Капитал» К. Малофеева, которая де-факто является представителем коммерческих интересов российской политической верхушки. По словам П. Дурова, К. Малофеев – тот самый человек, который в августе заказывал атаку в СМИ на «ВКонтакте» (истерия вокруг детской порнографии), параллельно инициировав переговоры о выкупе долей у партнеров П. Дурова в социальной сети.

Что касается текущих украинских событий, то И. Стрелков впервые приехал в Киев в январе 2014 г. «У меня совершенно неожиданный форс-мажор: завтра срочно вылетаю в командировку в Киев. На почте буду до сегодняшней полуночи», – написал И. Стрелков своему другу по исторической реконструкции Рудольфу. «Примите извинения – совершенно неожиданная для меня поездка! Я даже котелки и все прочее на рабочем месте оставляю», – поясняет «Стрелок» невозможность встретиться в заранее условленное время.

«Я считаю, что “Майдан” разгонять не надо. Наоборот. Почему так считаю – объясню при встрече. Так считаю, кстати, не только я», – написал И. Стрелков после возвращения из Киева. После этого переписка «Стрелка» стала смещаться в сторону военных противостояний в Украине.

Часть писем этого периода посвящена подготовке обращений к народу Крыма и Востока Украины, но большую часть переписки составляют анонимные угрозы, пожелания удачи и новостные рассылки. Похоже на то, что часть писем была удалена хакерами и, возможно, будет опубликована позже. Впрочем, не исключено, что переписка может быть частично подделана, ведь проверить ее подлинность достаточно сложно. Как и доподлинно узнать – кем же является «Стрелок» на самом деле.

В настоящее время «Стрелок» много и часто пишет на военно-исторических форумах – публикует свои стихи, дискутирует с украинскими реконструкторами и мечтает добраться до склада старого оружия в шахте Славянска. Как пишет газета Вести, 18 марта его друзья на форуме поздравляли друг друга «с русским Крымом». «Вообще-то, могли бы и меня лично поздравить. Я много и упорно работал над вопросом», – пишет им И. Стрелков. И зовет друзей посетить курорт. «Мне тут скифские пещеры обещали показать в Симферополе. Добраться вполне можно на пароме от порта Кавказ… В Керчи встречу, если еще тут буду», – пишет он 30 марта. «Вероятность моего личного появления в Москве к июню невелика», – резюмирует россиянин ***(Хакеры взломали и выложили в сеть электронную переписку Игоря «Стрелка» Гиркина за пять лет // AIN.UA (http://ain.ua/2014/05/19/524631). – 2014. – 19.05).***

***

Количество зараженных компьютеров в результате автоматической установки вредоносного ПО вместе с другими программами и файлами,

скачанными из Интернета, возросло в три раза за последний квартал 2013 г. и признано экспертами ключевой угрозой в 110 странах мира.

При этом Украина возглавила антирейтинг стран, в которых насчитывается самое большое количество сайтов, содержащих вредоносные программы. Об этом свидетельствуют данные 16-го выпуска отчета Microsoft Security Intelligence Report (SIRv16), в котором проанализированы уязвимости и угрозы по информации с более миллиарда систем и популярных сервисов по всему миру.

Исследование также зафиксировало рост количества заражений программами-вымогателями, например, распространение вируса Reveton выросло на 45 % за полгода. В IV квартале 2013 г. компьютеры почти 14 % украинских пользователей были атакованы такими программами, чаще всего типами Obfuscator (8,03 %), Brantall (4,14 %) и Deminnix (1,77 %).

«После установки программы-вымогатели могут блокировать работу системы или браузера, зашифровывать рабочие файлы на компьютере, делая их недоступными пользователю. При этом злоумышленник требует отправить платное SMS или пополнить какой-либо счет в замен на пароль для расшифровки файлов. Некоторые пользователи в страхе потерять личную информацию и файлы перечисляют средства и, конечно же, остаются обмануты», – поясняет А. Урденко, директор департамента исследований компьютерной техники, программных продуктов и телекоммуникационных систем ООО «Нотингем».

Исследование выявило, что каждый 16-й сайт в Украине содержит вредоносное ПО, которым потенциально может быть заражен компьютер пользователя. Так, на 1000 хостов приходится 59,2 зараженных сайтов. Это самый высокий показатель в мире, для сравнения, во всей сети Интернет в среднем заражен примерно каждый 54-й ресурс ***(Украину назвали лидером по количеству вредоносных сайтов // InternetUA (http://internetua.com/ukrainu-nazvali-liderom-po-kolicsestvu-vredonosnih-saitov). – 2014. – 20.05).***

***

Electronic Frontier Foundation (EFF) составил рейтинг, оценивающий работу 26 интернет-компаний в рамках сотрудничества с правительствами различных стран. Согласно показателям EFF, Snapchat имеет наихудший рейтинг. Компания получила всего лишь одну звезду среди всех поставщиков интернет-услуг. Единственную вещь, которую Snapchat делает хорошо, так это публикация руководств правоохранительных органов.

Компании, работу которых анализировал EFF, включают интернет-провайдеров, поставщиков услуг электронной почты, мобильной связи, провайдеров облачных центров, блоговые платформы и социальные сети.

Компании оценивались за шестью критериями: запросы ордеров на предоставление данных, уведомление пользователей о запросах данных со стороны государства, публикация отчетов о прозрачности, публикация

руководств правоохранительных органов, случаи борьбы за неприкосновенность частной жизни пользователей в судах, а также отстаивание прав пользователей на неприкосновенность частной жизни в Конгрессе США.

EFF отметил существенное улучшение стандартов в отрасли информирования пользователей о запросе данных государством, публикации отчетов о прозрачности, а также отстаивание прав пользователей в Конгрессе. Впервые за четыре года в отчете EFF каждая компания получила хотя бы одну звезду в одном из критериев.

Это огромный шаг вперед, если сравнивать результаты доклада EFF за 2011 г., в котором Comcast, MySpace, Skype и Verizon не получили ни одной звезды. Девять компаний получили свои оценки по каждому из критериев. Такими компаниями стали Apple, CREDO Mobile, Dropbox, Facebook, Google, Microsoft, Sonic, Twitter и Yahoo.

Некоторые компании также публикуют отчеты о количестве поступившим к ним писем о раскрытии персональной конфиденциальной информации, а также о количестве пострадавших учетных записей. Кроме Apple, в этот список вошли AT&T, Comcast, Credo, Dropbox, Facebook, Google, Internet Archive, LinkedIn, Lookout, Microsoft, Pinterest, Tumblr, Verizon, Wickr, WordPress и Yahoo.

Ряд компаний получили похвалу от EFF. Так, Facebook поднялся с 1-й звезды в 2011 г. до 6-й в текущем году, Yahoo получила отметку во всех шести категориях, Microsoft также отметили по всем критериям. Отчеты о прозрачности не публикуют Adobe, Amazon, Foursquare, Myspace, Wikimedia или Snapchat ***(EFF: Snapchat, AT&T, Amazon являются наихудшими защитниками конфиденциальности // InternetUA (http://internetua.com/EFF--Snapchat--AT-T--Amazon-yavlyauatsya-naihudshimi-zasxitnikami-konfidencialnosti). – 2014. – 21.05).***

***

Весьма известный ИБ-эксперт, занимающийся поиском уязвимостей, И. Хегази обнаружил критическую уязвимость, которая затрагивает шесть сайтов в домене Yahoo, четверо сайтов в домене MSN и несколько сайтов в доменах серверов Orange.

По его словам, брешь позволяет злоумышленнику получить неавторизованный доступ типа Admin. Это, в свою очередь, предоставляет возможность осуществления инъекции удаленного кода.

И. Хегази говорит, что посредством эксплуатации уязвимости ему удалось получить доступ к панели администратора домена Yahoo.net. При этом для входа в нее эксперту не пришлось вводить учетные данные. Затем он создал файл формата .aspx и попытался перехватить POST-запрос во время создания новых файлов.

Создав файл «zigoo.aspx», он заметил, что такой же файл появился на ряде других доменов:

Yahoo:
http://pe.horoscopo.yahoo.net;
http://mx.horoscopo.yahoo.net;
http://ar.horoscopo.yahoo.net;
http://co.horoscopo.yahoo.net;
http://cl.horoscopo.yahoo.net;
http://espanol.horoscopo.yahoo.net;
Microsoft MSN:
http://astrocentro.latino.msn.com/;
http://astrologia.latino.msn.com/;
http://horoscopo.es.msn.com/;
http://horoscopos.prodigy.msn.com;
Orange:
http://astrocentro.mujer.orange.es.

Обратившись в Microsoft с просьбой объяснить, почему происходит подобное, И. Хегази не получил ответ. Сам он считает, что дело в сервисе сети передачи данных (CDN) астрологического ресурса, который кеширует одинаковый контент для его передачи на поддомены.

Несмотря на то что Yahoo обычно не выплачивает вознаграждения за обнаружения уязвимостей в Yahoo.net, И. Хегази все же заплатили, отметив, что он проделал хорошую работу.

В Microsoft, как и в большинстве случаев, брешь исправили, но вознаграждения ИБ-эксперт не получил. С Orange ему связаться не удалось, однако исправление, выпущенное компанией из Редмонда, затронули и ее домены серверов ***(На сайтах Yahoo, Microsoft и Orange обнаружена критическая уязвимость // InternetUA (http://internetua.com/na-saitah-Yahoo--Microsoft-i-Orange-obnarujena-kriticseskaya-uyazvimost). – 2014. – 21.05).***

***

Специалисты «Лаборатории Касперского» обнаружили очередную уловку злоумышленников, нацеленную на выманивание денежных средств пользователей. В новой схеме расчет как всегда идет на желание адресата получить большую сумму денег, не прилагая при этом никаких усилий. Пользуясь этим, мошенники начали создавать множество онлайн-казино, в которых пользователь ни при каких обстоятельствах не может выиграть реальные деньги. Рекламу своих сайтов злоумышленники осуществляют посредством спама.

Для того чтобы получить доступ ко всем рекламируемым богатствам, пользователю требуется скачать программное обеспечение для игры. В данном случае риск установить вредоносную программу не столь велик, так как главные ловушки предусмотрены далее. Мошенники прибегают к двум сценариям. В рамках одного из них первая игра предлагается пользователю бесплатно. Заранее спланированная победа в ней становится для

пользователя приятным сюрпризом и стимулом продолжать, но для участия во второй игре требуется регистрация на сайте и оплата вступительного взноса. В более прямолинейном сценарии после регистрации и уплаты взноса на счет игрока в казино немедленно зачисляется довольно крупная сумма денег. Однако вывести эти деньги из казино не удавалось еще никому, равно как и получить тот выигрыш, который якобы случайно получен в рамках первого бесплатного кона.

Спам, продвигающий подобные онлайн-казино, встречается на всех распространенных в Интернете языках. При этом хостинг мошеннических сайтов осуществляется именно в тех странах, где игровой бизнес легален, но созданное казино при этом доступно для пользователей во всем мире. Злоумышленникам такой подход выгоден тем, что пострадавшим игрокам в случае возникновения претензий будет очень трудно найти владельцев исчезнувшего интернет-ресурса, зарегистрированного в другой части света.

Подобные нелегальные ресурсы имеют ряд отличительных черт. Во-первых, мошенники используют самые «дешевые» доменные зоны: net, biz, info. Также у таких казино нет лицензии, тогда как на легальных ресурсах о наличии лицензии стараются сообщать на главной странице. Еще одно отличие от настоящих онлайн-казино в том, что мошенники используют для рекламы спам. Наконец, веб-площадка для казино-ловушки обычно создается незадолго до рассылки и имеет короткий срок жизни.

Еще одним видом мошенничества, получившим популярность у «азартных» спамеров, являются письма об играх на скачках. Этот связанный с тотализатором спам особенно распространен в Японии, однако подобные рассылки все чаще можно встретить в США и России. Как правило, чтобы получить точный прогноз, заинтересованный в предсказании пользователь должен внести предварительную плату, при этом ресурс «гарантирует» возместить убытки в случае проигрыша. На деле этого, разумеется, не происходит. По схожей схеме действуют мошенники, предлагающие сделать ставку на договорной матч, предварительно заплатив за информацию о «гарантированном» победителе.

«Если вы играете онлайн, постарайтесь следовать нескольким простым правилам. Во-первых, никогда не регистрируйтесь на ресурсах, о которых вы узнали из спам-рассылок. Во-вторых, играйте только на сайтах с проверенной репутацией – обязательно ознакомитесь с отзывами в Интернете и историей казино. В-третьих, игнорируйте письма, в которых говорится о крупных суммах денег, которые, например, уже достались вам в результате случайного лотерейного отбора. Описанные схемы в очередной раз подтверждает старое наблюдение: хорошие вещи в спаме не рекламируют», – комментирует Т. Куликова, старший спам-аналитик «Лаборатории Касперского» ***(В Сети продвигается новая схема мошенничества, связанная с онлайн-казино // InternetUA (http://internetua.com/v-seti-prodvigaetsya-novaya-shema-moshennicsestva--svyazannaya-s-onlain-kazino). – 2014. – 21.05).***

***

Социальная сеть Facebook в ближайшем будущем начнет помогать пользователям, которые заходят в свою учетную запись с зараженных компьютеров бесплатными антивирусами, сообщает blog.imena.ua.

Facebook предложит им установить один из двух бесплатных антивирусных программ. Администрация соцсети обещает, что в будущем список доступных антивирусов будет расширен.

Чтобы установить, заражен ли компьютер пользователя, программа проанализирует активность учетной записи, и если сочтет действия подозрительными – порекомендует скачать программу F-Secure Online Scanner или HouseCall.

Уважая право пользователей на свободу выбора, социальная сеть предоставляет возможность игнорировать запрос на установку программ.

Бесплатный антивирус будет автоматически удаляться с пользовательского устройства после проведения проверки и уничтожения обнаруженных угроз.

Такое решение администрация социальной сети приняла, поскольку в последнее время фиксируется огромное количество вредоносных программ, предназначенных для совершения мошеннических действий в Facebook ***(Facebook предложит бесплатные антивирусы // Подробности.UA (http://podrobnosti.ua/internet/2014/05/22/977173.html). – 2014. – 22.05).***

***

Взлом базы данных одной из крупнейших онлайн-площадок по купле-продаже товаров eBay, в результате которого в руки злоумышленников попали зашифрованные пароли и другие персональные данные, затронул всех пользователей eBay, которых у сервиса насчитывается 145 млн. Это следует из документа, опубликованного на сайте eBay.

Пользователи eBay накануне начали получать от администрации сервиса письма с просьбой сменить пароль к аккаунту. Сам eBay опубликовал на сайте список часто задаваемых вопросов и ответов о взломе. На вопрос «Сколько аккаунтов затронул взлом?» eBay разместил следующий ответ: «Мы попросили всех пользователей eBay сменить пароль. Всем пользователям придет оповещение. По данным на конец I квартала, у нас было 145 млн активных покупателей».

В базе данных, взлом которой произошел в конце февраля – начале марта, находились имена пользователей eBay, пароли в зашифрованном виде, адреса электронной почты, физические адреса, номера телефонов и даты рождения.

Однако финансовая информация, в том числе данные банковских карт, во взломанной базе не хранились. Также там не было конфиденциальных персональных данных – номеров социального страхования, идентификаторов налогоплательщика или номеров паспортов, говорится в документе eBay.

Администрация eBay утверждает, что перекрыла пути неавторизованного доступа к системе, которые использовали злоумышленники, и предприняла дополнительные меры для усиления безопасности сайта. Мошеннических действий с использованием скомпрометированных данных не зафиксировано.

Данные пользователей платежной системы PayPal, которая принадлежит eBay, в руки хакеров не попали. Компания также не зафиксировала попыток неавторизованного доступа к другим сайтам, работающим на платформе eBay Marketplaces, включая StubHub, eBay Classifieds, Tradera, GMarket, Auction, GumTree и GittiGidiyor ***(Атака хакеров затронула все 145 миллионов пользователей eBay // InternetUA (http://internetua.com/ataka-hakerov-zatronula-vse-145-millionov-polzovatelei-eBay). – 2014. – 22.05).***

***

Аналитики из компании «Доктор Веб», исследуя файловый вирус Win32.Sector, с помощью которого хакеры создали обширный ботнет, пришли к выводу, что его распространенность по всему миру продолжает расти. Они также оценили возможные масштабы заражения.

Вирус Win32.Sector является сложным полиморфным вирусом, о котором стало известно еще в 2008 г. Опасность его состоит в том, что он загружается из P2P-сети и запускается на зараженном компьютере в форме различных исполняемых файлов. Встроившись в запущенные на инфицированном компьютере процессы, вредоносное ПО останавливает работу некоторых антивирусных программ и блокирует доступ к сайтам их разработчиков.

На 20 мая 2014 г. в ботнете Win32.Sector находилось 1,2 млн уникальных ботов, 109 783 из которых могут исполнять функцию маршрутизаторов для вредоносных узлов, поскольку имеют внешний IP-адрес. Каждый день около 60 тыс. компьютеров инфицируются вирусом.

Наибольшее число заражений машин Win32.Sector происходит на Тайване (212 401). За ней следуют Египет (108 770) и Индия (106 249). В общем, в России зафиксировано около 15,6 тыс. инфицированных компьютеров ***(Win32.Sector заражает все больше компьютеров по всему миру // InternetUA (http://internetua.com/Win32-Sector-zarajaet-vse-bolshe-kompuaterov-po-vsemu-miru). – 2014. – 22.05).***

***

Как сообщили эксперты из ИБ-компании Symantec, влиятельные российские киберпреступные группировки для атак на финансовые организации используют вредоносное ПО для Android премиум-класса, такое как iBanking. По словам экспертов, он является одним из наиболее дорогостоящих троянов на черном рынке, а его создатель использует хорошо

отлаженную бизнес-модель Software-as-a-Service (программное обеспечение как услуга).

Владелец iBanking продает подписку на ПО, в которую также сходит стоимость обновлений и технической поддержки, за 5 тыс. дол. Для тех, кто не может оформить подписку, он предлагает заключить сделку – троян в обмен на часть прибыли от его использования.

iBanking обычно маскируется под легитимное приложение для online-банкинга, соцсетей или защиты, и в основном используется для обхода безопасности в системах банков, перехватывая одноразовые пароли, которые отправляются в SMS-сообщениях. Кроме того, троян применяется для создания мобильных ботнетов и слежения за пользователями. iBanking выполняет ряд полезных для злоумышленников функций, таких как переключение контроля между HTTP и SMS в зависимости от интернет-соединения.

Эксперты отмечают, что высокая цена на троян означает, что изначально он был разработан для влиятельных киберпреступных группировок, располагающих большими суммами. Тем не менее, недавно произошедшая утечка исходного кода iBanking вызвала всплеск его активности в последнее время. В связи с этим в ближайшее время стоит ожидать рост количества атак с использованием этого трояна.

Для того чтобы заставить жертву установить iBanking на свое Android-устройство, злоумышленники используют социальную инженерию. Обычно ПК таких пользователей уже инфицированы вредоносным ПО, которое генерирует всплывающие окна, предлагающие установить на смартфон приложение, якобы обеспечивающее дополнительную защиту ***(В ближайшем будущем стоит ожидать рост атак с использованием iBanking // InternetUA (http://internetua.com/v-blijaishem-budusxem-stoit-ojidat-rost-atak-s-ispolzovaniem-iBanking). – 2014. – 22.05).***

***

Публікації нових користувачів Facebook за замовчуванням будуть показуватися тільки людям зі списку друзів, пише Корреспондент.net (http://ua.korrespondent.net/tech/technews/3367556-Facebook-vnis-znachni-zminy-v-polityku-konfidentsiinosti).

Компанія Facebook вирішила надати своїм користувачам більше прав для контролю за їхньою особистою інформацією. Цей крок став одним з найбільших в її політиці конфіденційності за останні роки, пише The Financial Times.

Facebook повідомив, що публікації нових користувачів соціальної мережі тепер за замовчуванням будуть показуватися тільки людям зі списку друзів, а не всім, як було раніше.

Існуючим користувачам Facebook запропонує провести «перевірку конфіденційності», що має дозволити спростити роботу щодо зміни часто складних налаштувань.

У минулому Facebook часто зазнавав критики за введення нових функцій, які дозволяли компанії збирати більше даних користувача. Особливо різка критика в бік соцмережі була чотири роки тому після нововведення, після якого записи після публікації були видні всім користувачам ***(Facebook вніс значні зміни в політику конфіденційності // Корреспондент.net (http://ua.korrespondent.net/tech/technews/3367556-Facebook-vnis-znachni-zminy-v-polityku-konfidentsiinosti). – 2014. – 23.05).***

***

Інтернет-видання Comments.ua заявляє, що 22 травня близько 14:20 зафіксувало хакерську атаку, унаслідок чого в новинах та статтях інтернет-видання з'явилося вірусне повідомлення, що перенаправляє читачів на інший ресурс (який саме – видання не уточнює). Про це йдеться в листі видання за підписом шеф-редактора Comments.ua і головного редактора тижневика «Коментарі» Т. Мокротоварової.

«Редакція Comments.ua докладає максимум зусиль для того, щоб виявити джерело хакерської атаки та ліквідувати її наслідки», – ідеться в повідомленні.

Видання нагадує, що несанкціоноване втручання в роботу електронно-обчислювальної машини (сервер, на якому розміщений веб-портал Comments.ua), що призвело до блокування інформації, спотворення процесу обробки інформації є злочином, який передбачений ст. 361 Кримінального кодексу України.

Нагадаємо, що наприкінці минулого року в холдингу «Еволюшен Медіа», якому належать Comments.ua і «Коментарі», змінився власник. За інформацією джерел «Телекритики», «Еволюшен Медіа» придбали люди, наближені до влади. Інші джерела стверджують, що «Еволюшен Медіа» придбали структури С. Курченка. Однак у прес-службі холдингу С. Курченка «ВЕТЕК-Медіа» «Телекритиці» сказали, що це неправда ***(Comments.ua заявляє про хакерську атаку // «Телекритика» (http://www.telekritika.ua/rinok/2014-05-22/93941). – 2014. – 22.05).***

***

Взлом серверов ЦИК в конце прошлой недели в буквальном смысле поставил на уши украинские спецслужбы. По утверждениям хакеров, в системе голосования были оставлены «закладки», и перед СБУ и Госспецсвязи была поставлена задача не допустить повторного взлома системы и предотвратить подтасовку голосов. Спустя два дня после выборов СБУ отчиталась о хакерских атаках последних дней и рассказала, как их удалось отбить. Ниже – приблизительная хроника событий, пишет AIN.UA (http://ain.ua/2014/05/28/526133).

Во время выборов сервер ЦИК и системы «Выборы» неоднократно подвергались атакам с использованием бот-сетей с территории Российской

Федерации. IT-специалистам удалось отбить атаку благодаря десятикратному резервированию каналов связи для информационных систем ЦИК.

В Киеве в рамках уголовного производства была задержана организованная хакерская группа, которая готовилась вывести из строя информресурсы ЦИК и хотела поставить под сомнение результаты голосования. У злоумышленников изъяли и отправили на экспертизу специализированное ПО российского производства, программный комплекс для мониторинга и взлома интернет-ресурсов, в т. ч. Wi-Fi сетей.

В Виннице обнаружили и заблокировали работа двух пораженных вирусами серверов, которые арендовались гражданином России. Злоумышленники взломали сервера хостинг-провайдера «Бестхостинг» и сгенерировали мощную DDOS-атаку на информационные ресурсы ЦИК (свыше 200 000 пакетов в секунду). По данному факту зарегистрировано уголовное производство.

На стационарные телефоны избирательных округов Тернопольской, Житомирской, Полтавской и Волынской областей осуществлялся непрерывный автодозвон. С помощью специальных средств СБУ удалось не допустить перегрузки линий связи.

В системе обработки данных ЦИК была обнаружена и обезврежена вирусная закладка. Таким образом была сорвана срежиссированная российской стороной информационная акция по дискредитации результатов выборов (предполагалось объявить лидером голосования Д. Яроша с рейтингом 37 %). Не будучи осведомленными об обезвреживании закладки украинскими спецслужбами, российский телеканал ОРТ обнародовал провокацию и прокомментировал в своем сюжете именно тот результат, который должен был сгенерировать вирус на сайте ЦИК.

Кроме всего вышеперечисленного, хакеры пытались переправить электронные протоколы результатов голосования на одном из участков Днепропетровской области на сторонний IP-адрес. Злоумышленники также пытались подделать результаты голосования в указанном регионе и таким образом скомпрометировать общие результаты выборов Президента Украины.

Напомним, что накануне выборов в результате хакерской атаки в Интернет попали все пароли доступа и структура компьютерной сети ЦИК. Как сообщил глава Госспецсвязи В. Зверев, установленный на компьютере администратора организации антивирус «Касперского» не сработал и злоумышленники смогли добраться до остальных серверов организации ***(В СБУ рассказали, кто и как пытался взломать сервера ЦИК во время виборов // AIN.UA (http://ain.ua/2014/05/28/526133). – 2014. – 28.05).***

***

В Интернете активизировались виды мошенничества, в ходе которых эксплуатируется тема чемпионата мира по футболу 2014 г. в Бразилии.

Киберпреступники всегда использовали значимые спортивные события в своих интересах. Однако на этот раз они не просто эксплуатируют известные приемы обмана пользователей, но делают это максимально профессионально, создавая фишинговые домены с SSL-сертификатами, используя цифровые подписи и взломанные базы данных клиентов онлайн-сервисов по продаже билетов, сообщает пресс-служба «Лаборатории Касперского», специализирующейся на разработке антивирусных программ.

По данным «Лаборатории Касперского», бразильские фишеры совершенно официально регистрируют домены с названиями широко известных брендов, в частности компании-представителя Visa в Бразилии или Mastercard. Более того, они покупают SSL-сертификаты у сертифицирующих органов, таких как Comodo, EssentialSSL, Starfield, Register.com и других. Сами фишинговые порталы при этом выглядят очень стильно и правдоподобно – очевидно, что в их разработке принимали участие профессионалы.

Злоумышленники, избирающие более адресный подход, рассылают интернет-пользователям письма с сообщениями о том, что они выиграли билеты на матч в рамках чемпионата мира по футболу. Получить билеты, по уверениям мошенников, можно, пройдя по ссылке в письме или открыв приложенный документ. Разумеется, никаких билетов там нет и быть не может – вместо этого доверчивый пользователь загрузит на свой компьютер банковского троянца. Схема подобного мошенничества довольно традиционна, но в данном случае бразильские киберпреступники усыпляют бдительность пользователей наличием цифровых подписей у прилагаемых документов, а также использованием корректных персональных данных человека, полученных, по всей видимости, из взломанных баз данных онлайн-сервисов по продаже ***(Мошенники начали распространять вирусы с помощью Чемпионата мира по футболу // InternetUA (http://internetua.com/moshenniki-nacsali-rasprostranyat-virusi-s-pomosxua-cempionata-mira-po-futbolu). – 2014. – 24.05).***

***

В сети зафиксирована новая волна фишинговой кампании, направленной на пользователей Google. Согласно данным Symantec, жертвам приходят поддельные электронные письма с темой «Документы». Сами письма содержат ссылки на фишинговую страницу.

«Это мошенничество более эффективное, нежели рассылка миллионов фишинговых писем, которую мы наблюдаем почти каждый день. Причина тому – фишинговая страница Google Drive имеет SSL-сертификат подлинного сервиса Google Drive», – сообщают исследователи компании.

В нижней части выпадающего меню можно увидеть искаженные наименования языков, однако этого далеко не всегда достаточно для того, чтобы распознать уловку. По словам экспертов, мало кто из пользователей

вообще обращает внимание на это меню, а если и обращают, то могут воспринять ошибку в написании языков обычной оплошностью.

В Symantec говорят, что авторами этой кампании, скорее всего, являются те же злоумышленники, которые виновны в оригинальном инциденте безопасности. Свидетельством тому является использование названия performact.php для скрипта, которое также было задействовано в рамках кампании в марте текущего года.

Тем не менее, эксперты считают, что в этот раз масштабы последствий могут быть гораздо больше и серьезнее, поскольку Google снизила стоимость сервисов в Google Drive.

Отметим, что авторизовавшиеся пользователи перенаправляются на скомпрометированный бразильский сайт, содержащий троянца. То есть риск инфицирования компьютера вирусом весьма высокий ***(Фишинговая кампания с Google Drive возобновлена // InternetUA (http://internetua.com/fishingovaya-kampaniya-s-Google-Drive-vozobnovlena). – 2014. – 24.05).***

***

Пять ошибок в Facebook, которые могут вам дорого обойтись

Мы не можем жить без Facebook. Здесь все наши друзья, у многих здесь еще и работа. С этой социальной сетью синхронизированы контакты в наших смартфонах, события в наших календарях. Через аккаунт в Facebook мы попадаем во множество других сервисов – и потерять все это смерти подобно. Нельзя так просто взять и уйти из Facebook, но можно (и нужно) поменять правила собственного поведения. Иначе вы рискуете лишиться денег, карьеры, уважения или даже ваших близьких, пишет AIN.UA (http://ain.ua/2014/05/26/525498).

Специалисты «Лаборатории Касперского» составили список из пяти типичных ошибок, которые почти каждый делает в Facebook, а также советы, как избежать неприятных последствий от них в будущем. И кстати, «не читать Facebook за рулем» среди них нет – это само собой разумеется.

Публикация полной биографии

Facebook активно подталкивает нас написать все про карьеру, место и дату рождения и т. д. Но множество сервисов, включая банки, используют эти данные (например, дату рождения, девичью фамилию матери, кличку питомца), чтобы открыть доступ к вашему счету или учетной записи. Преступники обожают Facebook, поскольку там можно собрать всю нужную информацию про человека, а затем взломать его куда более важные аккаунты.

Совет: Не публикуйте свою дату или хотя бы год рождения, избегайте упоминания имен родственников и домашних животных, а также других данных, регулярно применяемых в социально-инженерных атаках, а также атаках на банковские и финансовые счета.

Публикация постов «для всех»

Публичные записи могут прочесть не только ваши близкие, но и начальник, бывший муж/жена, сотрудник кадровой службы, многочисленные рекламные и маркетинговые фирмы и даже мошенники. Люди считают, что написать в Facebook – все-равно, что рассказать историю друзьям за столиком бара.

На самом деле это все-равно что громко прокричать свою мысль на городской площади. Кто-то может случайно или умышленно исказить ваши слова, вырвать их из контекста и рассказать другим, испортив вам репутацию. Случаи потери работы за неосторожную запись в соцсети также никто не отменял.

Совет: Настройте публикацию таким образом, чтобы все записи отправлялись в режиме «Для друзей» или «Для друзей друзей». Особенно внимательно публикуйте фото. Если же вы действительно захотите сказать что-то всему миллиарду пользователей Facebook, этот режим легко сменить на публичный.

Небезопасный пароль

Сегодня почти все пользователи входят на другие сайты и онлайн-сервисы при помощи Facebook. Если пароль к аккаунту в этой соцсети взломан, то все эти онлайн-сервисы тоже можно считать взломанными.

Совет: Используйте надежный пароль, а лучше двухфакторную аутентификацию. Не применяйте пароль к Facebook на других сайтах, он должен быть уникален.

Публикация местоположения

Посторонние могут следить за вами, узнать адрес вашего офиса или даже домашний. Особенно опасно для детей и подростков. Но даже если вы давно выросли и «чекинитесь» в невинном месте вроде ресторана или курортного отеля, это как минимум демонстрирует, что вы не дома, – очень ценная информация для грабителей.

Совет: Отключите геотеги в фотографиях, которые вы публикуете. Не публикуйте чекины Facebook или создайте ограниченный список людей, которые их видят.

Дружба с незнакомцами

Часто незнакомые люди добавляются в друзья. И если у вас много общих друзей, вы можете принять приглашение, чтобы не показаться невежливым. Чужак сразу получает доступ ко всей вашей информации «для друзей», включая вышеописанные чекины, жизненные даты и т. п. Теперь он сможет посылать вам и вашим друзьям сообщения (возможно, спам или вредоносные ссылки), а также добавлять все новых друзей, пользуясь тем, что дружба с вами повысила авторитет этого человека.

Совет: Дружите в Facebook только с теми, кого вы знаете лично ***(5 ошибок в Facebook, которые могут вам дорого обійтись // AIN.UA (http://ain.ua/2014/05/26/525498). – 2014. – 26.05).***

***

Специалисты по информационной безопасности обнаружили глобальную сеть из 1500 POS-терминалов, инфицированных специализированным вредоносным ПО. Созданная хакерами сеть работает в 36 странах и также включает в себя машины, используемые для прочих операций в розничной торговле.

Согласно данным компании IntelCrawler, созданная ботсеть получила название Nemanja, ее центр управления находится в Сербии. В отчете компании говорится, что размер ботсети и ее глобальная распределенность говорит о том, что атаковавшие хакеры очень хорошо знакомы с системами автоматизации торговли в разных странах и хорошо представляют себе бизнес-процессы в торговле.

В блоге IntelCrawler отмечается, что прежде большинство ИТ-инцидентов в розничной торговле были связаны с малым бизнесом или индивидуальными сетями, тогда как сейчас речь идет о мультинациональной кампании. «Мы ожидаем роста числа инцидентов с участием сектора торговли, не исключаем новых случаев крупных утечек данных, а также появления нескольких семейств вредоносных кодов, ориентированных именно на торговый сектор», – говорят в компании.

Согласно данным этой компании, ботсеть Nemanja включает в себя 1478 зараженных систем, большая часть которых работает в США, Великобритании, Канаде, Австрии, Китае, России, Бразилии и Мексике. Анализ позволил выявить, что все целевые PoS-терминалы работали на основе разных систем, разных систем управления запасами и другого софта. Компания идентифицировала как минимум 25 разных программ автоматизации.

«Выявленные данные не говорят о том, что одни системы более уязвимы, чем другие. Это, скорее, говорит о том, что вредоносное ПО эволюционирует таким образом, что может работать на разных системах автоматизации сразу», – отмечают в IntelCrawler ***(Выявлена сеть из 1500 зараженных PoS-терминалов // InternetUA (http://internetua.com/viyavlena-set-iz-1500-zarajennih-PoS-terminalov). – 2014. – 26.05).***

***

Новый компьютерный троянец, уже успевший заразить более 450 финансовых институтов по всему миру, заимствует функционал и возможности у нашумевших троянцев Zeus и Carberp. Новая угроза получила неофициальное название Zberp, говорят в компании Trusteer. По словам специалистов, новинка поддерживает широкий диапазон функциональных возможностей.

Вредонос может собирать IP-адреса и имена жертв, делать снимки экрана и передавать их на удаленный сервер, похищать FTP- и POP3-аккаунты, SSL-сертификаты, а также информацию из веб-форм. Вдобавок к этому, из продвинутого функционала вредонос может перехватывать браузерные сессии и внедрять поддельный контент на сайты.

В Trusteer говорят, что Zberp – это разновидность троянца ZeusVM (последняя из известных модификаций банковского вредоноса Zeus). ZeusVM был обнаружен в феврале этого года, тогда как все семейство Zeus базируется на базе исходников реализованных еще в 2011 г. Изюминка ZeusVM заключалась в том, что он использовал метод стеганографии (встраивания в графические файлы) и распространения таким образом. Zberp также использует эту концепцию, направленную на обман антивредоносных программ.

М. Корман, специалист Trusteer, говорит, что на сегодня Zberp обходит значительную часть антивирусов. Также он рассказал, что вредонос использует оригинальную технику сокрытия от антивирусов при обнаружении: он удаляет некоторые стартовые записи из реестра Windows при работе и возвращает их при отключении или перезагрузке комп'ютера ***(Новый банковский троянец поразил около 450 учреждений // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/05/27/Zberp.html). – 2014. – 27.05).***

***

Австралийское издание the Age сообщила о том, что ряд пользователей iOS и Mac в Австралии стали жертвами ранее неизвестного вредоносного программного обеспечения, удаленно блокирующего работу iPhone, iPad и Mac через облачный сервис iCloud. Скомпрометированные устройства выводят предупреждающее сообщение и требуют денег за разблокировку.

Согласно сообщениям многочисленных пользователей на форумах техподдержки Apple, организаторы атаки требуют 100 дол./евро за разблокировку устройств, причем большинство пользователей отмечает, что ничего не загружали на устройство и не посещали сомнительных сайтов. Другие говорят, что сообщения начали появляться во время работы iMessage, в которой ранее были выявлены баги (и Apple пообещала их исправить в ближайшее время).

The Age приводит данные ряда независимых экспертов, согласно которым блокировка могла быть возможной в связи с ранее выявленной утечкой данных из iCloud.

Apple официально еще не прокомментировала инцидент ***(Пользователи iPhone и Mac стали жертвой блокировщика // InternetUA (http://internetua.com/polzovateli-iPhone-i-Mac-stali-jertvoi-blokirovsxika). – 2014. – 27.05).***

***

Приложение от Microsoft для пользователей Android-устройств на самом деле не шифрует конфиденциальную информацию пользователей.

Представители компании Include Security обнаружили , что приложение Outlook.com для Android-устройств предоставляет очень низкий уровень безопасности для конфиденциальных данных. В частности, эксперты

утверждают, что приложение по умолчанию размещает все вложения из электронной почты на SD-карту, доступ к которой имеет любая другая программа с разрешением READ_EXTERNAL_STORAGE. В версии Android 4.4 у приложений есть отдельные папки на SD-карте, все предыдущие версии такой функцией не располагают.

Еще одна проблема в Outlook.com касается функции «пин-код». Приложение предоставляет пользователю возможность установить пин-код, т. е. пароль, который должен был бы шифровать электронную почту. На самом деле, это не так – пин-код только контролирует доступ к приложению. Эта функция также не включена по умолчанию.

Когда пользователь открывает меню Настройки в приложении Outlook.com, первое уведомление, которое отображается на экране устройства, гласит, что настройка позволит ему «защитить это приложение». При выборе этой функции пользователю открывается еще одно окно, в котором нужно установить пин-код. В уведомлении написано, что эта функция «защитит электронную почту», хотя, на самом деле, это не так. Более того, если на устройстве пользователя активирован режим USB-откладки, то кто-угодно может получить доступ к SD-карте через USB-интерфейс.

В Microsoft сложившуюся ситуацию прокомментировали следующим образом: «Microsoft считает своим долгом обеспечивать безопасности личным данным пользователей. Мы используем разные технологии и методы безопасности для того, чтобы защитить вашу личную информацию от несанкционированного доступа, использования или раскрытия. Все действия приложения Outlook.com на Android осуществляются в песочнице, где операционная система защищает данные пользователей. Кроме того, для шифрования электронной почты пользователи могут использовать настройки устройства и зашифровать данные на SD-карты».

Ранее стало также известно о том, что приложение электронной почты для iOS 7 также не шифрует почтовые вложения. В Apple знают о существующей проблеме, однако пока не устранили ее ***(Outlook.com для Android раскрывает личные данные пользователей // InternetUA (http://internetua.com/Outlook-com-dlya-Android-raskrivaet-licsnie-dannie-polzovatelei). – 2014. – 27.05).***

***

По данным экспертов из «Лаборатории Касперского», за последнее время в Рунете резко увеличилась мощность DDoS-атак. Так, если год назад максимальная мощность атаки едва достигала 60 Гб/с, то уже нынешней весной она составляла 70–80 Гб/с, а в пиковые моменты даже превышала 100 Гб/с.

Эксперты объясняют это тем, что злоумышленники стали применять метод отражения/усиления атаки – NTP Amplification, позволяющий достичь большой мощности атаки при минимальных усилиях. Преимуществом этого

вида атак является существенный коэффициент усиления (до 556 раз) и возможность для злоумышленника скрыть свой настоящий адрес.

По словам исследователей, нынешней весной киберпреступники осуществили DDoS-атаки типа NTP Amplification на ряд крупных российских банков (среди них Альфа-Банк и ВТБ24), компанию «Аэрофлот», телеканал Russia Today и пр., и в пиковые моменты их мощность доходила до 120 Гб/с.

Как сообщил менеджер по развитию бизнеса Kaspersky DDoS Prevention «Лаборатории Касперского» Е. Виговский, хакеры обнаружили в протоколе NTP команду, которая в ответ на запрос отправляет последние 600 IP-адресов, обращавшихся к серверу. Именно благодаря этому стало возможным усиливать DDoS-атаки. Эксперт добавил, что для борьбы с NTP Amplification IT-специалистам необходимо корректно настраивать NTP серверы ***(Мощность DDoS-атак в Рунете резко звеличилась // InternetUA (http://internetua.com/mosxnost-DDoS-atak-v-runete-rezko-uvelicsilas). – 2014. – 28.05).***

***

Во вторник, 27 мая, популярный музыкальный сервис Spotify стал жертвой утечки данных. Представители компании сообщили , что им стало известно о «неавторизованном доступе к системам и внутренним данным компании», и отметили, что незамедлительно начали принимать соответствующие меры.

В ходе расследования инцидента безопасности эксперты из Spotify обнаружили, что злоумышленники получили доступ только к одной учетной записи, которая не содержит паролей или каких-либо финансовых данных. Они сразу же связались с ее владельцем и убедились, что взлом никак не может ему навредить.

«Мы очень серьезно подходим к подобным вопросам, и в целях общей меры предосторожности попросим определенных пользователей Spotify в ближайшие дни сменить имя пользователя и пароль», – сообщили представители компании.

Кроме того, владельцам Android-устройств рекомендуется установить обновления. «Если Spotify предложит вам установить обновления, пожалуйста, следуйте инструкциям», – говорится в уведомлении. При этом необходимо помнить, что offline-плейлисты после установки обновлений не сохранятся, и их нужно будет загрузить заново ***(Сервис Spotify стал жертвой утечки даннях // InternetUA (http://internetua.com/servis-Spotify-stal-jertvoi-utecski-dannih). – 2014. – 28.05).***

***

Хакерам удалось проникнуть во внутреннюю систему электронной почты Министерства иностранных дел Бразилии, но им не удалось получить доступ к конфеденциальной информации правительственных документов. Как сообщает Reuters со ссылкой на представителя министерства.

Согласно данным издания, атаку могли осуществить активисты, которые протестуют против проведения чемпионата мира по футболу в Бразилии. Тем не менее, ответственность за реализацию инцидента безопасности на себя никто не взял.

Правоохранительные органы и службы государственной безопасности расследуют масштаб данной атаки. Министерство прекратило всю коммуникацию по электронной почте на целый день. Представитель МИД Бразилии сообщил, что конфиденциальная информация, которая передается при помощи электронной почты, была зашифрована. Сотрудникам ведомства и бразильских посольств за рубежом все же порекомендовали сменить пароли к учетным записям электронной почты ***(Хакеры взломали электронную почту правительства Бразилии // InternetUA (http://internetua.com/hakeri-vzlomali-elektronnuua-pocstu-pravitelstva-brazilii). – 2014. – 28.05).***

***

Обнаружен новый вариант вредоносной программы MiniDuke, который позволяет управлять атакой через сервис микроблогов Twitter. MiniDuke представляет собой бэкдор – разновидность вредоносного ПО, открывающего атакующим полный доступ к компьютеру жертвы. Его новая версия использует для этого эксплойт к уязвимости CVE-2014-1761, которой были подвержены все версии Microsoft Word 2003–2013 до выхода соответствующего обновления.

Бэкдор содержит вспомогательный модуль для работы с удаленным сервером через сервис микроблогов Twitter. Для управления вредоносным ПО его авторы используют twitter-аккаунт @FloydLSchwartz. MiniDuke обращается к нему втайне от пользователя и ищет твиты, содержащие тэг «X)))» (в предыдущей модификации программы – «uri!»).

Обнаружив твит с нужным тэгом, MiniDuke переходит по указанной в посте ссылке и передает данные о жертве на удаленный сервер. Авторы бэкдора получают имя компьютера и домена, код страны IP-адреса, информацию о версии ОС, список установленных антивирусных продуктов, конфигурацию прокси и другие сведения.

Кроме того, бэкдор способен загружать из сети и запускать на зараженном компьютере новые вредоносные программы.

MiniDuke детектируется антивирусными решениями ESET NOD32 как Win32/SandyEva.G, вредоносный RTF-документ, через который распространяется эксплойт, – как Win32/Exploit.CVE-2014-1761.D ***(Обнаружен бэкдор, управляемый через Twitter // IT Expert (http://itexpert.org.ua/rubrikator/item/36020-obnaruzhen-bekdor-upravlyaemyj-cherez-twitter.html). – 2014. – 29.05).***

***

Не успело приложение для анонимного обмена секретами Secret запуститься по всему миру, как его уже успели заблокировать и разблокировать в России, слить несколько забавных инсайдов и, конечно же, обнаружить уязвимость, с помощью которой можно пренебречь анонимностью сервиса и вычислить, что публикуют ваши друзья. Для этого достаточно иметь номер телефона человека, которого вы хотите идентифицировать, а также немного терпения, пишет AIN.UA (http://ain.ua/2014/05/29/526423).

Приложение Secret составляет список друзей на основании телефонных номеров из контактов на вашем смартфоне. Казалось бы, можно удалить все контакты кроме одного и узнать, какими секретами делился этот человек. Но не тут-то было – Secret начнет показывать записи только тогда, когда в приложении найдется как минимум трое ваших друзей, и пометки friend на их секретах не будет – они просто смешаются в ленте с незнакомцами.

Пометка friend появится только тогда, когда друзей станет минимум пять.

Такую защиту можно обойти элементарным способом. Создайте несколько поддельных аккаунтов. Аккаунты в Secret привязываются к номеру телефона, но для этого не нужно несколько разных SIM-карт. Просто введите случайные номера телефонов, игнорируя SMS-верификацию. Это удобнее делать в веб-версии. В телефонной книжке вашего смартфона должны остаться только эти вымышленные номера и номер того, кого вы хотите вычислить в Secret.

Если у вас уже есть учетная запись, придется создать новую. Понадобится новый номер, зато новый почтовый ящик создавать не нужно. Как заметили в TJournal, Gmail игнорирует точку в почтовом адресе, поэтому example@gmail.com, ex.ample@gmail.com и exam.ple@gmail.com будут вести в один и тот же электронный ящик. При этом Secret при регистрации такие адреса будет воспринимать как разные, так что владелец одного и того же почтового ящика сможет зарегистрировать на него несколько аккаунтов.

Вся операция занимает не более 10 минут. В итоге, создав пять поддельных аккаунтов и занеся в телефонную книгу интересующий номер, вы сможете увидеть его посты в ленте – только они будут появляться с пометкой friend.

Поэтому прежде чем «сливать» корпоративные инсайды в Secret, задумайтесь: а вдруг в этот самый момент за вами наблюдает ваш начальник? ***(В Secret обнаружена уязвимость, позволяющая вычислить анонимов // AIN.UA (http://ain.ua/2014/05/29/526423). – 2014. – 29.05).***

***

Новый банковский троян, маскирующийся под легитимное приложение WeChat, используется для сбора финансовых данных владельцев Android-устройств из Китая. Согласно данным «Лаборатории Касперского»,

злоумышленники выбрали эту программу, поскольку многие пользователи используют именно ее для осуществления платежей.

После установки на Android-устройства вредонос, получивший название «Banker.AndroidOS.Basti.a», запрашивает разрешение на получение доступа к сети, входящим SMS-сообщениям и пр.

Авторы трояна зашифровали его при помощи App Shield, позволяющим добавлять несколько «слоев защиты», говорят в ЛК. Тем не менее, ИБ-экспертам компании удалось расшифровать файл, после чего они установили, что он может также использоваться в качестве инструмента для осуществления фишинга.

После запуска вредоносного приложения жертве отображается страница, на которой ее просят ввести номера телефонов, банковских карт, PIN-коды и прочую банковскую информацию. Собранные данные отправляются на подконтрольный злоумышленникам адрес электронной почты.

В «Лаборатории Касперского» говорят, что исходный код трояна содержит название этого адреса и даже пароль, требуемый для входа в учетную запись. Воспользовавшись этим, специалисты обнаружили, что вредоносную программу скачало уже довольно много людей ***(Банковский троян маскируется под мессенджер WeChat // InternetUA (http://internetua.com/bankovskii-troyan-maskiruetsya-pod-messendjer-WeChat). – 2014. – 29.05).***

***

Эксперты по безопасности из Bitdefender сообщили, что троян для мгновенных сообщений заразил сотни компьютеров по всему миру.

Вредоносная программа, определена Bitdefender как Gen: Variant Downloader.167, распространяется благодаря опции мгновенного обмена сообщениями Facebook и Yahoo Messenger. Эксперты сообщают, что вредоносное ПО использует «вежливые» сообщения с зараженного компьютера, которые рассылаются по базе контактов жертвы. К примеру: «Я хочу разместить эти фотографии на Facebook, как думаешь, они нормальные?».

К сообщениям также прикреплены ссылки на популярные сервисы обмена файлами – Fileswap и Dropbox, где находится вредоносное ПО. Представители Bitdefender сообщили The Register о том, что вредоносный файл создает папку со случайным именем в Application Data и копирует себя в эту папку со случайным именем и .exe расширением.

Затем вирус создает запись в реестре HKCU\Software\Microsoft\Windows\CurrentVersion\Run с именем Counter Background WWAN Thread Mapper User NetBIOS. После того как все шаги выполнены, жертва получает уведомление на экране инфицированного компьютера: «Это приложение не совместимо с данной версией Windows. Проверьте системную информацию вашего компьютера, чтобы узнать

необходима вам x86 (32-разрядная) или x64 (64-разрядная) версия программы, затем свяжитесь с поставщиком программного обеспечения».

Другой исполняемый файл со случайным именем создается в той же папке – в Application Data. Этот файл запускается с двумя параметрами: WATCHDOGPROC, создавая путь к первому файлу. В конечнем итоге, файл конфигурации создается в той же папке, и вредоносная программа подключается к командованию и управлению сервером.

Согласно Bitdefender, киберпреступники могут управлять трояном для загрузки других вредоносных программ, что может создать угрозу конфиденциальности данных. Наибольшее число инфицированных компьютеров зарегистрировано в Румынии, Германии и Канаде ***(Новый чат-троян распространяется при помощи Yahoo Messenger и Facebook // InternetUA (http://internetua.com/novii-csat-troyan-rasprostranyaetsya-pri-pomosxi-Yahoo-Messenger-i-Facebook). – 2014. – 29.05).***

***

В парламент внесен проект закона об информационной безопасности. В нем впервые вводятся определения «киберпреступности», «кибербезопасности», «кибертерроризма» и «киберпространства». Текст закона разрабатывали специалисты Госспецсвязи, СБУ и МВД. До сих пор преступления, связанные с хакерскими атаками, взломами и т. п., рассматривались по ст. 361 Уголовного кодекса Украины («вмешательство в работу компьютеров или компьютерных сетей»), пишет AIN.UA (http://ain.ua/2014/05/30/526523).

Например, киберпреступность определяется как противоправные действия, которые совершаются с использованием компьютера и телеком-сетей, нарушают конфиденциальность, целостность и доступность данных, направлены на перехват, изменение или уничтожение данных и т. д.

Но сфера действия проекта закона – шире, чем проделки хакеров. Законопроект призван регулировать вопросы информационной безопасности в Украине. Авторы проекта поясняют, что такая необходимость появилась в связи с агрессивной информационной политикой России – в частности, с тем, что российские медиа разжигают сепаратистские настроения и межнациональную вражду.

В проекте предлагается защитать граждан «от негативного влияния информационных технологий и информационно-психологического влияния». В документе перечислены такие угрозы информационной безопасности, как недостоверная информация об Украине, которую распространяют иностранные державы, способы манипулирования сознанием, которые используют иностранные спецслужбы, незаконный перехват информации в сети, создание иностранными государствами кибервойск или киберподразделений в традиционных войсках и т. д.

Также, в законе упоминается «критическая зависимость» национальной информационной инфраструктуры от иностранных производителей технологической продукции.

Отдельный интересный пункт закона касается «улучшения правового регулирования» ситуаций, когда украинцы или другие лица покупают бумажные и электронные СМИ.

Предполагается также создать Национальную комиссию по информационной безопасности, которая и будет заниматься этими вопросами. Члены комиссии будут назначаться Кабмином. Органы, ответственные за информбезопасность, должны будут препятствовать распространению информации, которая угрожает суверенитету и территориальной целостности Украины, манипулирует сознанием ее населения.

Напомним, в начале мая и. о. Президента А. Турчинов подписал указ об информационной безопасности. Там, в частности, речь идет о создании национальной ОС и антивируса. В Госкомтелерадио уже разработали проект стратегии развития информационного пространства, где, кроме прочего, предлагается лицензировать онлайн-СМИ ***(МВД и СБУ написали первый в истории Украины закон о кибербезопасности // AIN.UA (http://ain.ua/2014/05/30/526523). – 2014. – 30.05).***

***

Специалист по безопасности С. Сидор заявляет, что камеру современного устройства можно заставить следить за владельцем. С. Сидор добился такого результата на смартфоне под управлением операционной системы Android.

Программист написал утилиту для камеры устройства Nexus 5. Размер фотографий или видео, которые делаются на камеру устройства, достигает 1x1 пиксель.

Они настолько малы, что человек не может их увидеть, даже если знает, где искать этот файл. Таким образом, злоумышленники могут заставить камеру работать против владельца мобильного устройства, а он, при этом, даже не будет подозревать о слежке.

Данное решение идеально подходит для шпионажа, и С. Сидор отмечает, что нам остаётся только гадать, какое именно количество смартфонов сегодня «подглядывает» за жизнью своих владельцев без их ведома.

В свою очередь, власти Германии и Австралии обеспокоены возможностями беспроводного контроллера Kinect, который будет поставляться вместе с консолью Xbox One. В частности, главы государств не исключают, что камеры Kinect будут следить за гостиной без ведома пользователей ***(Камера смартфона может шпионить за пользователем без его ведома // Блог Imena.UA (http://www.imena.ua/blog/android-camera-spy/). – 2014. – 30.05).***

***

С помощью недорогого оборудования можно нарушить работу систему отслеживания кораблей и прервать связь межу судами и портами. Такие результаты продемонстрировали два исследования по безопасности.

29 мая, на конференции Hack in the Box, в Амстердаме, старший научный сотрудник по безопасности Trend Micro М. Балдуци и независимый исследователь А. Паста описали три новых вида атаки, которые могут быть направлены на Автоматическую идентификационную систему (АИС). Ею пользуются более 40 тыс. судов по всему миру. АИС сообщает о месте локации, навигационном статусе, скорости и местонахождении береговых станций. Администрация портов также использует АИС для отправки важной информации на корабли.

Эксперты по безопасности в прошлом году предупреждали о том, что отсутствие аутентификации и проверки протокола связи АИС может позволить пиратам, террористам и другим злоумышленникам искажать информацию, посылаемую на судна, или указывать неверное местонахождение кораблей. М. Балдуци и А. Паста провели эксперимент на земле, использовав оборудование стоимостью 600 дол. Эксперты смогли посылать сигнал на расстояние в 20 км, но в море он может достигнуть и большего расстояния, из-за меньшего количества помех. Они добавили, что при использовании более дешевых запчастей АИС передатчик можно собрать менее чем за 100 дол.

АИС можно также использовать в качестве канала для эксплуатации уязвимостей в программном обеспечении, установленном на серверные системы, которые собирают и обрабатывают данные АИС. Эксперты обнаружили возможность внедрения SQL-инъекции в систему, использующуюся капитанами кораблей для хранения данных о прогнозе погоды, которые предоставляет АИС. Уязвимость может позволить полностью удалить базу данных или заменить информацию о погоде.

29 мая эксперты рассмотрели еще один тип атаки – спуфинг-атака на дифференциальную систему глобального позиционирования (DGPS). DGPS предоставляет более точные данные GPS. В случае, если поток данных DGPS будет сфальсифицированным – корабль отклонится от назначенного курса.

По данным Международной морской организации (ИМО), агентство ООН несет ответственность за безопасность судоходства. Все суды, которые являются пассажирскими и осуществляют международные рейсы должны использовать АИС. Представители ИМО пока никак не прокомментировали информацию об уязвимостях в АИС.

Полностью решение данной проблемы потребует встраивания защищенного протокола передачи данных в систему безопасности, а затем обновления или замены оборудования АИС, установленного на судах, в портах и наземных станциях ***(Система отслеживания местонахождения кораблей является уязвимой к разного рода кибератакам // InternetUA***

(http://internetua.com/sistema-otslejivaniya-mestonahojdeniya-korablei-yavlyaetsya-uyazvimoi-k-raznogo-roda-kiberatakam). – 2014. – 31.05).

***

Согласно прогнозу экспертов из исследовательской компании Gartner, до 2017 г. большинство кибератак будет осуществляться на мобильные устройства. По их данным, 75 % от всех инцидентов безопасности с планшетами и смартфонами будут связаны с ошибками в конфигурации приложений.

«Бреши в безопасности мобильных устройств являются в настоящее время и будут в дальнейшем, скорее, результатом ошибок в конфигурации и неправильного использования приложений, чем результатом глубоко технических атак на мобильные устройства, – сообщил главный аналитик по исследованиям Gartner Д. Зумерле. – Классическим примером ошибки в конфигурации является некорректное использование персональных облачных сервисов через приложения, установленные на смартфоны и планшеты. При использовании для передачи корпоративных данных эти приложения могут привести к утечке информации».

По словам Д. Зумерле, наибольший ущерб вредоносное ПО может нанести на устройствах, которые были изменены на административном уровне. Смартфоны и планшеты, на которых был осуществлен джейлбрейк, позволяют пользователям устанавливать приложения, недоступные на обычных устройствах. Тем не менее, необходимо помнить, что они также предоставляют угрозу безопасности данных, поскольку удаление защиты и безопасной песочницы позволяет загружать на устройство вредоносное ПО и осуществлять вредоносные действия ***(До 2017 года большинство кибератак будет осуществляться на мобильные устройства // InternetUA (http://internetua.com/do-2017-goda-bolshinstvo-kiberatak-budet-osusxestvlyatsya-na-mobilnie-ustroistva). – 2014. – 31.05).***