СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(7–20.09)

2015 № 16

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(7.09–20.09)
№ 16

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

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

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 4
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 18
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 25
Інформаційно-психологічний вплив мережевого спілкування на особистість 25
Маніпулятивні технології 26
Зарубіжні спецслужби і технології «соціального контролю» 29
Проблема захисту даних. DDOS та вірусні атаки 35

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Глобальная соцсеть для общения по профессиональным интересам анонсировала обновление функционала интерфейса личных сообщений, который на протяжении последних лет был объектом насмешек и критики среди пользователей ресурса. В новом продукте стали доступны современные средства общения, такие как GIF-анимация, стикеры и поддержка вложений. Об этом пишет cossa.ru

В компании заявляют, что ее новый инструмент для коммуникации стал больше похож на популярные мобильные мессенджеры, наподобие приложения-чата от Facebook, и включает целый набор современных опций, включая возможность написать сообщение сразу нескольким адресатам.

«Нам очень нравится концепция интеллектуальных помощников-мессенджеров, которые способны предлагать подходящие контакты для общения или предоставлять релевантную информацию о пользователе, которому вы собираетесь написать. Также нам интересно развитие голосового и видеофункционала, чтобы сделать коммуникацию более удобной», – говорит М. Халл (Mark Hull), директор департамента управления продуктами компании.

В настоящее время LinkedIn тестирует обновленный сервис для общения среди ограниченного количества англоязычных пользователей как в мобильных клиентах социальной сети и веб-версии сервиса ***(LinkedIn перезапустила сервис обмена сообщениями // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44560/118/lang,ru/). – 2015. – 7.09).***

***

Компания Microsoft готовит к выпуску новый универсальный мессенджер. Он получил название Skype Central и представляет собой агрегатор сообщений для Windows 10. Однако обычный Skype он не заменит.

По сути речь идет о новом приложении, которое заменит центр уведомлений. С его помощью разработчики смогут собирать и анализировать информацию о проблемах Windows 10, рассказывать об обновлениях и делиться важными новостями. Какие-либо другие подробности не уточняются.

Skype Central может дебютировать в ноябре 2015 г. в составе нового обновления для Windows 10, которое также принесет поддержку расширений для браузера Edge ***(Skype Central заменит центр уведомлений Windows 10 // InternetUA (http://internetua.com/Skype-Central-zamenit-centr-uvedomlenii-Windows-10). – 2015. – 7.09).***

***

Популярный микроблоговый сервис объявил о перезапуске мобильных клиентов для устройств на платформе iOS: теперь у продуктов будет обновленный и более универсальный функционал и дизайн.

Ранее «Твиттер»-приложения для iPhone и iPad предлагали довольно разный пользовательский опыт, но сейчас компания заявляет, что владельцы обоих устройств смогут создавать и просматривать ретвиты с комментариями, использовать функцию трендовых тем в поиске, заходить на страницы товаров и мест и т. д.

Кроме того, адаптивный дизайн – результат длительной совместной разработки дизайнеров и инженеров компании – способен поддерживать самые современные гаджеты и версии ОС от Apple, утверждают представители «Твиттера» в официальном блоге: «В конечном счете, больше не будет “Твиттера” для iPhone и “Твиттера” для iPad – будет “Твиттер” для iOS. Это та свобода, которая позволит нам предоставить лучший опыт для пользователей сервиса, независимо от устройства» ***(«Твиттер» унифицировал приложения для iPhone и iPad // ReklaMaster.com (http://reklamaster.com/business-and-innovations/tvitter-unificiroval-prilozhenija-dlja-iphone-i-ipad). – 2015. – 11.09).***

***

Сайт «ВКонтакте» запустил новый инструмент модерации для групп и публичных страниц – фильтр комментариев. Об этом «Ленте.ру» сообщил глава пресс-службы соцсети Г. Лобушкин.

«Это значительный шаг, облегчающий ведение крупных страниц СМИ и брендов, для которых чистота дискуссий в комментариях на их страницах “ВКонтакте” имеет решающее значение. Некоторые сообщества получают тысячи комментариев от своих подписчиков каждый день. Этот инструмент позволит снизить издержки на модерацию страниц и минимизирует репутационные риски для компаний», – рассказал Г. Лобушкин.

Фильтр позволит в автоматическом режиме удалять нежелательные записи, содержащие нецензурные выражения или любые другие ключевые слова, по выбору администратора страницы.

По словам Г. Лобушкина, нововведение уже сейчас доступно первым 50 млн групп, пабликов и страниц, посвященным мероприятиям. Для администраторов будет доступно два варианта модерации – с использованием нецензурных выражений на основе словаря, составленного при участии профессиональных филологов и лингвистов, а также появится возможность составлять свой список стоп-слов. Любые комментарии, попавшие под фильтр, будут автоматически удалены сразу после их публикации.

Фильтр нецензурных слов будет доступен на нескольких языках – русском, украинском, казахском и английском ***(Ругаться матом в комментариях на «ВКонтакте» теперь будет сложно // InternetUA (http://internetua.com/rugatsya-matom-v-kommentariyah-na--vkontakte--teper-budet-slojno). – 2015. – 11.09).***

***

Кількість українських користувачів за останній рік зросла на 30 %, в абсолютних цифрах приріст становив 1 млн. Станом на вересень 2015 р. в Україні 4,5 млн користувачів Facebook (у вересні 2014 р. було 3,5 млн).

За методологією Facebook користувачами соцмережі є люди, які хоча б раз протягом останніх 30 днів заходили в соцмережу, будучи при цьому залогіненими. Тобто в цій статистиці не враховуються, наприклад, зареєстровані користувачі, які не заходять у соцмережу протягом останніх 30 днів.

Аудиторія Facebook в Україні вже третій рік поспіль приростає стабільно на 25–30 % ***(Кількість користувачів Facebook в Україні за рік зросла на 30 % // UkrainianWatcher (http://watcher.com.ua/2015/09/11/kilkist-korystuvachiv-facebook-v-ukrayini-za-rik-zrosla-na-30/). – 2015. – 11.09).***

***

Компании Google и Twitter объединят усилия для создания новостного сервиса. Он будет отличаться от создаваемых продуктов конкурентов использованием открытого исходного кода. Об этом сообщает ресурс Re/Code, ссылаясь на источники на рынке.

Сервис получит название Instant Articles («мгновенные статьи»). С его помощью издатели смогут показывать свои материалы на мобильных устройствах, использующих сервисы двух интернет-компаний. Планируется, что тестировать продукт будут осенью при участии небольшой группы издателей.

Ожидается, что проект будет конкурировать с готовящимися к запуску аналогичными сервисами Facebook, Apple и Snapchat.

Основным отличием проекта является использование открытых исходных кодов, благодаря чему Google и Twitter надеются привлечь к нему крупные компании. Такой сервис не будет привязывать издателя к определенному рекламодателю, Google можно будет сменить на альтернативного поставщика. Кроме того, издателям не придется делать отдельную версию своих страниц для использования в этом сервисе.

Re/Code отмечает, что создание нового сервиса может быть выгодно Google для конкурентной войны с соцсетью Facebook, которая оттягивает пользователей на себя, что снижает доходы разработчика популярной поисковой системы. Также факт совместной работы с Twitter намекает на возможную покупку компанией Google сети микроблогов, однако не означает, что она обязательно произойдет.

Информация о создании новостной функции Lightning в Twitter появилась 19 июня этого года, но тогда речь шла о самостоятельном сервисе. Летом Facebook начал тестировать сервис Instant Articles с несколькими издателями – он позволял читать материалы, не выходя из соцсети. Также появлялась неофициальная информация о новостных сервисах Apple News, а Instagram запустил сервис актуальных фотографий Explore ***(Google и Twitter***

объединятся для создания новостного сервиса // InternetUA (http://internetua.com/Google-i-Twitter-ob-edinyatsya-dlya-sozdaniya-novostnogo-servisa). – 2015. – 13.09).

***

Современные пользователи все чаще читают интернет-новости и журнальные публикации с мобильных устройств и все реже готовы мириться с медленной загрузкой страниц, на которую может уходить по 5–10 секунд. Google и Twitter совместно работают над новой технологией, которая позволит сократить время загрузки до нескольких миллисекунд.

Речь идет о создании новой системы интернет-ссылок и хранения данных, которая позволит изданиям (в проекте участвуют, в частности, The Guardian и The New York Times) сделать потребление новостей более удобным для читателей, при этом не отказываясь от размещения рекламных баннеров и не адаптируя специальным образом форматирование материалов.

Источники The New York Times, осведомленные о ходе работы над проектом, подчеркивают, что он пока находится на ранней стадии, и многие детали до сих пор не определены окончательно. Однако отношение к нему самое серьезное – в Google и Twitter опасаются, что издания предпочтут распространять свой контент с помощью проприетарных систем вроде Facebook Instant Articles или Apple News.

В этом случае та же Google может потерять свои доходы как посредника при продажах рекламы. Целью Twitter, в свою очередь, является удержание пользователей внутри своих приложений или на сайте. Для этого им надо дать возможность с удобством читать материалы, ссылки на которые опубликованы в сервисе, не покидая приложение.

Для того, чтобы реализовать быструю загрузку, сайтам придется лишь незначительно модифицировать код своих веб-страниц, а также разрешить их кэширование для быстрой загрузки в браузерах, приложениях-клиентах Twitter или на других сервисах, даже тех, которые не участвуют в проекте. Известно, что решение будет совместимо и с блогами, работающими на платформе WordPress.

Официальный анонс, по данным The New York Times, может состояться в ближайшие 4–6 недель ***(Google и Twitter заставят веб-страницы загружаться мгновенно // InternetUA (http://internetua.com/Google-i-Twitter-zastavyat-veb-stranici-zagrujatsya-mgnovenno). – 2015. – 15.09).***

***

Фильтрация спама – одна из самых главных задач, которую решают инженеры Facebook. Крупнейшая социальная сеть обрабатывает сообщения от более 1,5 млрд человек, так что можно оценить масштаб проблемы. Недавно компания внедрила новые антиспамерские фильтры, для разработки которых использовала язык программирования Haskell.

Haskell – стандартизированный чистый функциональный язык программирования общего назначения. Разработан в начале 90-х группой ученых в качестве экспериментального языка для ленивого функционального программирования. На сайте Github сейчас занимает 23-ю строчку по популярности среди языков программирования.

Несмотря на молодость, экспериментальный статус и относительно низкую популярность, Facebook выбрал именно Haskell для создания важного модуля. Один из инженеров Л. Брэнди (Louis Brandy), который входит в группу разработчиков нового антиспамерского фильтра, провел два года за этим проектом вместе с коллегами. В интервью Wired он объяснил, чем они руководствовались.

Выбор языка программирования – по-настоящему больная тема для многих разработчиков. Вокруг этой темы постоянно разгораются споры. Почти у каждого есть личные предпочтения, которые влияют на объективные технические параметры для выбора ЯП.

Чтобы не разжигать флейм, Л. Брэнди, аккуратно подбирая слова, назвал Haskell идеально подходящим для реализации спам-фильтра в Facebook, потому что он отлично обрабатывает параллельные задачи и позволяет разработчикам легко и удобно устанавливать эти задачи на лету. Facebook настолько большой проект, а спамеры настолько быстро меняют тактику, что необходим инструмент для разработки и постоянной модификации спам-фильтров, которые вступят в действие немедленно.

Если посмотреть на развитие современного Интернета, то по этому пути должны пойти многие интернет-проекты, для которых важны масштабируемость и реагирование в реальном времени. По мнению разработчиков Facebook, у языка Haskell есть все шансы на широкую популярность. Мешает только тот факт, что Haskell довольно сильно отличается от других языков – и это затрудняет массовую миграцию на него. Тем не менее, индустрия точно двигается в нужном направлении, как показывает пример новых языков программирования, ориентированных на выполнение параллельных процессов, например, Go от Google и Rust от Mozilla. Пусть они не такие эффективные, как Haskell, зато проще в изучении. В любом случае, Haskell можно поблагодарить за то, что он подтолкнул к развитию другие языки программирования и способствовал запуску новых перспективных проектов ***(Почему Facebook выбрал редкий язык Haskell для антиспамерского фільтра // InternetUA (http://internetua.com/pocsemu-Facebook-vibral-redkii-yazik-Haskell-dlya-antispamerskogo-filtra). – 2015. – 14.09).***

***

Социальная сеть Facebook работает над созданием самостоятельного мобильного приложения с поддержкой сферического видео. Об этом сообщает lenta.ru со ссылкой на The Wall Street Journal (WSJ).

Детали проекта пока неизвестны. Как правило, формат «360 градусов» подразумевает возможность смены ракурса в роликах при помощи наклона смартфона.

Планируется, что приложение будет работать на операционных системах iOS и Android. Пока оно находится на ранней стадии разработки, и непонятно, увидит ли свет. В Facebook информацию источников WSJ не прокомментировали.

Как считает газета, приложение поможет Facebook популяризовать технологию виртуальной реальности среди тех, кто еще с ней не знаком, и закрепиться в этой перспективной сфере.

Гендиректор соцсети М. Цукерберг заявлял, что виртуальная реальность станет следующей «компьютерной платформой» для мобильных устройств. В марте на конференции Facebook для разработчиков F8 он анонсировал поддержку трехмерного видео для ленты новостей соцсети, которую в самой компании назвали функцией «телепортации». Просмотр роликов осуществляется при помощи очков Oculus Rift. М. Цукерберг не уточнил, когда компания внедрит новую опцию.

Компания Facebook приобрела Oculus VR, разрабатывающую очки дополненной реальности Oculus Rift, за 2 млрд дол. в прошлом году. Deutsche Bank подсчитал, что гаджеты Oculus разойдутся 1,5-миллионным тиражом в 2016 г.

В настоящее время просмотр с разных ракурсов реализовал Google: функция Choose Your View на YouTube позволяет в роликах переключаться между различными точками, с которых велась съемка. ***(WSJ сообщила о разработке приложения виртуальной реальности от Facebook // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44639/118/lang,ru/). – 2015. – 14.09).***

***

В Facebook появился режим потокового видеовещания, с помощью которого можно вести репортажи.

До сих пор репортеры и блогеры пользовались приложениями Periscope или Meerkat. Теперь эстафету перехватило приложение Facebook Mentions. Чтобы воспользоваться новой функцией Live Stream, достаточно иметь верифицированную учетную запись в Facebook. Репортаж становится доступен для просмотра всем, кто подключился к каналу, сразу после завершения съемки ***(Теперь в Facebook можно вести репортажи // GlavPost.Com (http://glavpost.com/post/14sep2015/Nets/59014-teper-v-facebook-mozhno-vesti-reportazhi.html). – 2015. – 15.09).***

***

В ближайшее время Skype начнет поддерживать отправку и просмотр Mojis – коротких нарезок из фильмов и мультиков.

Первые нарезки сделаны из «Маппет-шоу», мультфильма «Гадкий Я», а также фильмов «Парк Юрского периода», «Девичник в Вегасе», «Идеальный голос» и других. Партнером Microsoft в этом проекте выступили Disney Muppets, Universal Studios и BBC.

По мнению Microsoft, Mojis помогут пользователям Skype выражать свои эмоции. Сейчас мессенджер Microsoft поддерживает отправку смайликов эмодзи, фотографий, а также аудио- и видеоконента. Когда Skype начнет поддерживать Mojis, неизвестно. Microsoft пишет, что это случится в ближайшие несколько дней ***(В Skype появится отправка заготовленных нарезок из фильмов // InternetUA (http://internetua.com/v-Skype-poyavitsya-otpravka-zagotovlennih-narezok-iz-filmov). – 2015. – 16.09).***

***

Facebook має намір зробити свій внесок у підключення нашої планети до Інтернету. Торік соціальна мережа створила дослідний підрозділ Connectivity Lab, фахівці якого займаються проблемою розширення меж існуючої мережевої інфраструктури. Команда проекту регулярно рапортує про свої успіхи, і повідомлення про завершення будівництва гігантського дрона Aquila не залишилося без нашої уваги.

У Facebook збираються використовувати безпілотні літальні апарати для роздачі Інтернету у віддалених регіонах. За розмахом крил дрони не поступаються авіалайнеру Боїнг 737, а завдяки легкому корпусу з каркасом з вуглецевого волокна вони важать у сотні разів менше пасажирського літака. За допомогою повітряних куль безпілотники піднімуть на висоту 18–27 км, де вони будуть планувати над потрібним ділянкою поверхні до 90 днів.

Facebook Aquila працюють на сонячних батареях і укомплектовані спеціальною лазерною установкою, призначеної для обміну даними з іншими дронамі і наземними станціями. Під час випробувань інженерам вдалося передавати інформацію на швидкості в кілька десятків гігабайт у секунду. За словами представників Connectivity Lab, приймач сигналу був розміром з монету і розміщений на відстані 16 км.

Facebook вже запускала в небо зменшену копію Aquila. Коли компанія збирається почати тестування фінальної версії безпілотника, не повідомляється ***(Facebook показала фінальну версію інтернет-дрона Aquila // Webblack.net (http://webblack.net/facebook-pokazala-finalnu-versiyu-internet-d/). – 2015. – 16.09).***

***

Facebook працює над появою в соціальній мережі кнопки Dislike («Не подобається»). Про це повідомив засновник і керівник компанії М. Цукерберг під час сесії запитань та відповідей.

«Люди просили про кнопку Dislike вже багато років. Сьогодні – особливий день, коли я можу сказати, що ми активно тестуємо цю функцію і незабаром вона з’явиться в соцмережі», – розповів М. Цукерберг.

При цьому М. Цукерберг уточнив, що Dislike не буде схожа на голосування «проти» публікації. Інколи людина хоче якось відреагувати на пост у Facebook в один клік, але при цьому кнопка like в цій ситуації може бути не дуже коректною. Наприклад, коли мова йде про тексти із сумним змістом ***(У Facebook з'явиться кнопка Dislike («Не подобається») // UkrainianWatcher (http://watcher.com.ua/2015/09/16/u-facebook-zyavytsya-knopka-dislike-ne-podobayetsya/). – 2015. – 16.09).***

***

Разработчик мессенджеров Symphony Communication Services объявил о запуске социальной сети для финансовых организаций Уолл-стрит. Проект под названием Symphony позиционируется как более дешевая и удобная альтернатива терминалам Bloomberg и Thomson Reuters, которыми пользуются трейдеры по всему миру.

Корпоративные подписчики платформы Symphony должны будут платить по 15 дол. в месяц, тогда как стоимость использования терминалов Bloomberg за тот же период составляет 1850 дол. При этом малый бизнес и частные предприниматели могут работать с Symphony бесплатно.

Инвесторами в новом проекте выступают ряд крупных финансовых компаний, включая Goldman Sachs, Bank of America Merril Lynch, Deutsche Bank, Credit Suisse, Citigroup и др. Партнерами являются McGraw Hill Financial (поставляет финансовый инструмент S&P Capital IQ для новой соцсети), Dow Jones (отвечает за новостную составляющую) и Selerity (обеспечивает интернет-поиск информации, теоретически способной влиять на котировки).

Платформой Symphony в тестовом режиме уже пользуется более 30 тыс. банкиров и управляющих активами. Глава Symphony Дэвид Герл (David Gurle) отметил, что при поддержке партнеров компания стремится создать «незаменимый инструмент для коммуникаций, совместной работы и документооборота».

***

Российская социальная сеть «ВКонтакте» опубликовала статистику по украинскому сегменту. Компания подытожила количество десктопных и мобильных пользователей, гендерное и возрастное распределение, а также уровень достатка пользователей соцсети (http://tech.obozrevatel.com/hi-tech/37201-kakie-ukraintsyi-polzuyutsya-vkontakte-opublikovana-infografika.htm).

Данные основаны на результатах исследования Opinion Software Media от Factum Group, передает AIN.

В июле 2015 г., по данным Factum Group, среднесуточное количество пользователей «ВКонтакте» в Украине составило 12,9 млн пользователей.

Гендерно-возрастное распределение существенных изменений не претерпело. Украинская аудитория «ВКонтакте» взрослеет, доля 12-летних подростков почти полностью размылась, им на смену пришли люди, которым за сорок. Самые большие возрастные категории: 25–34 года и 45–46 года.

Если верить статистике, больше всего во «ВКонтакте» специалистов и руководителей. Меньше всего – служащих и домохозяек. Впрочем, не стоит забывать основную прелесть социальных сетей – в них ты можешь быть тем, кем душа пожелает.

Согласно данным Factum Group за июль 2015 г., расположение сил не изменилось – богачи все еще предпочитают «ВКонтакте» Facebook и «Одноклассникам».

За последние полгода заметно возросла доля мобильных устройств среди пользователей «ВКонтакте». Если в октябре 2014 г. на мобайл приходилось 28 % всех заходов, то в июле их количество достигло 39 %. При этом сразу на 10 % уменьшилось количество тех, кто заходит одновременно с десктопа и мобильного. Вероятно, за их счет и возросла доля исключительно мобайла.

Доля iOS-пользователей не изменилась, а вот Android вырос с октября 2014 г. на 600 тыс. пользователей. Суммарно на сайт, во данным LiveInternet за август 2015 года, ежедневно заходит 4,9 млн мобильных пользователей ***(Какие украинцы пользуются «ВКонтакте»: опубликована инфографика // Обозреватель (http://tech.obozrevatel.com/hi-tech/37201-kakie-ukraintsyi-polzuyutsya-vkontakte-opublikovana-infografika.htm). – 2015. – 16.09).***

***

Facebook запустит корпоративную версию соцсети Facebook at Work, сообщает Bloomberg. Директор Facebook по глобальному партнерству Ж. Кодорню рассказал изданию, что бета-тестирование новой системы начнется в конце 2015 г. Об этом пишет sostav.ru

Корпоративный Facebook будет ориентирован именно на деловую обстановку и будет доступен для офисных сотрудников бесплатно. В описании системы говорится, что Facebook at Work – инструмент, который помогает коллегам общаться и сотрудничать в профессиональной среде на Facebook.

Причин для создания такой сети у руководства FB было несколько. Во-первых, пользователи Facebook чаще всего общаются по рабочим вопросам, и выделить эту часть аудитории в отдельную соцсеть в компании посчитали удачным решением. К тому же, Facebook не прочь посоперничать с аналогичными продуктами – закрытой сетью Yammer (Microsoft) и корпоративным мессенджером Slack, который оценивается в 2,8 млрд дол.

Сами сотрудники Facebook уже активно используют корпоративную версию для выполнения служебных обязанностей. К тому же, с января этого года соцсеть проводит закрытое тестирование, в котором приняли участие более 100 компаний. Facebook сообщил Business Insider, что он уже выкатила продукт для нескольких известных компаний, в частности для брендов Heineken и HootSuite. В этих компаниях уже сообщили, что по результатам тестирования зафиксировали повышение производительности среди сотрудников.

Корпоративная версия FB доступна и для российских компаний. «Facebook at Work позволяет создавать рабочие аккаунты Facebook, не

связанные с личными. Аккаунт Facebook at Work позволяет использовать инструменты Facebook для взаимодействия с коллегами. Материалы, которыми вы делитесь с рабочего аккаунта, увидят только ваши колеги», – говорится в описании русскоязычного проекта.

Для настройки рабочего аккаунта сотрудника в соцсети нужно, чтобы компания начала использовать Facebook at Work. Сделать это можно будет только в конце 2015 г., когда начнется бета-тестирование корпоративной системы.***(Facebook запустит корпоративную соцсеть // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44702/118/lang,ru/). – 2015. – 17.09).***

***

Социальная сеть Twitter запускает во всем мире функцию Highlights, благодаря которой владельцы Android-устройств будут получать подборку самого интересного контента.

Функция Highlights была запущена в апреле 2015 г., однако до настоящего момента была доступна только на английском языке. С ее помощью пользователи могут знакомиться с подборками самых интересных событий в их ленте твитов.

При создании сводок Highlights Twitter учитывает различные факторы, связанные с вашей лентой и популярными событиями в регионе. Приложение будет дважды в день сообщать о готовности дайджеста с помощью push-уведомлений. Однако с подборкой можно ознакомиться в любое время. В скором времени функция будет доступна и на других платформах ***(Twitter запускает сервис для подбора интересных твитов // InternetUA (http://internetua.com/Twitter-zapuskaet-servis-dlya-podbora-interesnih-tvitov). – 2015. – 17.09).***

***

Пользователи Facebook скоро получат возможность устанавливать временную аватарку в своем профиле взамен основной.

Смена аватарки считается пользователями Facebook важным событием, поэтому они уделяют большое внимание ее выбору. Но иногда возникает желание заменить временно основную аватарку, например, чтобы отразить настроение, место пребывания или текущее занятие. Facebook проводит тестирование такой опции. Через пару месяцев она станет доступна всем желающим ***(Facebook разрешит пользователям устанавливать временную аватарку // GlavPost.Com (http://glavpost.com/post/17sep2015/Nets/59610-facebook-razreshit-polzovatelyam-ustanavlivat-vremennuyu-avatarku.html) – 2015. – 17.09).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Представительство компании, государственной структуры или медиа в социальных сетях – уже давно необходимость, а не прихоть. Это самый быстрый способ узнать, что подписчики думают о вашей работе, рассказать о новостях и просто поддержать контакт. В то же время социальные сети – бесплатный инструмент пиара, работа с которым может обернуться катастрофой, если допустить пару ошибок при работе с негативом (http://ain.ua/2015/09/14/603549).

От негатива застраховаться невозможно. Даже безобидный пост о новинках компании может вызвать бурю возмущения среди подписчиков из-за мелочи, которую вы сами не углядели. Еще большую бурю возмущения может вызвать отсутствие реакции на событие в офлайне. Мы решили собрать пять советов по отработке негатива в социальных сетях, основанные на живых примерах из украинской блогосферы.

1. Отвечайте быстро

Социальные сети – это, в первую очередь, инструмент быстрой коммуникации. Чтобы прокомментировать ситуацию – не нужно вызванивать журналистов, писать обширные пресс-релизы или искать выходы на профильные медиа. Если вы видите, что поднимается волна негатива – напишите пост с с пояснениями.

За примерами далеко ходить не надо – один из самых популярных политиков в украинском Facebook – одесский губернатор М. Саакашвили – регулярно отрабатывает негатив на своей странице. На прошлой неделе, после форума YES, по Facebook начала распространятся фотография М. Саакашвили в обнимку с бывшим Президентом Украины Л. Кучмой. Пользователи резко осудили М. Саакашвили за проявление теплых эмоций по отношению к экс-президенту.

Уже на следующий день М. Саакашвили опубликовал пост, суть которого сводилась к тому, что несмотря на недостатки Л. Кучмы, он предоставил Грузии военную помощь во время конфликта с Россией, тогда, когда другие президенты отказались это делать. Оценивать политическую подоплеку можно по-разному, но по скорости и содержанию негатив отработан. Результат – около 10 тыс. лайков под постом и волна публикаций в СМИ с цитированием поста.

2. Извинитесь и признайтесь в своей неправоте

Ахиллесова пята коммуникационной стратегии – противоречие извечному принципу «Клиент всегда прав». Даже в ситуации, когда вам кажется, что клиент перегибает палку или же далек от правды – нельзя ему хамить, обвинять и рассказывать о собственных проблемах. Если речь идет об откровенном троллинге или нарочитой клевете – лучше перевести проблему в

правовое поле или же обратиться к клевещущим в личных сообщениях, но не «срываться» публично.

Пример категорически неправильного поведения и грамотного выхода из ситуации одновременно – конфликт вокруг твиттера Министерства культуры Украины.

В ответ на замечание пользователя SMM-менеджер Twitter-аккаунта огрызнулся, вместо того, чтобы исправить ошибку. Это вызвало сейсмическую реакцию в украинском твиттер-сообществе и последующее закрытие твиттера министерства. Спустя пару дней SMM-менеджера отстранили и назначили другую, которая одним твитом вернула репутацию аккаунта и позволила за один день добрать около 500 новых подписчиков.

3. Не блокируйте своих подписчиков

Банить своих собственных подписчиков можно разве что в исключительных случаях, когда читатель наносит ощутимый вред жизнедеятельности бренда. Например, когда оставляет однотипные комментарии под всеми постами или публикует откровенно оскорбительные или отвратительные изображения. В остальных случаях блокировка пользователей приведет скорее к ударам по репутации, нежели к положительным результатам.

Данная практика в ходу у украинских политиков. Многие из них держат комментарии открытыми до того момента, пока не возникает первый резонансный конфликт. В результате львиная доля несогласных с решением политика блокируется. Результат – потеря доверия у избирателей, ради которых и ведутся страницы в соцсетях.

То же касается брендов. Если вам есть что ответить на критику – ответьте. Если нет – уж лучше просто промолчать.

4. Помните, что сотрудники олицетворяют собой бренд

Нельзя забывать, что сотрудники компании ассоциируются с брендом. Даже если они пишут в нерабочее время, неаккуратное высказывание могут воспринять как позицию компании. Особенно, если этот сотрудник – директор или основатель.

Еще раз повторимся про «клиент всегда прав». Если вы решили разобраться с несогласным у него на стене, отвечая из личного аккаунта – негатив все равно свяжут с брендом.

Основатель небольшого магазина HIVER BOOKS не так давно пришел в комментарии к негативному отзыву о работе магазина на стене Игоря Стефурака, украинского блогера, популярного в IT-сообществе. В результате, вместо того, чтобы обелить репутацию бренда, он загнал ее в еще худшее положение. Вместо этого, стоило лишь извиниться и пообещать внедрение необходимых клиенту функций.

5. Поощряйте пользователей

Сгладить конфликт можно, предоставив недовольному клиенту извинения и поощрение. Главное – не переборщить, дабы другие пользователи не подумали, что лучший способ получить скидку – это раскритиковать вашу

продукцию или услуги. Отработку негатива такого рода лучше производить не публично.

Поощряйте пользователей за позитив. Проведите мониторинг положительных отзывов и предложите авторам бонусы/скидки/бесплатные товары. Поощрять за позитив можно прямо в комментариях. Таким образом, вы повысите уровень лояльности к бренду и продемонстрируете уровень своей открытости и прогрессивности.

К примеру, после положительного отзыва с фотографией трех рюкзаков, основатель бренда GUD в комментариях предоставил их владельцам 20 % скидку на последующую покупку. Результат – повышение лояльности и намек другим пользователям, как можно заработать скидку и для себя ***(5 советов по отработке негатива в соцсетях на украинских примерах // AIN.UA (http://ain.ua/2015/09/14/603549). – 2015. – 14.09).***

***

Ця історія не є унікальною. Чимало шкіл у різних містах і селах України мають представництва в соцмережах, є окремі групи, які створюють класні керівники у Viber чи інших сервісах. Але представництва, які створює і сам же наповнює директор – не таке вже й поширене явище.

С. Горбачов – відома багатьом київським, і не тільки, журналістам людина. Він тривалий час працював у медіа, був лектором програм нових медіа в «Інтерньюз-Україна», директором інформаційного центру газети «КоммерсантЪ-Украина». Хоча до медіа-роботи, у 90-х, мав майже 15-річний досвід в освіті.

Цього року С. Горбачов вирішив повернутись до освіти і погодився очолити спеціалізовану школу №148 у м. Київ. Новий директор вирішив осучаснити методи взаємодії зі школярами та їхніми батьками – і завів представництва школи в соцмережах, які сам же й наповнює. Він залишив у відкритому доступі – на дошці оголошень школи свій приватний імейл та скайп – щоб при потребі батьки могли задати йому питання чи уточнити моменти, які їм не зрозумілі. При цьому С. Горбачов обіцяє, що незабаром дасть можливість наповнювати шкільні екаунти й самим школярам. Щоправда, на початку з премодерацією – щоб помилки не виставляли – пояснює він, – а потім повний доступ за репутацією.

Щодо закидів створення представництва школи й у російській соцмережі «ВКонтакте», С. Горбачов пояснює, що й самому не дуже це подобається, але «світ не такий ідеальний, як хотілося б бачити, і я маю бути там, де наші діти, більшість з них зараз у “ВКонтакте”. А у Facebook можна тільки з 13 років».

В акаунтах розміщується інформація, яка може бути цікавою як для учнів, так і батьків. Наприклад, фінансовий звіт про надходження та використання благодійних внесків батьків на підтримку освітньої діяльності школи протягом минулого навчального року ***(Директор київської школи створив представництва закладу в соцмережах і сам же їх наповнює // UkrainianWatcher (http://watcher.com.ua/2015/09/14/dyrektor-kyyivskoyi-shkoly-***

stvoryv-predstavnytstva-zakladu-v-sotsmerezhah-i-sam-zhe-yih-napovnyuye/). – 2015. – 14.09).

***

Згідно з рейтингом, складеним виданням Watcher, в українському сегменті соцмережі найбільшою популярністю користуються політики. Разом з А. Аваковим до п'ятірки потрапили нардепи Д. Тимчук, С. Семенченко, М. Найєм та О. Ляшко.

Зауважимо, що в десятці також немає нікого, крім представників української політики ***(Аваков найпопулярніший в українському Facebook // Радіо24 (http://radio24.ua/news/showSingleNews.do?objectId=40388). – 17.09).***

***

Останнім часом почастішали випадки поширення чиновниками неправдивої та неперевіреної інформації в соцмережах. Експерти вважають, що карати політиків за такі дії неможливо, оскільки діючі закони не мають на увазі відповідальність за інформацію в соцмережах.

Проблема дезінформації стає дедалі гострішою у зв'язку з наближенням місцевих виборів. Експерти зазначають, що останнім часом почастішали випадки поширення неправдивої інформації в соціальних мережах.

Цікаво, що інформація ця виходить від високопоставлених осіб. Почастішали випадки, коли український чиновник публікує якусь новину в себе на сторінці, а на наступний день сам же спростовує її.

Про відповідальність за розголошення інформації в ефірі радіостанції «Голос Столиці» розповів заступник директора інституту інформаційного суспільства Я. Павловський.

Яка нині існує відповідальність за поширення неправдивої інформації з боку чиновників?

– Є загальна відповідальність за поширення неправдивої інформації. Але закон щодо поширення такої інформації в соцмережах, на жаль, не передбачає відповідальності, тому що соцмережі не є ані ЗМІ, ані офіційне джерело, на яке можна було б посилатися.

Чому пости в соцмережах не можна сприймати як ЗМІ?

– Звичайно, що Facebook – це соціальні медіа. Але в будь-якому разі, якщо журналіст перецитовує, або бере інформацію із соцмереж, його потрібно перепровірити.

Якщо чиновник щось пише в соцмережах, чи можна це вважати за офіційну інформацію?

– А. Аваков, якщо говорити про нього, крім того, що він чиновник, він ще і політичний діяч. Відповідно, за поширення неперевіреної, недостовірної або неправдивої інформації він матиме репутаційні ризики, але оцінку мають дати виборці, враховуючи подібні фактори, при голосуванні за ту політичну силу, яку він буде представляти. Я згоден з вами, що діяльність деяких чиновників у соцмережах є дещо більш активною, ніж потребує суспільство, і потрібно було б більш обережно ставитися до таких заяв. Таким чином він намагається набрати політичні очки, але є інший приклад, коли просто розповсюджуються пропагандистські моделі, пропагандистські штампи, і вони, навпаки, орієнтовані на заспокоєння суспільства, що є корисним для суспільства.

Чи варто посилити відповідальність за такі заяви?

– Журналісти вже мають практику використання закону про доступ до публічної інформації, про захист інформації, і ви ж розумієте, що які б норми не закладали в чинну правову базу, є певні складнощі, що не дозволяють вам їх використовувати. Останнім часом дуже активно обговорюють механізм блокування користувачів за поширення неправдивої інформації, або якоїсь, яка не відповідає стандартам роботи Facebook. Це було б показово, наприклад, якби заблокували А. Авакова за поширення неправдивої інформації, це був би прецедент в інформаційному просторі України ***(Соцмережі як інструмент поширення неправдивої інформації політиками // Голос Столиці (http://newsradio.com.ua/2015_09_11/Socmerezh-jak-nstrument-poshirennja-nepravdivo-nformac-pol-tikami-3526/). – 2015. – 11.09).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Компания YouTube продолжает демонстрировать мощный рост в секторе онлайн-видео: согласно данным статистики, ежемесячно на платформе отмечается до 240 млрд просмотров видео. На долю 100 ведущих многоканальных сетей (MCN), сотрудничающих с YouTube, ежемесячно приходится более 100 млрд просмотров. Об этом пишет mediasat.info.

Это ещё одно увеличение среднегодовых показателей, отображающее мощный рост в секторе онлайн-видео по всему миру на фоне продолжающейся нестабильности в секторе традиционных кабельных платформ. В отчёте, подготовленном агентством Ampere Analysis, указывается на то, что 75 % всех этих MCN-сетей принадлежит крупным телевизионным корпорациям.

Среди них – такие компании, как Disney, Discovery и Dreamworks, которым принадлежат MCN-сети на платформе YouTube. Компании Disney принадлежит Maker Studios – известная сеть, которая владеет крупнейшим каналом на YouTube – Let’s Play, под её крылом работает также геймер PewDiePie.

Наличие у телекомпаний каналов на YouTube означает, что падение популярности кабельного телевидения не станет для них слишком грандиозной потерей, в особенности, если данные телекомпании продолжат активно инвестировать в YouTube. Компания Disney уже вложила 500 млн дол. и, в общем-то, готова продолжать инвестировать.

Собственный канал геймера PewDiePie принёс в 2015 г. доход в размере 7,4 млн дол., что представляет рост в более чем 2,27 млрд дол. в сравнении с показателями прошлого года. Канал получает доход от видео- и баннерной рекламы, которую YouTube показывает на всех каналах, позволяющих это делать.

На фоне данного роста YouTube, компания Google планирует провести ряд масштабных изменений, касающихся способа монетизации ресурса. Проект YouTube Music Key, стоимость месячной подписки на который составляет 7,99 дол., представляющий службу с потоковой музыкой, является одним из таких новых способов монетизации. Он должен привлечь внимание пользователей, которые часто обращаются к каналам с музыкальным видео.

Существуют также планы, предусматривающие введение подписки для пользователей каналов на YouTube, позволяющий им, заплатив определённую сумму, отключать надоедливую рекламу, а также получить доступ к просмотру дополнительных материалов, отображающих то, что происходило за кулисами съёмок и т. д. Это не первый случай попытки платформы запустить платные каналы, однако, похоже, это наиболее мудрый способ сделать такой шаг.

По-видимому, для YouTube ещё не настали те времена, когда можно смело говорить о прибыльности службы, даже несмотря на все эти огромные цифры. Стоимость использования серверов Google по-прежнему велика, и, в немалой степени, это связано с тем огромным количеством контента, который на них ежедневно загружается и с них воспроизводится.

Доля платформы YouTube на рынке в настоящее время уменьшается, по мере того, как в конкурентную борьбу включаются Netflix, Facebook и т. д. ***(YouTube берёт новую высоту: 240 миллиардов просмотров видео в месяц // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44577/118/lang,ru/). – 2015. – 8.09).***

***

Основатель Википедии Д. Уэлс заявил, что ресурс не является коррупционным. По его словам, обнаружение отдельных случаев, когда пользователи брали плату за публикации, лишь служит доказательством хорошей работы сайта в сфере безопасности. Об этом сообщает lenta.ru со ссылкой на The Guardian.

«Из некоторых сообщений могло показаться, что в нашем сообществе (Википедии. – Прим. «Ленты.ру») есть коррупция, но это довольно примитивный способ смотреть на ситуацию, – заявил Д. Уэлс. – На самом деле это неверно». По словам Д. Уэлса, из всех удаленных аккаунтов, вероятно,

«всего один или два» не были ботами. Он добавил, что расследовавшие инцидент ни разу не столкнулись с электронными письмами, в которых отправители притворялись бы администраторами ресурса или утверждали, что у них есть полномочия, которых на самом деле нет.

Те, кто платил за то, чтобы страницы о них редактировали, по словам Д. Уэлса, скорее жертвы, чем нарушители. «Их заставили ошибочно думать, что только так (заплатив. – Прим. «Ленты.ру») можно получить страницу в “Википедии”», – пояснил основатель ресурса. Считать, что платить за публикацию любого контента онлайн – это нормально, бизнесменов научил современный маркетинг, отметил Д. Уэлс.

В начале сентября отвечающая за содержание Википедии Wikimedia Foundation сообщила о блокировке 381 аккаунта за исправления, которые, по мнению ресурса, вносились в статьи из финансовой заинтересованности. Основными заказчиками правок были отдельные предприниматели, компании и публичные персоны. Нарушение, которое совершили владельцы заблокированных аккаунтов, квалифицируется как «скрытая оплачиваемая защита чужих интересов» (undisclosed paid advocacy) и противоречит внутренним правилам ресурса ***(Основатель «Википедии» опроверг сообщения о коррупции на ресурсе // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44576/118/lang,ru/). – 2015. – 8.09).***

***

9 сентября утром Instagram объявил о запуске рекламных постов сразу в 30 странах, включая Испанию, Италию, Мексику, Южную Корею и т. д. Запуск во всем мире, в том числе в Украине, запланирован на 30 сентября. Аналитики прогнозируют, что новый формат уже к 2017 г. сможет принести Facebook 3 млрд дол. прибыли (http://ain.ua/2015/09/09/602655).

Ранее Instagram тестировал разные форматы рекламных объявлений и убедился в их эффективности. Согласно данным компании, 97 % тестовых рекламных кампаний достигли своих целей. Теперь рекламные компании будут доступны брендам в 30 странах мира. Ранее, реклама была доступна лишь в США, Канаде, Великобритании, Японии, Австралии, Германии, Франции и Бразилии.

Новый рекламный формат будет включать в себя не только размещения «спонсорских постов» в лентах пользователей, но и дополнительные опции под этими постами – например, кнопки «купить» или «установить», ведущие по соответствующим ссылкам.

Список нововведений, помимо рекламных постов, включает:

Запуск приложения Marquee, созданного для разработки и ведения краткосрочных рекламных кампаний. В основном, данный инструмент пригодится для рекламы новых фильмов или продуктов.

Рекламные кампании в Instagram можно будет синхронизировать с Facebook.

Длительность видео в Instagram увеличилась вдвое и теперь составляет 30 секунд.

Аналитики уже успели назвать Instagram новым «золотым яйцом» Facebook, купленным за 1 млрд дол. Согласно исследовательской компании eMarketer, к концу 2016 г. выручка Instagram от рекламы достигнет 1,5 млрд дол., а к 2017 – 2,8 млрд дол. Количество пользователей Instagram на сегодняшний день насчитывает около 300 млн пользователей ***(Instagram запускает рекламные фото в ленты пользователей // AIN.UA (http://ain.ua/2015/09/09/602655). – 2015. – 9.09).***

***

Социальная сеть начинает тестирование нового сервиса, благодаря которому администраторы групп и публичных страниц получат возможность создавать витрины товаров. В настройках сообщества администратор сможет включить новый раздел «Товары», добавить описание магазина, указать регионы доставки и контактное лицо. После этого руководители сообщества смогут создавать карточки товаров и объединять их в подборки. У посетителей страниц появится возможность просматривать подборки и карточки товаров, комментировать и делиться ими, ставить отметки «Мне нравится», а также связываться с продавцом для уточнения деталей и совершения покупки. «В последние несколько лет мы наблюдаем бурное развитие электронной коммерции. Всё больше пользователей совершают покупки в интернете, в том числе и в социальных сетях, поэтому сегодня мы запускаем тестирование самого востребованного формата – товарной витрины в сообществах. Мы создаём новую платформу, при помощи которой малые и средние магазины смогут получить доступ к многомиллионной аудитории “ВКонтакте”, а тесная социальная интеграция позволит вывести интернет-магазины на новый уровень за счет синергетического эффекта», – считает операционный директор «ВКонтакте» А. Рогозов ***(«ВКонтакте» позволит создавать интернет-магазины // Marketing Media Review (http://mmr.ua/show/vkontakte_pozvolit_sozdavaty_internet-magaziny). – 2015. – 11.09).***

***

Компания Google решила снова удивить всех и до конца года начнет доставлять свежую еду в ряде городов США. Все это в рамках конкуренции с аналогичным сервисом Amazon и стартапом Instacart. Об этом со ссылкой на The Verge сообщает Газета.ру.

Сервис по доставке еды будет запущен в Сан-Франциско, а позже будет опробован еще в одном американском городе, сообщил генеральный директор Google Express Б. Эллиот. Ранее данное подразделение Google уже занималось доставкой ряда товаров, в том числе и долгохранящихся продуктов.

При этом ранее Google объявил о разработке технологии для подсчета калорий по фото еды, а также представил миниатюрные датчики, следящие за

уровнем сахара в крови. В конце июля стало известно, что Google попытался приобрести производителя синтетического мяса Impossible Foods за 200 млн дол., однако компания ответила на данное предложение отказом.

Украинцы стали чаще заказывать еду через Интернет. За последний год средний чек украинца на заказ еды с доставкой возрос на 25 %. Таким образом, если в 2014 г. он составлял 250 грн, то в 2015-м он возрос до 312,5 грн ***(Google планирует заняться доставкой свежей еды // Минфин (http://minfin.com.ua/2015/09/10/8859364/). – 2015. – 10.09).***

***

В китайском мобильном приложении для отправки коротких сообщений WeChat появится сервис, с помощью которого пользователь сможет подать заявку и оформить кредит без залога и гарантий. Об этом сообщает The Wall Street Journal, ссылаясь на источники, близкие к компании.

Новый сервис получит название Weilidai, что в переводе с китайского означает буквально «маленький кредит». У пользователей будет возможность получить до 200 тыс. юаней, или чуть больше 31 тыс. дол. Всю операционную деятельность по выдаче ссуд будет вести WeBank – банк, открытый корпорацией Tencent, которой принадлежит WeChat, в партнерстве с несколькими китайскими финансовыми фирмами. Как передает WSJ, аудиторию мессенджера составляют живущие в больших городах офисные работники со стабильным доходом.

По данным Bloomberg, WeChat является самым стремительно растущим мессенджером на рынке: число его пользователей за последний квартал увеличилось на 37 % и составляет около 600 млн пользователей. WeChat является четвертым по популярности сервисом для отправки сообщений в мире. Для сравнения, у крупнейшего в мире мессенджера QQ (также принадлежит Tencent) 843 млн пользователей, у WhatsApp – 800 млн, а у Facebook Messenger – 700 млн пользователей.

Мессенджеры, в частности WeChat, не обладают таким обширной информацией о пользователях, как социальная сеть, отмечает создатель российского финансового сервиса UBank Ф. Хачатрян. «Им идеально подходит модель микрокредитования, когда очень высокая процентная ставка по кредитам позволяет финансовой организации покрыть потери по невозврату некоторых платежей», – оценил он для «Ленты.ру» перспективы нового сервиса.

В августе Facebook сообщил о том, что планирует предоставлять финансовым организациям информацию о пользователях, которая позволит определить их уровень благонадежности для выдачи кредита. Среди параметров оценки большое число факторов, начиная со списка друзей и мест, которые пользователь часто посещает, и заканчивая информацией, которую он указал в профиле, но решил не обнародовать ***(Китайский мессенджер WeChat начнет выдавать кредиты без залога // InternetUA***

(http://internetua.com/kitaiskii-messendjer-WeChat-nacsnet-vidavat-krediti-bez-zaloga). – 2015. – 13.09).

***

Google запустил платежный сервис Android Pay, который позволит владельцам смартфонов расплачиваться за покупки, прикладывая гаджет к кассе в магазине. Об этом сообщается в официальном блоге разработчиков приложения.

Android Pay заработает на всех устройствах, где активирована функция NFC (near field communication, «ближняя бесконтактная коммуникация»). Сделать покупку с помощью сервиса можно через любой платежный терминал, на котором установлено соответствующее программное обеспечение. Компания открыла доступ к интерфейсу для разработчиков, чтобы увеличить число платежных терминалов и даже торговых автоматов, где можно будет расплатиться, используя Android Pay. В случае утраты телефона пользователь заблокирует устройство или удалит всю хранящуюся на нем личную информацию дистанционно.

Сервис запустят в США, где подтверждено сотрудничество с крупнейшими национальными банками. Android Pay заменит электронный кошелек Google Wallet, а карты постоянного покупателя и скидки, хранившиеся в приложении, автоматически перейдут в новый продукт. В феврале Google приобрел занимающийся мобильными платежами стартап Softcard, компетенции разработчиков которого должны были помочь поисковику улучшить Wallet.

Свой платежный сервис есть у Samsung, но пока расплачиваться за покупки с его помощью можно лишь с последних моделей смартфонов и только в Южной Корее. В 2014 г. собственный сервис для оплаты с помощью смартфона запустила Apple, однако на сегодняшний день сервис Apple Pay доступен только жителям США и Великобритании. Он поддерживает оплату с iPhone 6 и 6 Plus без использования NFC-терминалов. ***(Google запустил бесконтактную платежную систему // InternetUA (http://internetua.com/Google-zapustil-beskontaktnuua-platejnuua-sistemu). – 2015. – 12.09).***

***

Стартап Stripe представил новый продукт под названием Relay, благодаря которому ритейлеры смогут продавать свои продукты в рамках сторонних приложений, который используют Stripe, включая и Twitter. Ранее разработчикам приходилось направлять пользователей на вебсайт или отдельное приложение, чтобы завершить транзакцию, но Relay позволяет совершить покупки в рамках того же приложения. Стартап был основан в 2010 г. братьями Патриком и Джоном Коллисонами и оценивается в 5 млрд. Ритейлер Warby Parker и коробочный сервис FabFitFun уже продемонстрировали кнопку в своем Twitter. Ранее о тестировании кнопки

«Купить» в мобильной рекламе сообщила Google. ***(В Twitter появится больше кнопок «Купить» (Marketing Media Review (http://mmr.ua/show/v_twitter_poyavitsya_bolyshe_knopok_kupity_). – 2015. – 15.09).***

***

Компанию Google обвинили в злоупотреблении своим положением на рынке России, что грозит штрафом.

Об этом сообщили в российской Федеральной антимонопольной службе (ФАС), сообщает УНН со ссылкой на РИА «Новости».

В антимонопольном ведомстве заявили, что Google нарушил закон, устанавливая некоторые приложения на мобильные устройства. Нарушение грозит компании штрафом в размере до 15 % выручки за 2014 г. в этом сегменте российского рынка.

ФАС не назвала сумму выручки компании, сославшись на коммерческую тайну и отметив, что точный размер штрафа будет определен после 28 сентября. Google должен будет заплатить штраф и устранить нарушения под угрозой новых штрафов.

В представительстве Google в России заявили, что изучат решение ФАС, а пока комментировать его не будут.

После решения ФАС акции «Яндекса» выросли. В компании, которая подала жалобу на Google в феврале, приветствовали решение регулятора ***(Россия оштрафует Google за «антимонопольные нарушения» // DailyUA (http://daily.com.ua/world/15-09-2015219902). – 2015. – 15.09).***

***

Об этом социальная сеть сообщила в своем блоге. Новый рекламный формат позволит таргетировать аудиторию за пределами сообществ, благодаря системам rb.mail.ru и MyTarget. «Промопосты позволяют увеличить охват публикаций группы с детальным таргетингом на целевую аудиторию. При этом рекламодатель получает виральный эффект от поста бесплатно. В ленте пользователя, не подписанного на сообщество, пост будет отображаться с кнопкой “Подписаться”, что дополнительно принесет новых подписчиков сообществу», – прокомментировал С. Боярский, менеджер по развитию бизнеса проекта «Одноклассники». Платные посты во «ВКонтакте» появились еще этой весной. ***(В «Одноклассниках» появились промопосты // Marketing Media Review (http://mmr.ua/show/v_odnoklassnikah_poyavilisy_promoposty_). – 2015. – 16.09).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Подросткам кажется, будто они обязаны постоянно находиться онлайн и отвечать на сообщения. Такое давление может привести к тревоге, депрессии и снизить качество сна. Ученые из Университета Глазго опросили 467 подростков. Участники рассказали, как часто они использовали соцсети.

Кроме того, добровольцы выполнили тесты на качество сна, самооценку, тревогу и депрессию. Также исследователи оценили эмоциональную вовлеченность участников. Например, у добровольцев узнали, что они чувствовали, если не могли сразу же ответить на сообщения в социальной сети, информирует news.eizvestia.com (http://news.eizvestia.com/news_technology/full/853-socialnye-seti-opasny-dlya-psihiki-podrostkov).

Анализ показал: использование соцсетей и эмоциональная вовлеченность были связаны с низким качеством сна, сниженной самооценкой, высокими уровнями тревоги и депрессии. Особенно страдали те подростки, которые сидели в социальных сетях ночью. Кстати, согласно данным другого исследования, если подросток проводит в день более двух часов в Facebook, Twitter или Instagram, у него повышается риск умственных проблем, психологического дистресса и даже суицидальных наклонностей ***(Социальные сети опасны для психики подростков // Экономические известия (http://news.eizvestia.com/news_technology/full/853-socialnye-seti-opasny-dlya-psihiki-podrostkov). – 2015. – 14.09).***

***

Психологи из США провели анкетирование подростков, которые отвечали на ряд вопросов. В частности, по полученным ответам психологи смогли оценить самооценку, качество сна, уровень тревожности и склонность к депрессии. Также подростки отвечали, сколько времени (и в какое время суток) они проводят в соцсетях.

Оказалось, что, чем больше подросток проводит времени в социальных сетях, тем больше он склонен к депрессии и тревожности, к тому же часто имеет проблемы со сном.

Особенно опасная ситуация у тех подростков, которые «висят» в социальных сетях по ночам, и проводят в своих аккаунтах по несколько часов в сутки. В частности, многие подростки переживают по поводу «лайков» и комментариев, а также стремятся постоянно быть онлайн, чтобы «не обидеть» друзей. Сами соцсети не представляют собой ничего плохого, отмечают психологи, однако чувствительные личности могут попасть в зависимость от

данного средства коммуникации, а в случае с подростками эта зависимость может быть слишком сильной и формировать их самооценку ***(Почему социальные сети опасны для подростков // Healthy Living (http://healthyliving.com.ua/ru/zdorove/novosti/4487-pochemu-sotsialnye-seti-opasny-dlja-podrostkov). – 2015. – 12.09).***

***

Ученые из Университета Окленда установили: женщины в возрасте 35–45 лет, активно пользующиеся социальной сетью Facebook, часто не удовлетворены своим внешним видом, передает издание Supreme2.ru.

Всего в исследовании приняли участие 11 тыс. человек, средний возраст составил 39 лет. 58 % опрошенных женщин заходили на Facebook хотя бы один раз в неделю.

Неудовлетворенность своей внешностью у женщин снижалась в 30 лет, к 35 нарастала, а в 38 лет достигала максимума.

Особенно критично к себе относили активные пользователи Facebook. Мужчины же уделяли вопросам красоты значительно меньше времени.

Однако и в этом случае активные пользователи социальных сетей оказались более критичны к себе, чем мужчины, которые совсем не пользуются Facebook ***(Социальные сети заставляют женщин переживать из-за своей внешности // S2 (http://supreme2.ru/20855-socialnye-seti-zastaaaavlyayut-zhenshhin-perezhivat-iz-za-svoej-vneshnosti/). – 2015. – 13.09).***

Маніпулятивні технології

Польська журналістка, репортерка видання Tygodnik powszechny М. Андрушевська, яка робить репортажі з зони АТО в Україні, заявляє про погрози на її адресу з боку невідомих користувачів соціальної мережі Facebook. Про це повідомляє Інститут масової інформації з посиланням на саму журналістку.

«Недавно знову мені писали нахальні молодики. Я хотіла когось запросити на каву, але на жаль ніхто з них не використовує справжній профіль. Більше того, мають тенденцію швидко ці профілі ліквідувати, не даючи мені шансів довше поговорити. Маю враження, що молодики особливо активізуються, коли я перебуваю в АТО. Їх є багато, всі скорше за все дуже молоді, жоден не грішить розумом чи орфографією», – написала вона у своєму Facebook.

У коментарі ІМІ М. Андрушевська зазначила, що «ми вже до того звикли». За її словами, таких коментаторів є багато, вона вважає, що їх залишають троллі. «Це наша ціна за те, що ми підтримуємо Україну», – сказала вона.

Також вона вважає, що частина цих коментаторів є російськими (або оплачуваними Кремлем), оскільки їхні повідомлення скоріше за все перекладені Google-перекладачем.

Восени минулого року на одному з варшавських кладовищ невідомі створили імпровізовану могилу польського журналіста Д. Вільдштейна. Його ім'я було написане на дошці з зіркою Давида, на якому написано: «Давид Вільдштейн, він жив 30 років, помер. 13 XII 2014 в Краматорську». Журналіст поскаржився до прокуратури.

Як повідомляла «Телекритика», 27 липня польська журналістка Б. Залевська отримала тяжкі травми в зоні проведення АТО на Донбасі, серед яких вогнепальне поранення та перелом хребта. Їй зробили операцію на ключиці в харківський лікарні, а потім відправили літаком на лікування до Варшави. З Польщі вона готувала сюжети для телеканалу «Еспресо TV», а також заявляла, що планує повернутися працювати в Україну.

1 грудня польську журналістку Б. Залевську Президент України П. Порошенко нагородив орденом княгині Ольги III ступеня.

Співголова так званого «Народного фронту Новоросії», один з лідерів так званого «Харківського опору» К. Долгов заявив, що польська журналістка Б. Залевська є бійцем батальйону «Айдар» і начебто причетна до військоих злочинів. Він стверджує, що громадянка Польщі є не журналісткою, а снайпером добровольчого батальйону «Айдар» і «брала безпосередню участь у тортурах і знущаннях над полоненими ополченцями» в місті Щастя (Луганська область). Він погрожує докласти всіх зусиль, аби покарати журналістку. Доказом того, що Б. Залевська є снайпером, на думку К. Долгова, може слугувате те, що польська журналістка була одягнута в камуфляж, і те, що її начебто упізнав якийсь невідомий чоловік з Луганщини, прізвище якого він не наводить.

Телеканал «Еспресо.TV» поки ніяк не зреагував на погрози журналістці з боку сепаратистів ***(Польській журналістці, що працює в зоні АТО, погрожують розправою у Facebook // Телекритика (http://www.telekritika.ua/profesija/2015-09-07/110918). – 2015. – 7.09).***

***

Невідомими в соціальній мережі Twitter було створено фейкову сторінку Національної гвардії України – NatsGvardiya. Про це УНН повідомили в прес-службі НГУ.

«Зміст матеріалів на цій сторінці не відповідає дійсності. У зв'язку з цим просимо утриматися від розповсюдження і посилання на матеріали, які розміщуються на ній», – ідеться в повідомленні.

У прес-службі закликали отримувати достовірну інформацію з офіційного сайту НГУ ***(Шрамко Ю. Невідомі створили фейкову сторінку Нацгвардії в Twitter // Українські Національні Новини (http://www.unn.com.ua/uk/news/1498363-u-natsgvardiyi-zayavili-pro-feykovu-storinku-vidomstva-u-twitter). – 2015. – 7.09).***

***

Останнім часом у мережі з'являється багато неправдивої інформації про львівських поліцейських. Зокрема, зловмисники підробляють фотографії, де нібито поліцейські вчиняють некоректні дії. Про це повідомляє патрульна поліція Львівщини на своїй сторінці у Facebook, передає кореспондент Львівського порталу.

«Нещодавно у мережі з'явилася фотографія, на якій нібито патрульні поліцейські розливають дизпаливо у пластикові пляшки. Так от, це – не ми», – заявляють «копи» і в підтвердження публікують фото з такими позначками:

1. у працівників патрульної поліції кепки не мають ніяких лейбів у районі застібки (якщо наблизити оригінальне фото, там є світлий фрагмент);

2. на автомобілях патрульної поліції з боків немає синьо-жовтої смужки (на оригінальному фото вони є);

3. щодо багажника, в автомобілях патрульної поліції обов'язково є бронежилети і червона аптечка, на провокативному фото їх немає;

4. на задніх дверях на сонці мало б віддзеркалюватись слово "поліція";

5. на задніх дверях має бути видно малюнок, тут його взагалі немає;

6-7. будівля з червоної цегли і червоним дахом, а також багатоповерхівка позаду знайшлись в Обухові, поруч із заправкою WOG, де й було зроблене фото. Переконайтесь самі: goo.gl/taL4j0

«Патрульна поліція наразі є лише в Києві, Одесі та Львові. Ми фізично не могли там бути, бо це місто поза нашою компетенцією та й всі патрульні машини оснащено GPS-передавачами, які ми цілодобово відстежуємо», – стверджують поліцейські. ***(Львівських поліцейських підставляють фейками // Львівський портал (http://portal.lviv.ua/news/2015/09/10/lvivskih-politseyskih-pidstavlyayut-feykami). – 2015. –10.09).***

***

У терористичній «ДНР» – свої закони та способи заробляння грошей. Місцеві жителі займаються навіть інтернет-тролінгом, маючи на цьому непогані прибутки. Зокрема, писати треба антиукраїнські коментарі в соцмережах. Зароблені кошти такі «працівники» отримують на російські банківські карточки, а знімають їх у банкоматах Ростова.

Про це сепаратистському виданню «Афиша Новороссии» розповів 25-річний блогер із «ДНР» Іван.

Подаємо текст мовою оригіналу:

«Если у тебя хорошие "прокачанные" аккаунты в социальных сетях, на них можно неплохо заработать. Не буду здесь называть конкретные адреса, но есть несколько бирж в Сети, где можно регулярно получать заказы на рекламные посты в Твиттере и ВКонтакте. Обычно цена поста – от 2 до 7 рублей.

Я зарабатываю около 500–600 рублей в день. У меня есть старый аккаунт с более чем десятью тысячами подписчиков и четыре "украинских" аккаунта, которые "топят" за Правый сектор и Яроша против Порошенко. Какие-то люди

из Одессы щедро платят за такие посты. Мне наплевать – пусть они там все друг другу глотки перегрызут, поскорей бы.

Деньги вывожу обычно через Яндекс.кошелек и российские карты. У меня есть карта российского Альфа-банка, раз в полтора месяца я выезжаю в Ростов и вывожу деньги без процента. Это не основная моя работа, я занимаю должность в одной государственной структуре ДНР, использую только свободное время для дополнительного заработка. В месяц выходит более тридцати тысяч» ***(У «ДНР» антиукраїнським інтернет-тролям платять до 600 російських рублів на день, – блогер // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/09/17/u_dnr_antyukrainskym_internettrolyam_platyat_do_600_rosiyskyh_rubliv_na_den__bloger_625276). – 2015. – 17.09).***

Зарубіжні спецслужби і технології «соціального контролю»

Google, Apple і Microsoft відмовилися відкрити доступ до повідомлень користувачів.

Про це повідомляє Еспресо.TV із посиланням на статтю New York Times.

Раніше влада США неодноразово зверталися із запитами до корпорації для надання доступу до приватних даних.

Останній подібний запит був влітку 2015 р.: Мін'юст США зажадав у Apple надати повідомлення підозрюваних у поширенні наркотиків і зброї. Корпорація відмовилася, пославшись на шифровку інформації в iMessage.

Співрозмовники видання вважають, що подібна скритність корпорацій пов'язана з вчинком Е. Сноудена. Тепер все більше компаній намагається убезпечити інформацію своїх клієнтів ***(Google, Apple і Microsoft відмовились показувати владі США повідомлення користувачів // Espreso.tv (http://espreso.tv/news/2015/09/08/google_apple_i_microsoft_vidmovylys_pokazuvaty_vladi_ssha_povidomlennya_korystuvachiv). – 2015. – 8.09).***

***

На Черкащині співробітники Служби безпеки України затримали місцевого жителя, який вів сепаратистську пропаганду через соціальні мережі.

Тимчасово безробітний зловмисник був активним учасником груп в одній із соціальних мереж російського походження. Там він розповсюджував матеріали антиукраїнського змісту із закликами до насильницької зміни конституційної влади та дискредитації процесу мобілізації. Пропагував насильницькі методи політичної боротьби.

Також затриманий надавав терористам так званих «ДНР/ЛНР» відомості про військовослужбовців Збройних сил України, командирів, представників добровольчих батальйонів, волонтерів. Правоохоронці вилучили у зловмисника комп'ютерну техніку, флеш-носії з антиукраїнськими агітаційними матеріалами.

Правопорушник затриманий та перебуває в слідчому ізоляторі. Йому оголошено про підозру за ч. 1 ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України, інформують у прес-центрі Служби безпеки України ***(На Черкащині СБУ затримала пропагандиста сепаратизму // InternetUA (http://internetua.com/na-cerkasxin--sbu-zatrimala-propagandista-separatizmu). – 2015. – 11.09).***

***

Російський Центральний науково-дослідний інститут економіки, інформатики та систем управління може в односторонньому порядку розірвати контракт із МВС РФ щодо ідентифікації користувачів мережі Tor.

Ідентифікувати користувачів мережі Tor виявилося складніше, ніж уявлялося.

Інститут, який входить в Об'єднану приладобудівну корпорацію «Ростех», уклав контракт на 10 млн р. з юридичною фірмою «Плешаков, Ушкалов і партнери». Як випливає з інформації, розміщеної на сайті держзакупівель, юристи знадобилися організації для «підготовки правової позиції щодо порядку розірвання» чотирьох держконтрактів між інститутом і структурою МВС Росії «Спеціальна техніка і зв'язок», повідомляє видання «Коммерсант».

За інформацією видання, один із чотирьох згаданих контрактів передбачав дослідження можливості отримати інформацію про користувачів анонімної мережі Tor та їхнього обладнання. Ще один контракт передбачав «створення апаратно-програмного комплексу з проведення негласного і прихованого віддаленого доступу до оперативно значимої інформації на цільовій електронно-обчислювальній машині».

Як відомо, за допомогою системи проксі-серверів Tor і відповідного програмного забезпечення користувачі можуть зберігати анонімність в Інтернеті при відвідуванні сайтів, публікації матеріалів, відправці повідомлень і при роботі з іншими додатками ***(В МВС Росії не змогли зламати мережу Tor // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/09/09/v_mvs_rosii_ne_zmogly_zlamaty_merezhu_tor_622950). – 2015. – 9.09).***

***

Роскомнадзор внес видеосервис Yahoo! в реестр запрещенных сайтов, рассказал vedomosti.ru представитель ведомства В. Ампелонский. Это было сделано по представлению Генпрокуратуры, которая обнаружила на одной из страниц сервиса экстремистский материал – видео об «Исламском государстве».

По данным ресурса «Роскомсвобода», некоторые операторы уже начали закрывать доступ к Yahoo! в России: многие пользователи жалуются на то, что не могут зайти и на другие сервисы Yahoo!, например в фотосервис Flickr.

Представитель Yahoo! пока не ответил на запрос «Ведомостей».

Обычно Роскомнадзор вносит в реестр только те страницы, на которых размещен запрещенный контент. Но в данном случае в черный список попал весь видеосервис Yahoo!, который располагается на домене screen.yahoo.com. По словам В. Ампелонского, это было сделано потому, что Yahoo! использует технологию шифрования трафика https, а это не позволяет операторам закрывать доступ к отдельным страницам сайта – только к сайту целиком.

В. Ампелонский говорит, что у российских пользователей будут сложности с доступом не только к видеосервису Yahoo!, но и ко всем сервисам, располагающимся на доменах третьего уровня. Все они, по его словам, располагаются на одном IP-адресе.

Похожая история недавно произошла с «Википедией», заблокировать которую за размещение статьи о производстве наркотика «чарас» пытался Роскомнадзор. Ведомство внесло сервис в реестр и сообщило, что из-за использования технологии https пользователям рунета будет недоступен весь сервис. Роскомнадзор предложил «Википедии» удалить с сайта запрещенный контент.

Но «Википедия» заняла принципиальную позицию и не выполнила требование службы, объяснив это тем, что решение об удалении статей в организации не принимается централизованно. «Если государство в лице Роскомнадзора решило заблокировать “Википедию”, то так тому и быть. У нас похожая ситуация в Китае, Сирии, Иране и Саудовской Аравии, – говорил исполнительный директор «Викимедиа» (российское подразделение Wikimedia Foundation, обслуживающей Wikipedia) С. Козловский. – Если государство в лице Роскомнадзора решило заблокировать “Википедию”, то так тому и бать».

Позже «Википедия» перенесла спорную статью на другой адрес, а по указанному в решении суда адресу оставила лишь перечень обозначений слова «чарас» со ссылками на соответствующие статьи энциклопедии. Роскомнадзор сообщил, что «Википедия» выполнила закон, и отменил блокировку ***(Роскомнадзор внес видеосервис Yahoo! в реестр запрещенных сайтов // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44606/118/lang,ru/). – 2015. – 10.09).***

***

У Росії Facebook на деякий час заблокував можливість поширення посилання на публікацію «Нової газети» про зустріч журналіста з батьками затриманого в Україні військового ГРУ О. Александрова.

Про це повідомив автор статті П. Канигін у себе на сторінці у Facebook.

За його словами, «Facebook заблокував всі пости, які містять посилання на матеріал про батьків Александрова».

«При спробі заново запостити на стіну відповідь така – небезпечне посилання», – написав журналіст.

Після того як у ЗМІ написали про це, Facebook розблокував матеріал.

В Україні такої проблеми не було, і матеріал легко поширювався в мережі ***(Facebook почав блокувати статті російських журналістів // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/09/10/facebook_pochav_blokuvaty_statti_rosiyskyh_zhurnalistiv_623531). – 2015. – 10.09).***

***

У соціальній мережі Facebook заблокували сторінку глави Луганської обласної військово-цивільної адміністрації (ОВГА) Г. Туки.

Про це Тука повідомив у своєму блозі, передає Еспресо.TV.

«Знову заблокували мій ФБ. На 30 днів. В цей раз – з-за посту, в якому я процитував ідіота-лжепатриота, який закликав кару небесну на мою "кацапсько-жидівську" голову. Вам ніколи не зрозуміти, що любов до Батьківщини починається не з мови спілкування, а з готовності віддати за неї життя. З вас же 99 % ніколи не бували на передку. Вам і не снилося слово "доброволець". А, отримавши повістку, ви моментально знаходите у себе плоскостопість з криворукием і косоокістю. Я вас зневажаю, панове вишиватники!» – написав Г. Тука ***(Facebook заблокував сторінку глави Луганської ОВГА Туки // Espreso.tv (http://espreso.tv/news/2015/09/15/facebook_zablokuvav_storinku_glavy_luganskoyi_ovga_tuky). – 2015. – 15.09).***

***

В России суд приговорил Р. Кашапова к трем годам колонии общего режима за посты в сети «ВКонтакте» об оккупации Крыма.

Р. Кашапова признали виновным в экстремизме, ст. 282 УК (Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства), передает Медиазона.

Осужденный – председатель набережночелнинского отделения Татарского общественного центра (ТОЦ) – обвинял президента РФ Путина в развязывании войны в Украине и писал «ВКонтакте» об оккупации Крыма.

Дело по ст. 282 УК против Р. Кашапова было возбуждено в декабре прошлого года. Активиста обвиняли в создании публикаций, «направленных на возбуждение ненависти или вражды, а также унижения достоинства человека или социальной группы по признакам пола, расы, национальности, языка, происхождения, отношения к религии».

Речь идет о четырех опубликованных на странице общественника материалах с заголовками «Крым и Украина будут свободны от оккупантов», «Вчера Гитлер и Данциг, сегодня Путин и Донецк!», «Где Россия, там слёзы и смерть», «Защитим Украину и весь тюркский мир».

Как пишет Медиазона, автором последнего текста является не сам активист, а его брат-близнец Н. Кашапов, эмигрировавший из России в 2005 г.

Эксперты заключили, что опубликованные на странице Р. Кашапова в соцсети фото и тексты «нацелены на разжигание ненависти между группами,

выделенными по признаку национальности, проживания на территории, отношения к власти».

В суде Р. Кашапов говорил, что своими публикациями желал привлечь внимание общества к происходящим в Украине событиям: «В результате войны на Украине гибнут тысячи людей, с обеих сторон, разрушаются города и деревни. Я неравнодушен к этим событиям. Я тяжело переживаю эти события. Только из Татарстана погибли 10 человек (по официальным данным). Я обвиняю в начале войны на Украине президента России Путина».

Прокуратура требовала приговорить Кашапова к четырем годам лишения свободы ***(За сравнение Путина с Гитлером татарского активиста приговорили к 3 годам тюрьмы // Центр журналистских расследований (http://nikcenter.org/newsItem/20656). – 2015. – 15.09).***

***

В Северной Корее зарубежным дипмиссиям и представительствам международных организаций закрыли доступ к социальной сети Facebook и видеохостингу YouTube.

Соответствующее уведомление им направил государственный провайдер «Звезда», передает ТАСС.

«Сотрудники компании не будут обеспечивать доступ к интернет-ресурсам, содержащим угрожающие и клеветнические сообщения, в том числе выпады и критику в адрес правительственных органов КНДР», – говорится в заявлении. Также иностранцам теперь закрыт доступ в пиринговые сети, работающие по технологии P2P (прямой обмен данными между пользователями в обход централизованных серверов).

В Северной Корее функционирует черный список запрещенных веб-сайтов, а в сентябре 2014 г. зарубежным дипломатам «в интересах безопасности» запретили пользоваться Wi-Fi. Нарушителям грозит крупный штраф, а также конфискация оборудования.

Граждане КНДР не имеют доступа в Интернет – его заменяет национальная компьютерная сеть «Кванмён», в которой можно узнать об успехах Трудовой партии Кореи и ее руководителей. Пользоваться всемирной сетью в республике могут лишь сотрудники иностранных дипмиссий и представительств международных организаций ***(Иностранцам в Северной Корее запретили Facebook и YouTube // Хартии'97 (http://www.charter97.org/ru/news/2015/9/16/169193/). – 2015. – 16.09).***

***

Представители Facebook и правительства Германии заявили о создании рабочей группы, которая займется мониторингом антимигрантских публикаций и проявлений ксенофобии в сети. Об этом сообщает The Wall Street Journal.

Принять подобную меру вынудило давление со стороны немецких правоохранительных органов. Полицию волнует всплеск расистских настроений в связи с массовой миграцией беженцев с Ближнего Востока.

«Идея заключается в том, чтобы находить неприемлемый контент и удалять его как можно скорее», – прокомментировал создание мониторинговой группы министр юстиции Германии Х. Маас (Heiko Maas).

В Facebook также выразили уверенность, что эта мера ускорит обнаружение публикаций и их последующую блокировку. Однако представители компании в очередной раз напомнили, что обратить внимание на неприемлемый контент может любой человек. В социальной сети дополнительно подчеркнули, что действующие правила и без того ограничивают пользователей в публикации материалов, содержащих ненависть.

Наравне с удалением неприемлемого контента специалисты займутся выявлением диверсионных групп. Предполагается, что это поможет предотвратить городские акции протеста, которые ведут к эскалации насилия ***(Facebook удалит антимигрантские публикации // InternetUA (http://internetua.com/Facebook-udalit-antimigrantskie-publikacii). – 2015. – 15.09).***

***

Сервис микроблогов Twitter обвинили в том, что он перехватывает и анализирует прямые сообщения пользователей, тем самым нарушая неприкосновенность личной переписки. Коллективный иск предъявили юристы фирмы Edelson. Об этом сообщает The Wall Street Journal.

«Как только пользователь отправлял личное сообщение, Twitter перехватывал его, читал и в некоторых случаях даже изменял содержимое», – цитирует WSJ текст искового заявления.

В качестве примера заявители приводят замену ссылок, в частности на опубликованные в The New York Times материалы. Twitter изменял вид ссылок, сокращая их через собственный сервис оптимизации, www.t.co. Обычно этим инструментом пользуются, чтобы опубликовать ссылку на интернет-ресурс в стандартном сообщении и уложиться в ограничение в 140 символов. С личных сообщений Twitter снял этот лимит.

Коллективный иск предъявлен фирмой Edelson, которая выступила от лица жителя штата Техас Уилфорда Райни, а также всех граждан США, отправлявших и получавших личные сообщения через Twitter. Сумма компенсации, которую они предполагают получить, составляет 100 дол. за каждый день, в который сервис «шпионил» за своими пользователями.

Официальный представитель компании заявил, что руководство сервиса считает обвинения необоснованными и готово к судебной тяжбе.

Интернет-сервисы регулярно обвиняют в чтении (автоматическом анализе) переписки. Так в 2004 г. калифорнийские губернаторы собирались запретить Google анализировать содержание писем (для последующего таргетирования рекламы), а в 2013 г. попала под подозрение компания Microsoft. Однако интернет-сервисам всегда удается доказать, что они действовали в рамках пользовательского соглашения ***(Twitter обвинили в чтении личных сообщений пользователей // InternetUA***

(http://internetua.com/Twitter-obvinili-v-cstenii-licsnih-soobsxenii-polzovatelei). – 2015. – 16.09).

Проблема захисту даних. DDOS та вірусні атаки

Эксперты датской ИБ-компании CSIS обнаружили новый вариант печально известного банковского трояна Carbanak, который теперь имеет цифровую подпись и использует собственный проприетарный протокол передачи данных.

По данным экспертов «Лаборатории Касперского», Carbanak используется уже в течение нескольких лет. В феврале текущего года ЛК раскрыла подробности о масштабной кампании с использованием этого трояна, стоившей банкам 1 млрд дол. Атака была нацелена непосредственно на финансовые организации, а не на конечных пользователей.

Инфицирование системы начиналось с получения жертвой фишингового письма с вредоносным вложением. После установки Carbanak предоставлял злоумышленникам полный контроль над компьютером, что позволяло им проникать в банковские сети и похищать средства несколькими способами.

Особенностью Carbanak является то, что для заражения системы не имеет значения, на каком программном обеспечении она работает. Даже если ПО уникальное, троян все равно проникает в сети, и хакеру даже не нужно взламывать сервисы банка. Попав в сеть, Carbanak эффективно маскирует вредоносную активность за легитимными действиями.

По словам экспертов CSIS, теперь новый вариант трояна получил несколько уникальных характеристик. Папка, в которую Carbanak инсталлирует себя, а также имя файла являются статическими. Для сокрытия себя вредоносное ПО внедряется в процесс svchost.exe.

Подобно другим похищающим средства вредоносам, Carbanak использует плагины, которые устанавливаются по собственному протоколу, а передача данных осуществляется с жестко закодированного IP-адреса через TCP-порт 443. В ходе исследования эксперты загрузили вредоносные плагины wi.exe и klgconfig.plug.

Обнаруженная на образцах Carbanak цифровая подпись принадлежит Comodo, а сертификат выдан компании в Москве ***(Обнаружен новый вариант банковского трояна Carbanak // InternetUA (http://internetua.com/obnarujen-novii-variant-bankovskogo-troyana-Carbanak). – 2015. – 7.09).***

***

На Львівщині правоохоронці викрили кіберзлочинця-адміністратора сайту, на якому розміщувалися фільми та аудіофайли для скачування. Про це Львівському порталу повідомили в прес-службі ГУМВС України у Львівській області.

Працівники відділу боротьби з кіберзлочинністю ГУМВС України у Львівській області встановили, що один з веб-сайтів надає можливість своїм користувачам незаконно, без дозволу правовласника та в порушення вимог Закону України «Про авторське право і суміжні права» відтворювати і розповсюджувати велику кількість аудіовізуальних творів, у тому числі новинки кінопрокату.

Таким чином були порушені права компаній-членів MPA (Motion PicturesAssociation): Disney, Paramount, Twenties Centuries Fox, Universal Pictures, Sony Pictures, Warner Bros, а також українських компаній-кінодистриб'ютерів: Ukrainian Film Distribution, Кіноманія, Галеон кіно, Гемені, Вольга Україна та Каскад Україна.

«Ми встановили, що вказаний сайт адмініструє 25-річний мешканець одного з міст у Львівській області, якому повідомлено про підозру у скоєнні злочину, передбаченому ч. 3 ст. 176 (порушення авторського права і суміжних прав) КК України», – розповів начальник відділу боротьби з кіберзлочинністю ГУМВС України у Львівській області підполковник міліції О. Кріп.

Санкція статті передбачає покарання у вигляді штрафу від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк від трьох до шести років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого та з конфіскацією та знищенням всіх примірників творів, матеріальних носіїв комп'ютерних програм, баз даних, виконань, фонограм, відеограм, програм мовлення та знарядь і матеріалів, які спеціально використовувались для їх виготовлення.

Під час проведення санкціонованих обшуків правоохоронці вилучили системні блоки, ноутбук та жорсткий диск. Слідство триває, невдовзі суд обере для підозрюваного міру запобіжного заходу ***(Правоохоронці Львівщини спіймали «пірата» крупного масштабу // Львівський портал (http://portal.lviv.ua/news/2015/09/07/pravoohorontsi-lvivshhini-spiymali-pirata). – 2015. – 7.09).***

***

Android-приложение для просмотра контента для взрослых Adult Player незаметно фотографирует пользователя, после чего блокирует смартфон и требует выкуп. Мошенники уповают на чувство стыда, подвергая опасности репутацию человека.

Снимок пользователя делается фронтальной камерой без его ведома. После этого приложение блокирует экран смартфона и запрашивает на разблокировку 500 дол. подобно вирусу типа WinLocker для персональных компьютеров. О подобном поведении рассказали специалисты компании Zscaler.

Zscaler специализируется на компьютерной безопасности, и по ее информации, подобные приложения-вымогатели набирают популярность у мошенников. Такие приложения, которые требуют выкупа у пользователя,

угрожая опубликовать компрометирующую его информацию, получили общее название ransomware.

Главный технический директор Intel Security в Европе Р. Самани отметил, что злоумышленники в данном случае уповают на чувство стыда пользователя, подвергая опасности его репутацию. Зачастую человек готов распрощаться с крупной суммой денег, чтобы избежать распространения нежелательной информации о себе в интернете.

По словам главного разработчика компании Intel Security Р. Самани, такие приложения очень просты в разработке и обходятся дешево. Есть программисты, которые с готовностью пишут подобные программы. Одна из таких групп, за деятельностью которой следила Intel Security, заработала более 75 тыс. дол. за два с половиной месяца.

Приложение Adult Player стало вторым примером подобных Android-приложений, обнаруженных специалистами фирмы Zscaler ***(Хакеры перешли на новый уровень. Теперь они могут шантажировать пользователей // InternetUA (http://internetua.com/hakeri-pereshli-na-novii-uroven--teper-oni-mogut-shantajirovat-polzovatelei). – 2015. – 8.09).***

***

Представители Mozilla обнародовали отчет о взломе багтрекера Bugzilla, согласно которому неизвестным удалось похитить информацию о 185 «непубличных» уязвимостях в браузере Firefox и других продуктах Mozilla. Предположительно, хакеры использовали эти данные для атак на пользователей «Огнелиса».

Согласно официальному FAQ об инциденте, хакеры проникли в систему, получив доступ к некому привилегированному аккаунту и, через него, к закрытым обсуждениям. Расследование компании показало, что один из пользователей, очевидно, использовал один и тот же пароль для Bugzilla и других сайтов. Один из сайтов оказался скомпрометирован, в результате чего пароль попал в руки злоумышленников. Получив доступ к аккаунту Bugzilla, те добрались до информации об уязвимостях в Firefox и других проектах Mozilla.

Несанкционированный доступ к багтрекеру был у хакеров давно. Первый подтвержденный случай неавторизованного доступа датирован сентябрем 2014 г. Некоторые улики указываю на то, что хакеры, возможно, имели доступ к Bugzilla даже дольше – начиная с сентября 2013 г.

Суммарно за это время атакующие получили доступ к 185 уязвимостям. Сто десять из них не относились к проблемам с безопасностью, данные о них не раскрывались, так как были сопряжены с проприетарной информацией. Двадцать две оценивались как проблемы средней тяжести. Пятьдесят три оценивались как критические. Десять багов, из числа критических, долгое время оставались в неисправленном состоянии, в то время, как 43 были своевременно устранены. Что касается десятки, которой могли воспользоваться хакеры:

– 2 бага были устранены в течение менее чем 7 дней

– 5 багов устранили в период от 7–36 дней

– 3 бага оставались неисправленными более 36 дней (131 день, 157 дней и 335 дней).

Теперь представители Mozilla пишут, что злоумышленники, похоже, действительно использовали для атак некоторые из десятка, неисправленных на тот момент, багов. Об одной такой проблеме компания уже рассказывала ранее, в августе 2015 г. Тогда пользователям Firefox угрожала реклама на российских новостных сайтах. Используя дырку в Firefox, малварь переправляла конфиденциальные данные пользователей на предположительно украинский сервер. Конкретно эта уязвимость была закрыта 6 августа 2015 г.

Представители Mozilla сообщают, что упомянутый привилегированный аккаунт закрыт, а к расследованию случившегося привлечены специалисты со стороны – некая компания киберкриминалистов. В последнем релизе Firefox, вышедшем 27 августа 2015 г., все упомянутые уязвимости были успешно исправлены для всех платформ ***(Взломан багтрекер Mozilla, хакеры украли данные о 185 багах // InternetUA (http://internetua.com/vzloman-bagtreker-Mozilla--hakeri-ukrali-dannie-o-185-bagah). – 2015. – 7.09).***

***

По данным французского ИБ-эксперта Kafeine, в наиболее популярный набор эксплоитов Angler добавлены самые последние уязвимости в Adobe Flash. В общей сложности Angler получил поддержку 35 брешей, раскрытых и исправленных в прошлом месяце. Восемь из них связаны с повреждением памяти.

В частности, добавлена уязвимость целочисленного переполнения CVE-2015-5560, позволяющая удаленное выполнение кода. Все бреши затрагивают необновленные версии Adobe Flash. Тем не менее, по словам Kafeine, эксплоит для бреши CVE-2015-5560 не работает на 32-битных системах.

В августе нынешнего года Adobe настоятельно рекомендовала установить обновления. Компания советовала администраторам установить их вручную, если пользователи уже не получают обновления автоматически. Учитывая скорость, с которой злоумышленники добавляют эксплоиты в Angler, Adobe даже сопроводила августовские патчи надписью «panic now!».

Angler является весьма эффективным – по данным Cisco, успешными являются 40 % атак с применением этого набора эксплоитов. Благодаря постоянным обновлениям инструмент пользуется большой популярностью у хакеров. Пользователям, которые всерьез беспокоятся о своей безопасности, стоит задуматься над тем, чтобы отказаться от использования Adobe Flash ***(В Angler добавлены исправленные в прошлом месяце уязвимости в Adobe Flash // InternetUA (http://internetua.com/v-Angler-dobavleni-ispravlennie-v-proshlom-mesyace-uyazvimosti-v-Adobe-Flash). – 2015. – 7.09).***

***

Користувач Facebook Є. Строкін зробив запис у соцмережі про те, що виявив на своїх пристроях з «Яндекс.Навігатором» аудіофайл stream.wav, що містить запис із мікрофону пристрою більше ніж за добу. Запис припинився, коли на пристрої закінчилося місце, що і викликало інтерес користувача, який встановив, що запис вів додаток «Яндекс.Навігатор», пишуть «Ведомости».

Представник «Яндекса» вже підтвердив, що проблема з додатком для Android існувала. За його словами, вона з'явилася 8 вересня після оновлення програми і була виправлена новим оновленням того ж дня. Зараз ніякі дані додаток не записує і не зберігає, а «зайві» файли видалені з пам'яті. Якщо не підключено автооновлення, то потрібно завантажити свіжу версію з Google Play, радить представник «Яндекса» і запевняє, що запис нікуди не відправлявся і доступ до нього мав лишге власник пристрою ***(«Яндекс.Навігатор» записував всі розмови своїх користувачів // UkrainianWatcher (http://watcher.com.ua/2015/09/09/yandeks-navihator-zapysuvav-vsi-rozmovy-svoyih-korystuvachiv/). – 2015. – 9.09).***

***

Хакер windknown опубликовал в блоге разработчиков джейлбрейка Pangu заметку, в которой рассказано о трех уязвимостях, обнаруженных им в iOS 8.4.1.

Обычно хакеры помалкивают о подобном и втихаря используют найденные уязвимости, однако windknown подробно расписал их. Одна из уязвимостей, к примеру, позволяет запускать сторонний код в ядре операционной системы, что может быть очень опасно.

Две из трех уязвимостей уже закрыты в бета-версиях iOS 9, а последняя, вероятно, будет локализована специалистами компании после прочтения заметки хакера. Можно не сомневаться, что хакеры найдут уязвимости и в iOS 9, но вряд ли они будут подробно расписывать их, ведь «дыры» используются в основном для джейлбрейка ***(Хакер рассказал об уязвимостях в iOS 8.4.1 // InternetUA (http://internetua.com/haker-rasskazal-ob-uyazvimostyah-v-iOS-8-4-1). – 2015. – 9.09).***

***

Основатель и глава компании Vulnerability Lab Бенджамин Кунц Межри (Benjamin Kunz Mejri) сообщил об уязвимости в мобильном приложении PayPal, позволяющей обойти двухфакторную аутентификацию и получить доступ даже к заблокированной учетной записи пользователя. Брешь затрагивает версии программы для iOS и Android.

С целью предотвращения мошенничества в некоторых случаях PayPal может запрашивать у пользователя подтверждение личности и блокировать его учетную запись. Для того чтобы ее разблокировать, необходимо позвонить или отправить электронное письмо на адрес сервиса согласно всплывающей форме. По словам Межри, уязвимость позволяет удаленному злоумышленнику

получить доступ к заблокированному аккаунту путем множественных попыток авторизации.

«Осуществляя множественные попытки запросить форму с помощью реально существующей учетной записи (x01445@gmail.com:chaos666), мы смогли обойти проверку подлинности личности ее владельца, – сообщил Межри. – API загружает контекст сайта, и пользователь может включить в процесс идентификации с помощью движка браузера собственный пользовательский аккаунт. Даже если учетная запись заблокирована, пользователь может получить доступ через мобильный API с уже существующими файлами cookie».

Эта техника также срабатывает для обхода двухфакторной аутентификации, поскольку, получив доступ к учетной записи, атакующий может изменить ее настройки, в том числе, пароль.

По словам Межри, он сообщил PayPal об уязвимости еще в апреле нынешнего года. Компания не исправила брешь, не посчитав ее критической. Эксперт не согласился с такой оценкой и опубликовал видео, демонстрирующее эксплуатацию уязвимости ***(Уязвимость в PayPal позволяет обойти двухфакторную аутентификацию // InternetUA (http://internetua.com/uyazvimost-v-PayPal-pozvolyaet-oboiti-dvuhfaktornuua-autentifikaciua). – 2015. – 9.09).***

***

9 сентября Adobe выпустила новую версию Shockwave Player, исправляющую две критические уязвимости. Бреши повреждения памяти CVE-2015-6680 и CVE-2015-6681 позволяли злоумышленнику удаленно выполнить код и получить контроль над системой. Уязвимым является Shockwave для Windows 12.1.9.160 и более ранних версий. Рекомендуется как можно скорее обновить плеер до версии 12.2.0.162. В настоящее время свидетельства эксплуатации этих уязвимостей отсутствуют.

Бреши существовали из-за некорректной проверки программным обеспечением вводимых пользователем данных. Злоумышленник мог проэксплуатировать их, вынудив жертву посетить веб-сайт, содержащий вредоносный Shockwave-контент. Обработка такого контента могла вызвать повреждение памяти, позволяющую атакующему выполнить код с правами пользователя. В результате успешной атаки хакер мог получить контроль над уязвимой системой.

Отметим, что это уже третье исправление, выпущенное Adobe за последние несколько недель. Так, 18 августа состоялся релиз патча для уязвимости в инструменте для разработки приложений Adobe LiveCycle Data Services. Брешь существовала в компоненте Apache Flex BlazeDS. 27 августа эта же уязвимость была исправлена в ColdFusion ***(Adobe исправила две критические уязвимости в Shockwave Player // InternetUA (http://internetua.com/Adobe-ispravila-dve-kriticseskie-uyazvimosti-v-Shockwave-Player). – 2015. – 9.09).***

***

Уязвимость в популярном мессенджере WhatsApp позволила злоумышленникам устанавливать на ПК пользователей трояны-вымогатели и другие типы вирусов. Уязвимость затронула все 200 млн пользователей веб-версии мессенджера.

200 млн пользователей WhatsApp

Специалист по информационной безопасности К. Декель (Kasif Dekel) из компании Check Point сообщил об обнаружении уязвимости в веб-версии мессенджера WhatsApp, затронувшей около 200 млн пользователей этого сервиса.

Суть уязвимости

Воспользовавшись уязвимостью, злоумышленник может отправить пользователю безобидную, на первый взгляд, контактную карточку vCard, содержащую вредоносный код. После открытия пользователем этой карточки хакер получает доступ к его системе. Он может дистанционно устанавливать на компьютер программы-вымогатели, ботов, инструменты для дистанционного доступа к пользовательским данным и т. д. vCard – это стандартизированный файл, который содержит имя, номер телефона, электронный адрес и другие контактные данные.

Достаточно знать номер телефона

Для того чтобы совершить атаку, злоумышленнику достаточно знать номер мобильного телефона жертвы, к которому привязан аккаунт WhatsApp. Веб-версия WhatsApp автоматически открывает вложения, отправленные с мобильного приложения, включая изображения, видео, аудиофайлы и vCard.

Уязвимость была устранена в версии 0.1.4481. Во всех предыдущих версиях WhatsApp она присутствует. Патч был выпущен 27 августа 2015 г.

«К счастью, команда WhatsApp среагировала достаточно быстро и в кратчайшие сроки смогла устранить уязвимость», – прокомментировал О. Вануну (Oded Vanunu), исследователь из Check Point.

Размер пользовательской базы

WhatsApp – самый популярный сервис обмена мгновенными сообщениями. Его пользовательская база включает около 900 тыс. человек, из которых около 200 млн пользуются веб-версией. WhatsApp принадлежит компании Facebook, которая купила его в 2014 г. за рекордную для индустрии сумму в 19 млрд дол.

Веб-версия

Веб-версия WhatsApp заработала в январе 2015 г. Чтобы начать пользоваться веб-версией WhatsApp, необходимо связать браузер с мобильным приложением, то есть доказать сервису, что это конкретный владелец смартфона хочет прибегнуть к веб-клиенту WhatsApp. Для этого требуется пройти по ссылке web.whatsapp.com на компьютере и отсканировать появившийся на экране QR-код с помощью камеры мобильного телефона, запустив на телефоне WhatsApp и пройдя в настройки приложения.

Пользователям реализация WhatsApp не понравилось. Они недоумевают, для чего вообще была создана веб-версия, если при ней остается необходимость в использовании смартфона.

Альтернативные мессенджеры, такие как Telegram, Viber, iMessage и Facebook Messenger, не требуют подключения к Интернету мобильного устройства для их использования на компьютере. При этом вся переписка также синхронизируется ***(Мессенджер WhatsApp стал «дырой» для установки троянов на 200 млн ПК // InternetUA (http://internetua.com/messendjer-WhatsApp-stal--diroi--dlya-ustanovki-troyanov-na-200-mln-pk). – 2015. – 9.09).***

***

По данным ИБ-эксперта Б. Кребса, в Европе арестованы главные подозреваемые в создании и применении сложного банковского вредоносного ПО Citadel и Dridex. Гражданин России и гражданин Молдовы были арестованы за пределами своих стран проживания, и теперь их ждет экстрадиция в США.

30-летний гражданин Молдовы был задержан властями в городе Пафос на Кипре, где он отдыхал со своей женой. По данным следствия, арестованный несет ответственность за причинение банкам ущерба на сумму 3,5 млн дол. в результате мошенничества с использованием компьютера. Обвиняемый является ключевой фигурой в преступной группировке, создавшей и использовавшей банковский троян Dridex, также известный как Cridex и Bugat. В свое время она отделилась от стоящей за созданием ботнета GameOver Zeus группировки Business Club, похитившей у банков порядка 100 млн дол. Dridex впервые появился в июле 2014 г., спустя месяц после ликвидации ботнета GameOver Zeus.

Согласно норвежским СМИ, независимо от гражданина Молдовы, в городе Фредрикстад, Норвегия, по запросу ФБР США был произведен арест 27-летнего россиянина по имени Марк. По данным американских правоохранителей, арестованный является разработчиком и продавцом созданного на базе исходного кода трояна ZeuS вредоносного ПО Citadel, которое сыграло ключевую роль в ряде преступлений против компаний малого бизнеса в США и Европе. Кроме того, вредонос предположительно использовался для атак на Target в ноябре и декабре 2013 г.

В течение 11 последних месяцев Марк находился в Норвегии под домашним арестом, в то время как ФБР добивалось его экстрадиции в США. Российские власти противились экстрадиции, ссылаясь на недостаток улик против Марка ***(Правоохранители арестовали создателей Citadel и Dridex // InternetUA (http://internetua.com/pravoohraniteli-arestovali-sozdatelei-Citadel-i-Dridex). – 2015. – 9.09).***

***

Исследователи из Heimdal Security сообщили об увеличении числа атак, в ходе которых злоумышленники внедряют вредоносный скрипт в популярные сайты и используют их в качестве распространителей вымогательского ПО. Хакеры атакуют интернет-ресурсы, работающие на устаревшей системе управления содержимым (CMS) и используют популярный набор эксплоитов Neutrino.

Согласно данным компании, большинство потенциально инфицированных таким образом сайтов работают на платформе WordPress – около 58,8 %. 20 % основанных на WordPress ресурсов работают еще на устаревших версиях CMS. Из этого следует, что около 142 млн сайтов уязвимы к внедрению вредоносных скриптов. Даже ресурсы, использующие последние версии WordPress, потенциально могут быть скомпрометированы, если работают на устаревших плагинах или из-за слабой защитой.

Блоги на платформе WordPress читают около 409 млн пользователей каждый месяц. Число потенциальных жертв вымогательского ПО может достигнуть крайне высоких показателей. Так как подобные атаки злоумышленников направлены не только на сайты на WordPress, последствия могут быть катострофическими.

Вредоносный скрипт внедряется в ссылки на целевой сайт на «полпути» к домену thedancingbutterfly.com. Данный домен перенаправляет трафик на nkzppqzzzumhoap.mi, содержащй набор эксплоитов Neutrino, который усиленно старается инфицировать систему жертвы вымогательским трояном TeslaCrypt. Neutrino эксплуатирует уязвимости состояния записи в Adobe Flash Player, Internet Explorer и Adobe Reader/Acrobat.

В свою очередь, троян TeslaCrypt шифрует файлы с различными расширениями, которые могут содержать важную информацию, а также добавляет файлы, в которых рассказывается, как расшифровать данные за биткоины ***(124 млн сайтов на базе WordPress могут распространять троян-вымогатель // InternetUA (http://internetua.com/124-mln-saitov-na-baze-WordPress-mogut-rasprostranyat-troyan-vimogatel). – 2015. – 9.09).***

***

В минувшем августе компания «Доктор Веб» уже рассказывала об одном из весьма распространенных троянцев, предназначенных для скрытой установки на компьютеры различных приложений.

Однако эта вредоносная программа является далеко не единственной в ряду рекламных установщиков: другой троянец с подобным набором функций, которому посвящена данная статья, носит наименование Trojan.InstallCube.339.

Как и многие другие установщики рекламных и нежелательных приложений, Trojan.InstallCube.339 может быть загружен пользователями с различных файлообменных сайтов и поддельных торрент-трекеров, специально созданных злоумышленниками для распространения вредоносного ПО.

Размер троянца Trojan.InstallCube.339 в упакованном виде составляет порядка 3,5 МБ. После распаковки в памяти компьютера он заполняет часть

имеющихся в его структуре данных информацией об управляющих серверах – вероятно, это сделано с целью затруднить анализ данной вредоносной программы. После этого троянец собирает сведения о компьютере, на котором он запущен, и демонстрирует на экране окно с индикатором процесса загрузки.

После получения данных с управляющего сервера Trojan.InstallCube.339 отображает диалоговое окно с информацией о загружаемом объекте, при этом окно имеет значок популярного торрент-клиента mTorrent. Особенность управляющих серверов данной вредоносной программы состоит в том, что они позволяют скачать полезную нагрузку только в том случае, если обращающийся к ним клиентский компьютер имеет российский IP-адрес.

При щелчке мышью по едва заметной ссылке Settings, расположенной в нижней части окна, пользователю демонстрируется список дополнительных программ, которые троянец установит на его компьютер. Обозначающие список данных приложений флажки являются неактивными, однако их можно сбросить в режиме «Выборочная установка».

Нажатие на кнопку «Сохранить» в предыдущем окне приводит к началу процесса загрузки требуемого пользователю файла и всех дополнительных программ. Перед завершением работы Trojan.InstallCube.339 удаляет себя ***(«Доктор Веб» предупреждает об очередном установщике нежелательных программ // ITnews (http://itnews.com.ua/news/78247-quotdoktor-vebquot-preduprezhdaet-ob-ocherednom-ustanovshhike-nezhelatelnykh-programm). – 2015. – 10.09).***

***

Check Point Software Technologies представляет Check Point SandBlast, новое улучшенное решение для предотвращения угроз, обеспечивающее самый высокий уровень защиты на рынке.

Благодаря использованию диагностики на уровне ЦП для обнаружения угроз до заражения Check Point SandBlast выводит безопасность на новый уровень. С помощью устойчивых к попыткам обхода средств обнаружения вредоносного ПО и улучшенной защиты даже от самых серьезных атак новое решение позволяет значительно снижать риск затрат от взломов.

В постоянной борьбе хакеров и специалистов по безопасности киберпреступники используют все более совершенные инструменты, в том числе атаки «нулевого дня» или модифицированные варианты существующего вредоносного ПО, которые легко обходят традиционные «песочницы» и проникают в инфраструктуры их жертв незамеченными. Эти новые направления атак требуют превентивного подхода с применением современных решений и технологий, которые смогут не только улавливать известные угрозы, но и идентифицировать и останавливать незнакомый вредоносный код с момента его первого появления. Новый передовой механизм обнаружения эксплойтов на уровне ЦП от Check Point имеет уникальную способность идентифицировать самые опасные угрозы «нулевого дня» на начальной стадии

до того, как вредоносная программа внедрится в инфраструктуру или попытается обойти системы обнаружения.

Кибервойна продолжается, и чтобы оставаться на шаг впереди всех современных угроз, необходимо применять превентивные меры безопасности для получения максимального уровня защиты без ущерба для эффективности эксплуатации, – говорит М. Стиглианезе (Mike Stiglianese), управляющий директор компании Axis Technology LLC и бывший директор по информационным технологиям и рискам крупной финансовой организации. – С новыми возможностями обнаружения на уровне ЦП Check Point снова поднимают планку для всей отрасли. Компания предлагает инновационные комплексные решения с самым совершенным арсеналом защиты от продвинутых таргетированных кибератак».

«В современном мире, где ландшафт угроз постоянно меняется, безопасность – один из самых важных приоритетов. Использование технологии, которая может защитить наши критически важные активы от новейшего вредоносного ПО и при этом позволит доставлять данные без ущерба для бизнес-процессов, является огромным шагом вперед, – говорит Р. Пирс (Richard Peirce), директор отдела инфраструктурных сервисов компании Boston Properties. – Для нас важно тщательно оценивать ресурсы, необходимые для внедрения любого нового продукта в нашу среду. “Песочница” от Check Point была установлена и запущена очень быстро, ее эксплуатация требует минимального текущего контроля управления».

Ключевые особенности Check Point SandBlast включают:

– обнаружение вредоносного кода на стадии вторжения еще до того, как он применит методы уклонения от обнаружения. Механизм обнаружения нельзя обойти с помощью циклов временной задержки, попыток вычислить использование виртуализованной ОС или иных методов обхода «песочницы»;

– сочетание мощности обнаружения на уровне ЦП с эмуляцией на уровне ОС позволяет анализировать содержимое файлов различных типов, включая документы MS Office, PDF, flash, исполнительные файлы, архивы и т. д.;

– быстрая доставка безопасных версий файлов с данными с помощью встроенной функции Threat Extraction, позволяющей блокировать вредоносный контент в режиме реального развертывания без значительных задержек ***(Check Point представляет новое решение SandBlast для борьбы с вредоносным ПО // ITnews (http://itnews.com.ua/news/78243-check-point-predstavlyaet-novoe-reshenie-sandblast-dlya-borby-s-vredonosnym-po). – 2015. – 9.09).***

***

Скандал вокруг уязвимости под названием Stagefright, которая позволяет хакерам получить доступ практически к любому Android-устройству, вынудил Google и другие крупные компании пойти на крайние меры и с прошлого месяца начать ежемесячно выпускать обновления системы безопасности для своих устройств. К сожалению, первое обновление от Google лишь частично закрывало уязвимость Stagefright. Теперь для линейки Nexus было выпущено

свежее обновление безопасности, после которого номер прошивки меняется на LMY48M. При этом Nexus 6 обновляется до версии LYZ28K, а Nexus 7 – LMY48P.

На сегодняшний день обновление доступно для клиентов T-Mobile и их Nexus 4, 5, 6, 7 и 9, но в ближайшее время апдейт будет выпущен и для остальных версий Nexus-устройств. Также ожидается, что данное обновление получат планшет Nexus 10 и телеприставка Nexus Player. Как обычно, в описании лишь указано, что эта версия улучшит систему безопасности Android, поэтому ничего конкретного об изменениях неизвестно ***(Google выпускает сентябрьское обновление безопасности Android // InternetUA (http://internetua.com/Google-vipuskaet-sentyabrskoe-obnovlenie-bezopasnosti-Android). – 2015. – 10.09).***

***

Американские энергосистемы были взломаны хакерами более 150 раз за последние пять лет.

Причем это только успешные проникновения. А кибератаки на компьютеры министерства идут постоянно. За указанный период их было не менее полутора тисяч (http://nikolaev-city.net/16863/hakery-atakovali-obekty-yadernoy-energetiki-ssha).

Взломы пока ничем страшным или даже примечательным не обернулись, но это-то, по словам экспертов, и настораживает. Дело в том, что никто до сих пор не знает, с какой именно целью производились эти атаки.

Судя по тому, что более половины проникновений совершены в сети научного отдела департамента энергетики, речь идет в основном об обычном промышленном шпионаже. Тем не менее, около 20 успешных атак пришлись на объекты ядерной энергетики. А это уже грозит не просто отключениями или похищениями личных данных: достаточно вспомнить вирус Stuxnet, который атаковал компьютерные системы иранского центра по обогащению урана в Натанзе. Тогда изменение частоты вращения центрифуг едва не привела к катастрофе и отбросила иранскую ядерную программу на несколько лет назад.

В случае с США почти половина успешных взломов позволяла хакерам получить полный доступ к компьютеру и делать с ним все, что угодно.

Самое интересное, что департамент энергетики признает, что не справляется со всеми угрозами. Если хакеры задумают что-то действительно нехорошее, при определенном упорстве и сноровке у них это, скорее всего, получится. При этом постоянная модернизация только облегчает задачу взломщикам: системы автоматического контроля энергосетей, позволяющие экономить электроэнергию, в то же время открывают новые уязвимости ***(Хакеры атаковали объекты ядерной энергетики США // Nikolaev-City (http://nikolaev-city.net/16863/hakery-atakovali-obekty-yadernoy-energetiki-ssha). – 2015. – 11.09).***

***

Русскоговорящие хакеры используют спутники для доступа к конфиденциальным данным дипломатических и оборонных ведомств США и Европы, передает The Washington Post.

«Группа продвинутых русскоязычных хакеров использует коммерческие спутники, чтобы получить доступ к данным дипломатических и военных ведомств в Соединенных Штатах и Европе, а также для маскировки своего расположения», – говорится в статье со ссылкой на специалиста российского производителя антивирусов «Лаборатория Касперского» С. Тэнасе.

По информации С. Тэнасе, речь идет о группе хакеров Turla. Группа взяла название в честь одноименного вредоносного программного обеспечения, которым она пользуется.

Их целью уже на протяжении нескольких лет являются государственные организации, посольства и компании в России, Китае и других странах.

С.Тэнасе отметил, что раньше компания никогда не фиксировала использование вредоносного ПО для захвата спутника. Данная группа хакеров – первая, кто это сделал ***(Русские хакеры используют спутники для доступа к данным дипведомств США // InternetUA (http://internetua.com/russkie-hakeri-ispolzuuat-sputniki-dlya-dostupa-k-dannim-dipvedomstv-ssha). – 2015. – 10.09).***

***

На днях мы сообщали о четырех уязвимостях, обнаруженных в продуктах FireEye ИБ-экспертом Кристианом Эриком Эрмансеном (Kristian Erik Hermansen). Исследователь потребовал у компании вознаграждение за обнаруженные бреши (по 10 тыс. дол. за каждую), однако FireEye не только не выплатила вознаграждение, но также попросила Эрмансена не раскрывать подробности об этих уязвимостях.

Эксперт опубликовал PoC-код для одной из брешей на сайте Pastebin, сопроводив публикацию заявлением: «Всего лишь одна из многих полезных уязвимостей нулевого дня в продуктах FireEye/Mandiant. Существует уже более 18 месяцев без каких-либо исправлений от этих “экспертов” безопасности из FireEye. Уверен, что эту и другие бреши в продуктах допустили сотрудники Mandiant. Что еще хуже, у FireEye нет внешних исследователей безопасности».

Как сообщает ИБ-эксперт Грэм Клули (Graham Cluley), представители ИБ-компании связались с Эрмансеном и его коллегой Р. Перрисом (Ron Perris) и напомнили о важности «ответственного раскрытия».

«Сегодня FireEye стало известно о четырех уязвимостях в ее продуктах благодаря их публичному раскрытию Кристианом Эрмансеном. Теперь бреши можно купить. Мы уважаем усилия исследователей безопасности, таких как Кристиан Эрмансен и Рон Перрис, которые ищут уязвимости в безопасности наших продуктов, но мы выступаем за ответственное раскрытие», – говорится в заявлении FireEye ***(Эксперт требует у FireEye 40 тыс. дол. за обнаруженные уязвимости в ее продуктах // InternetUA (http://internetua.com/ekspert-trebuet-u-FireEye--40-tis--za-obnarujennie-uyazvimosti-v-ee-produktah). – 2015. –10.09).***

***

ИБ-исследователь обнаружил семь опасных уязвимостей в программном обеспечении Advantech WebAccess. Данное ПО, ранее известное как Broadwin WebAccess, является программным обеспечением HMI/SCADA, работающим на базе стандартного веб-браузера. Продукт разработан тайваньской компанией Advantech и используется в энергетике, а также коммерческими и правительственными организациями по всему миру.

Согласно данным эксперта П. Даршанама (Praveen Darshanam), компонент AspVCObj.dll в Advantech WebAccess 8.0 и более ранних версиях подвержен семи уязвимостям переполнения стекового буфера (CVE-2014-9208), эксплуатация которых может привести к удаленному выполнению кода.

По словам П. Даршанама, злоумышленник может удаленно выполнить код, передав специально сформированную строку на ConvToSafeArray API в ActiveX-элементе ASPVCOBJLib.AspDataDriven. Для успешной эксплуатации бреши необходимо, чтобы жертва перешла по вредоносной ссылке или открыла вредоносный веб-сайт.

Специалист заявил, что компании Advantech стало известно о данных уязвимостях еще в декабре 2014 г. Advantech сообщила, что исправит бреши в апреле текущего года, однако обновления так и не были выпущены. За последние несколько лет Команда реагирования на киберугрозы систем индустриального контроля опубликовала десятки бюллетеней о уязвимостях в продуктах Advantech. В число выявленных брешей вошли XSS-уязвимости, бреши, позволяющие выполнить SQL-инъекции, CSRF-уязвимости и пр. Стоит отметить, что продукты Advantech неоднократно становились мишенью в хакерской кампании, в рамках которой использовался вредонос BlackEnergy ***(В Advantech WebAccess обнаружены семь опасных уязвимостей // InternetUA (http://internetua.com/v-Advantech-WebAccess-obnarujeni-sem-opasnih-uyazvimostei). – 2015. – 11.09).***

***

ИБ-эксперт Ж. Аренс (Julien Ahrens) сообщил об уязвимости в приложении для обмена мгновенными сообщениями Yahoo! Messenger, которую компания не намерена исправлять. По словам исследователя, брешь переполнения буфера CVE-2014-7216 позволяет злоумышленнику удаленно выполнить код. Несмотря на опасность уязвимости, Yahoo! не спешит выпускать исправления, поскольку мессенджер больше не поддерживается компанией.

Эксплуатация бреши возможна, когда жертва устанавливает на свое устройство новые эмотиконы. Учитывая, что «улыбочки» пользуются огромной популярностью у пользователей, этот вектор атак может представлять серьезную угрозу безопасности. Заставив жертву инсталлировать специальным образом сконфигурированный набор эмотиконов, злоумышленник получает те же права, что и владелец устройства.

Ж. Аренс пояснил, что мессенджер загружает контент файла emoticons.xml из двух разных директорий, когда пользователь авторизуется для того, чтобы проверить доступность новых эмотиконов и ссылок на них. Проблема заключается в том, что приложение некорректно проверяет длину строки ссылки и ключевые значения названия. Это может вызвать переполнение буфера и, как результат, привести к удаленному выполнению кода.

По словам Ж. Аренса, он сообщил Yahoo! о бреши еще в мае прошлого года. В прошлом месяце компания разрешила исследователю раскрыть подробности об уязвимости, заявив, что не будет ее исправлять ***(Yahoo! отказалась исправлять опасную уязвимость в своем мессенджере // InternetUA (http://internetua.com/Yahoo--otkazalas-ispravlyat-opasnuua-uyazvimost-v-svoem-messendjere). – 2015. – 11.09).***

***

Кибергруппировка Carbanak, похитившая сотни миллионов долларов, вернулась в Россию. Об этом говорят в международной антивирусной компании Eset.

По словам экспертов, были обнаружены вирусы, при помощи которых хакеры осуществляют таргетированные атаки на крупные финансовые учреждения, среди которых банки – Forex-трейдеры из России, США, Германии, Объединенных Арабских Эмиратов, Великобритании и некоторых других стран.

В Carbanak используют несколько семейств вредоносных программ, основанных на разных кодовых базах, но содержащих общие черты, например, подписи на основе одного цифрового сертификата. Среди прочих инструментов кибергруппировка применяет троян Win32/Spy.Agent.ORM, бэкдор Win32/Wemosis для кражи конфиденциальных данных карт с PoS-терминалов и вирус Win32/Spy.Sekur.

Одним из вариантов атаки киберпреступников является отправка по электронной почте фишинговых сообщений с вредоносным вложением в виде RTF-файла с различными эксплойтами или файла в формате SCR. В частности, были замечены следующие названия вложенных опасных файлов: «АО “АЛЬФА-БАНК” ДОГОВОР.scr», «Перечень материалов для блокировки от 04.08.2015г.scr», «Правила Банка России от 06.08.2015.pdf %много_пробелов% .scr» и др. ***(Хакеры Carbanak возвращаются в Россию // InternetUA (http://internetua.com/hakeri-Carbanak-vozvrasxauatsya-v-rossiua). – 2015. – 11.09).***

***

Мешканець м. Львова систематично з власної домівки, через створений ним інтернет-магазин, здійснював продаж облікових даних інших осіб, зокрема логінів та паролів до платіжних систем, а саме: до автоматизованих систем «WEBMONEY» та «Yandex.Money».

Як повідомляє прес-служба прокуратури Львівської області, окрім того, зловмисник продавав логіни та паролі інших осіб до електронних адрес «YANDEX.RU», «MAIL.RU», ігрового сервісу «ADVANCE-RP.RU», сервісу букмекерської контори «MARATHONBET.COM» та соціальної мережі «VK.COM».

За процесуального керівництва прокуратури Франківського району м. Львова останньому повідомлено про підозру у вчиненні кримінального правопорушення, передбаченого ч. 1 ст. 361-2, ч. 2 ст. 361-2, ч. 3 ст. 15 ч. 2 ст. 361-2 КК України.

Вироком Франківського районного суду його визнано винним та призначено покарання у вигляді двох років позбавлення волі з іспитовим строком два роки ***(На Львівщині вперше засудили злочинця за торгівлю інформацією з обмеженим доступом // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/na_lvivshchyni_vpershe_zasudyly_zlochyntsya_za_torgivlyu_informatsiieyu_z_obmezhenym_dostupom_191616.html). – 2015. – 11.09).***

***

Как следует из отчета компании Akamai, с апреля нынешнего года начала действовать новая киберпреступная группировка, осуществляющая DDoS-атаки на жертв и шантажируя их. Группа, известная как DD4BC, за обозреваемый период осуществила как минимум 114 DDoS-атак со средней мощностью в 13,34 Гбит/с.

Киберпреступники шантажировали крупные финансовые организации и прочие предприятия, угрожая осуществить DDoS-атаку, которая вывела бы из строя их сети. Главной целью группировки становились финансовые учреждения, банки и кредитные союзы, online-сервисы обмена валют и компании по обработке платежей. В одном случае был произведен UDP-флуд мощностью в 56,2 Гбит/с. Для того чтобы прекратить атаку, жертва должна была отправить киберпреступникам от 25 до 50 биткоинов (порядка 6000–12000 дол. на момент написания статьи).

Akamai опубликовала образцы писем, в которых группировка требовала перевода денежных средств на их кошельки Bitcoin.

«Ваш сайт будет находиться под атакой, пока вы не заплатите 25 биткоинов, – сообщалось в одном из писем. – Учтите, что вам будет нелегко отразить нашу атаку – мощность нашего UDP-флуда составляет 400-500 Гб/с. Можете даже не пытаться».

Киберпреступники обещали прекратить атаку, как только жертва пойдет на их условия и заплатит выкуп ***(Киберпреступники осуществляют DDoS-атаки на жертв с целью выкупа // InternetUA (http://internetua.com/kiberprestupniki-osusxestvlyauat-DDoS-ataki-na-jertv-s-celua-vikupa). – 2015. – 13.09).***

***

Хакеры «Исламского государства» пытались заполучить доступ к секретной информации, касающейся высших министров Великобритании, пишет газета Mirror.

Издание ссылается на расследование Центра правительственной связи (GCHQ), которое в том числе занимается защитой информации органов власти и армии.

По предварительным данным, исламисты не смогли получить доступ к каким-либо важным данным, но хотели взломать почтовые ящики и узнать расписание кабинета министров Д. Кэмерона.

В связи с неудачной попыткой ИГ в GCHQ усилили процедуры сетевой безопасности чиновников и поменяли пароли ***(Хакеры ИГ пытались добыть информацию о расписании британских министров // InternetUA (http://internetua.com/hakeri-ig-pitalis-dobit-informaciua-o-raspisanii-britanskih-ministrov). – 2015. – 13.09).***

***

Китайские власти гневно отреагировали на заявление директора национальной разведки США Д. Клеппера о хакерских атаках и просят прекратить «необоснованно» обвинять их в этом, сообщает Reuters.

Китай регулярно отрицает какую-либо причастность ко взломам. «Поддержание безопасности в киберпространстве должно быть точкой сотрудничества, а не источником конфликта между Китаем и Соединенными Штатами», – заявил представитель китайского МИДа Х. Лэй на еженедельном брифинге. «Мы надеемся, что США прекратят свои необоснованные нападки против Китая и начнут диалог на основе взаимного уважения», – добавил он.

Также по этому вопросу высказался член Госсовета КНР Я. Цзечи. Он надеется, что США, Китай и другие страны будут работать вместе для создания правил кибербезопасности на международной арене. Я. Цзечи также отметил, что Китай сам зачастую становится жертвой хакерских атак, и эти случаи должны быть тщательно расследованы.

Ранее директор американской национальной разведки Д. Клэппер заявил, что действия китайских хакеров угрожают национальной безопасности, важным экономическим данным и интеллектуальной собственности США ***(Китай просит прекратить «необоснованные» обвинения США в кібератаках // InternetUA (http://internetua.com/kitai-prosit-prekratit--neobosnovannie--obvineniya-ssha-v-kiberatakah). – 2015. – 13.09).***

***

«Украинские Кибервойска» обнаружили, что Яндекс официально предоставляет услуги террористам. Об этом сообщил в Facebook координатор УКВ Е. Докукин, пишет donpress.com.

«Еще в августе мы захватили много официальных ящиков “ДНР”, об одном из них я недавно писал, что мы взломали электронную почту “Народного Совета ДНР”.

Эти ящики размещены на корпоративной Яндекс. Почте (сервис “Яндекс.Почта для домена”). На домене своего официального сайта dnr-sovet.su террористы сделали почтовые ящики с использованием сервиса Яндекса.

За 15 месяцев УКВ взломали сотни почтовых ящиков сепаратистов, террористов и государственных органов России. Среди них было много ящиков на бесплатной почте, в том числе Емайл ДНР на Mail.ru, Yandex, Gmail и других сервисах.

Но в данном случае имеет место корпоративная почта от Яндекса. Компания должна была проверить используют этот сервис и на каком домене. А пользуются они этим сервисом с 2014 г., и Яндекс имел достаточно времени, чтобы обнаружить это и отказать этим “клиентам”, но до сих пор этого не сделал», – сообщил Е. Докукин ***(Яндекс предоставляет свои услуги террористам? // Донбасс (http://donbass.ua/news/region/2015/09/13/jandeks-predostavljaet-svoi-uslugi-terroristam.html). – 2015. – 13.09).***

***

Пользователь GitHub распространил в сети модели для 3D-печати универсальных ключей Администрации транспортной безопасности США, способных открывать большинство популярных кодовых замков для багажа. Об этом сообщает Wired.

В 2014 г. газета The Washington Post опубликовала материал «Что происходит с вашим багажом?», рассказывающий о работе погрузочной службы. На одном из снимков, опубликованных в статье, была показана полная связка универсальных мастер-ключей, с помощью которых грузчики или сотрудники охраны могут открыть почти любой чемодан – например, для того, чтобы установить, кому он принадлежит.

9 сентября модели для печати всех ключей, созданные на основе фотографии из материала, были опубликованы на GitHub пользователем под ником Xylitol. С их помощью любой человек, имеющий доступ к 3D-принтеру может создать себе полный комплект, используемый службами аэропорта.

Спустя считанные часы после публикации в сети появились первые тесты самодельных ключей, которые действительно способны открывать кодовые замки.

В разговоре с Wired автор 3D-моделей заявил, что не предполагал, что они действительно окажутся пригодными для открытия замков.

Если кто-то говорит, что мои 3D-модели работают, что ж, это круто, и демонстрирует, как одна фотография связки ключей может нарушить работу всей системы. Xylitol

Как отмечает The Verge, Администрации транспортной безопасности США рекомендует всем производителям замков оставлять «лазейки» для себя, поэтому утечка может привести к необходимости замены почти всех

находящихся в использовании кодовых замков компаний Master Lock, Samsonite и American Tourister.

В разговоре с Wired профессор компьютерных наук и известный взломщик М. Блэйз (Matt Blaze) пояснил, что на кодовые замки в принципе не стоит всерьёз надеяться: опытный вор способен справиться с ними и без мастер-ключей ***(Универсальные ключи для багажных замков «утекли» в сеть в виде моделей для 3D-печати // InternetUA (http://internetua.com/universalnie-kluacsi-dlya-bagajnih-zamkov--utekli--v-set-v-vide-modelei-dlya-3D-pecsati). – 2015. – 13.09).***

***

Киберспециалисты рассказали о том, что в Интернете появился новый вирус под названием ОС Android. Об эом пишет Гривна.

Этот троян легко ломает систему защиты телефона, а, кроме того, меняет пароли на свои. После чего у людей не только пропадают деньги со счета, но также мошенники научились требовать деньги для того, чтобы владелец мог полноценно пользоваться девайсом.

Вирус был обнаружен известной компанией по защите устройств от разных мошеннических программ ESET.

«Заразиться» трояном можно посредством скачивания нелегального приложения Porn Droid. От пользователей сразу после установления Porn Droid мошенники потребуют перевести на их счет 500 дол., в противном случае – телефон не будет выполнять основные функции.

От вируса можно избавиться путем сбрасывания всех настроек ***(Новый троян для Android меняет PIN-код устройств // INSHE.TV (http://inshe.tv/society/2015-09-12/54868/). – 2015. – 12.09).***

***

Доцент Университета Иллинойса (США) Ромит Рой Чоудхури (Romit Roy Choudhury) совместно с группой студентов разработал приложение, способное определять, какие клавиши на экране смарт-часов нажимает пользователь, и перехватывать вводимый текст. Созданная в рамках проекта Motion Leaks (MoLe) программа будет представлена на конференции MobiCon 2015.

С помощью встроенных в часы Samsung Gear Live датчиков движения, а также данных акселерометра и гироскопа исследователям удалось создать 3D-карту движений рук пользователя во время набора текста. После этого были разработаны два алгоритма – один для определения нажимаемых клавиш и другой для составления слов из набранных букв. Первый из них фиксирует места, где датчик смарт-часов улавливает глубокое нажатие, а затем создает карту из наиболее часто используемых клавиш. С учетом раскладки клавиатуры каждая кнопка ассоциируется с отдельной буквой.

Полученные данные обрабатываются с помощью второго алгоритма. Анализируя паузы между нажатиями левой руки, эксперты смогли определить

количество букв, введенных правой рукой. Далее алгоритм позволил выяснить, какие слова были набраны на дисплее «умных» часов.

Создателям приложения еще предстоит проделать большую работу над совершенствованием своей системы, поскольку в ней есть несколько недостатков. К примеру, на данном этапе она не способна определять специальные символы (числа, знаки препинания и пр.), также существуют проблемы с определением пробела, а для обработки подходят только данные пользователей со стандартной моделью ввода текста.

По мнению исследователей, их разработка демонстрирует потенциальную угрозу безопасности данных, которую могут представлять «умные» часы ***(Эксперты создали приложение для перехвата вводимого текста через клавиатуру смарт-часов // InternetUA (http://internetua.com/eksperti-sozdali-prilojenie-dlya-perehvata-vvodimogo-teksta-cserez-klaviaturu-smart-csasov). – 2015. – 14.09).***

***

Один из крупнейших в мире производителей SCADA-систем, японская компания Yokogawa предупредила о наличии трех опасных уязвимостей в своих продуктах. Как сообщается в бюллетене ICS-CERT, бреши позволяют удаленному пользователю вызвать переполнение стекового буфера и выполнить произвольный код.

Уязвимостям подвержена 21 промышленная система Yokogawa, включая CENTUM, ProSafe-RS, STARDOM и FAST/TOOLS. Бреши существуют как в решениях на основе Windows, так и в SCADA-системах со встроенной ОС.

Для того чтобы успешно проэксплуатировать уязвимость, удаленный пользователь должен отправить специально сформированный пакет процессу, связанному с сетевыми подключениями. В зависимости от содержимого пакета произойдет либо отказ в обслуживании, либо аварийное завершение работы данного процесса. Во втором случае злоумышленник сможет выполнить произвольный код.

Некоторые из уязвимых продуктов уже получили обновления, в то время как ряд SCADA-систем все еще остается подвержен уязвимостям. Производитель обещает выпустить исправление для оставшихся систем в ближайшее время ***(В SCADA-системах Yokogawa обнаружены множественные уязвимости // InternetUA (http://internetua.com/v-SCADA-sistemah-Yokogawa-obnarujeni-mnojestvennie-uyazvimosti). – 2015. – 15.09).***

***

Специалисты компании «Доктор Веб» исследовали очередного троянца, умеющего заражать платежные терминалы, который на поверку оказался модификацией другой вредоносной программы, хорошо знакомой нашим вирусным аналитикам.

POS-троянец, добавленный в вирусные базы Dr.Web под именем Trojan.MWZLesson, после своего запуска регистрирует себя в ветви системного реестра, отвечающей за автозагрузку приложений. В его архитектуре предусмотрен модуль, сканирующий оперативную память инфицированного устройства на наличие в ней треков банковских карт. Этот код злоумышленники позаимствовали у другой предназначенной для заражения POS-терминалов вредоносной программы, известной под именем Trojan.PWS.Dexter. Обнаруженные треки и другие перехваченные данные троянец передает на управляющий сервер.

Trojan.MWZLesson умеет перехватывать GET- и POST-запросы, отправляемые с зараженной машины браузерами Mozilla Firefox, Google Chrome или Microsoft Internet Explorer, – эти запросы троянец дублирует на принадлежащий злоумышленникам управляющий сервер. Кроме того, данная вредоносная программа может выполнять следующие команды:

CMD – передает поступившую директиву командному интерпретатору CMD;

LOADER – скачивает и запускает файл (dll – с использованием утилиты regsrv, vbs – с использованием утилиты wscript, exe – осуществляется непосредственный запуск);

UPDATE – команда обновления;

rate – задает временной интервал сеансов связи с управляющим сервером;

FIND – поиск документов по маске;

DDOS – начать DDoS-атаку методом http-flood.

Обмен данными с управляющим центром Trojan.MWZLesson осуществляет по протоколу HTTP, при этом пакеты, которые троянец отсылает на удаленный сервер, не шифруются, однако вредоносная программа использует в них специальный параметр cookie, при отсутствии которого командный сервер игнорирует поступающие от троянца запросы.

В процессе изучения внутренней архитектуры Trojan.MWZLesson вирусные аналитики компании «Доктор Веб» пришли к выводу, что этот троянец им хорошо знаком, поскольку часть его кода раньше встречалась им в составе другой вредоносной программы. Ею оказался BackDoor.Neutrino.50, урезанной и сокращенной версией которого по сути и является Trojan.MWZLesson.

BackDoor.Neutrino.50 – это многофункциональный бэкдор, использующий при своем распространении эксплойты для уязвимости CVE-2012-0158. Зафиксированы случаи загрузки этой вредоносной программы с различных взломанных злоумышленниками сайтов. При запуске BackDoor.Neutrino.50 проверяет наличие в своем окружении виртуальных машин, в случае обнаружения таковых троянец выводит сообщение об ошибке «An unknown error occurred. Error - (0x[случайное число])», после чего BackDoor.Neutrino.50 удаляет себя из системы.

Помимо функций троянца для POS-терминалов, данный бэкдор обладает возможностью красть информацию из почтового клиента Microsoft, а также

учетные данные для доступа к ресурсам по протоколу FTP с использованием ряда популярных ftp-клиентов. Кроме директив, характерных для Trojan.MWZLesson, троянец BackDoor.Neutrino.50 умеет выполнять и другие команды, в частности, он способен осуществлять несколько типов DDoS-атак, удалять некоторые другие работающие на инфицированной машине вредоносные программы, а также может попытаться заразить компьютеры, доступные в локальной сети.

Сигнатуры этих троянцев добавлены в вирусные базы Dr.Web, поэтому они не представляют опасности для пользователей наших антивирусных продуктов ***(Trojan.MWZLesson – троянец для POS-терминалов // ITnews (http://itnews.com.ua/news/78306-trojanmwzlesson-troyanets-dlya-pos-terminalov). – 2015. – 16.09).***

***

Росіянин визнав себе винним в участі у найбільшій хакерській атаці в історії США, яка призвела до викрадення даних 160 млн банківських карт і 300 млн дол.

Про це повідомляє Еспресо.TV із посиланням на Reuters.

Федеральне обвинувачення заявило, що 34-річний В. Дрінкман зізнався в зговорі з метою незаконно отримати доступ до комп'ютерів і змові з метою здійснити шахрайство.

Серед компаній, які піддалися кібератакам у період з 2005 по 2012 р., були Nasdaq, торгова мережа 7-Eleven, французька компанія Carrefour SA, JC Penney Co, авіакомпанія JetBlue та ін. Усього від діяльності хакерів постраждали 16 компаній.

В. Дрінкману може загрожувати до 30 років позбавлення волі. Вирок буде оголошено 16 січня. Росіянин був арештований у 2012 р. в Нідерландах, а потім екстрадований до США.

Також серед обвинувачуваних у цій справі ще троє росіян і один українець.

Росіянин Д. Смілянець також був у 2012 р. заарештований у Нідерландах і екстрадований до Сполучених Штатів Америки. Нині він перебуває під вартою. Троє інших обвинувачених – росіяни О. Калінін і Р. Котов, а також українець М. Ритіков – перебувають у розшуку.

Нагадаємо, 14 вересня прес-секретар російського президента Д. Пєсков повідомив, що хакери здійснили потужний напад на сайт Кремля ***(Росіянин зізнався у найбільшій кібератаці в історії США // Espreso.tv (http://espreso.tv/news/2015/09/16/rosiyanyn_ziznavsya_u_naybilshiy_kiberataci_v_istoriyi_ssha). – 2015. – 16.09).***

***

Провайдер решений в сфере кибербезопасности FireEye зафиксировал новый вирус, который угрожает банкоматам. С помощью вредоносного ПО мошенники могут получить доступ к информации о платежных картах.

Вирус под названием Suceful способен хорошо маскировать атаки на банкомат.Чтобы системы безопасности банка не зафиксировали действия мошенников, программа способна вывести из строя сигнализацию, отключить датчики обнаружения, а также взломать замок на двери, ведущей внутрь банкомата.

Вредоносную программу можно использовать на разных типах банкоматов, потому, что межплатформное программное обеспечение устройства не зависит от производителя АТМ.

Пока злоумышленники используют вредоносное ПО для атак на банкоматы марок Diebold и NCR, но перечень потенциальных мишеней может измениться достаточно скоро.

На сегодняшний день действия преступников настолько аккуратны, что пользователь банкомата не сможет распознать скомпрометированное устройство по внешнему виду. Чаще всего такие банкоматы не отдают обратно платежную карту. В таком случае необходимо позвонить в банк и не отходить от терминала, чтобы не позволить злоумышленникам изъять платежный инструмент из машины ***(Банкоматам угрожает новый вирус // InternetUA (http://internetua.com/bankomatam-ugrojaet-novii-virus). – 2015. – 16.09).***

***

Основатель «Украинских Кибервойск» Е. Докукин в прямом эфире «Обозревателя» рассказал о том, как отечественным IT-специалистам удается успешно вести «кибервойну» с пророссийскими террористами и ФСБ России (http://tech.obozrevatel.com/news/46851-ukrainskie-hakeryi-zablokirovali-bolee-200-sajtov-fsb-i-terroristov.htm).

Как пояснил Е. Докукин, «Кибервойска» заняты как блокировкой, так и закрытием сайтов и отдельных страниц террористов, пророссийских сил и ФСБ России.

«Закрытие происходит через написание жалоб провайдерам или администрации сервисов, – рассказал он. – Блокируются также отдельные страницы блог-хостингов, к которым относится также популярный ресурс Live Journal. Возможностью бесплатных и свободных публикаций пользуются террористы, связанные с ФСБ, а также “путинисты и заядлые рашисты”». Закрытием или блокированием таких страниц и занимаются «Украинские Кибервойска».

Кроме того, украинцы закрывают страницы, на которых ФСБ размещает персональную информацию об украинских патриотах-любителях «хунты». В этом контексте Е. Докукин заметил: «Есть тысячи сайтов, где размещен мой адрес».

Как рассказал эксперт, на сегодняшний день «Украинские Кибервойска» полностью закрыли или заблокировали 213 подобных сайтов ***(Украинские***

хакеры заблокировали более 200 сайтов ФСБ и террористов // Обозреватель (http://tech.obozrevatel.com/news/46851-ukrainskie-hakeryi-zablokirovali-bolee-200-sajtov-fsb-i-terroristov.htm). – 2015. – 16.09).

***

«Доктор Веб» предупреждает о появлении новой вредоносной программы Trojan.RoboInstall.1, атакующей пользователей персональных компьютеров под управлением операционных систем Windows.

Названный зловред представляет собой трояна-установщика, загружающего на ПК жертвы рекламные и нежелательные приложения. Программа распространяется с использованием файлообменных сайтов, поддельных торрентов и иных аналогичных интернет-ресурсов, созданных злоумышленниками.

Запустившись на компьютере, троян проверяет хранящуюся в его структурах конфигурационную информацию, и в случае если она повреждена или отсутствует, демонстрирует на экране сообщение об ошибке.

На адрес управляющего сервера зловред отправляет POST-запрос, содержащий массив информации в формате JSON (JavaScript Object Notation), сжатый при помощи библиотеки ZLIB. В ответ он принимает сведения о загружаемых исполняемых файлах и настройках демонстрации флажков для отказа их установки.

Примечательно, что, в отличие от многих других установщиков рекламного ПО, в отображаемых трояном диалоговых окнах такие флажки зачастую отсутствуют, и запуск на исполнение загружаемых зловредом файлов осуществляется без каких-либо дополнительных условий ***(Троян RoboInstall устанавливает нежелательные приложения // InternetUA (http://internetua.com/troyan-RoboInstall-ustanavlivaet-nejelatelnie-prilojeniya). – 2015. – 16.09).***

***

Эксперты обнаружили серьезную уязвимость в операционной системе Android версии 5.0 и выше. По информации исследователя Техасского университета Д. Гордона, злоумышленникам не составит труда взломать любой запароленный Android-смартфон. Правда, для этого он должен находиться в руках хакера.

Для того чтобы обойти пароль на защищенном устройстве, не обязательно даже обладать специальными знаниями. Сперва нужно открыть экран экстренного вызова на телефоне и ввести там длинный номер с большим количеством символов (можно даже использовать одни только звездочки). Затем пользователь должен удваивать все эти символы с помощью копирования и вставки, пока поле ввода окончательно не заполнится (придется сделать около 11 повторений).

После проделанных манипуляций нужно вернуться на начальный экран блокировки, включить камеру, открыть на ней панель уведомлений и нажать на

шестеренку, которая должна открыть настройки. Пользователю предложат ввести пароль: вместо него придется вставить те символы, которые были скопированы ранее. Такую процедуру надо повторить несколько раз, пока система не начнет зависать, а камера не перейдет в полноэкранный режим.

В итоге через некоторое время приложение камеры «вылетит», а перед пользователем откроется рабочий стол заблокированного устройства. Таким образом злоумышленник может получить доступ ко всем приложениям и данным на телефоне.

Как сообщают эксперты, разработчики Android уже начали исправление проблемы, однако не все производители смартфонов успели внедрить новый патч ***(Хакеры научились взламывать любой пароль на Android-смартфонах // InternetUA (http://internetua.com/hakeri-naucsilis-vzlamivat-luaboi-parol-na-Android-smartfonah). – 2015. – 17.09).***

***

Эксперты из финской компании F-Secure сообщили об обнаружении группировки хакеров, «работающих на правительство России» как минимум с 2008 г., то есть не менее чем на протяжении семи лет. Этой находке посвящен доклад, опубликованный на сайте F-Secure.

По словам исследователей, группировка носит название the Dukes (возможно, от английского «герцог» или от имени персонажа Duke Nukem) и представляет собой высокоорганизованную группу глубоко посвященных своему делу хакеров, специализирующихся на кибер-шпионаже и имеющих хорошую базу ресурсов для проведения атак.

В инструментарий «Герцогов» входит большое разнообразие вредоносных приложений, включая PinchDuke, GeminiDuke, CosmicDuke MiniDuke, CozyDuke, OnionDuke, SeaDuke, HammerDuke (другое название — Hammertoss) и CloudDuke (или MiniDionis).

Цели группы

Данные, которые «Герцогам» (другое название группировки – APT29) удается заполучить в результате кибер-шпионажа, помогают правительству России формировать внешнюю политику и политику национальной безопасности, утверждают в F-Secure.

В основном атаки проводятся на страны Запада и западные организации, такие как министерства и агентства, политические научно-исследовательские центры и организации, оказывающие услуги правительственным органам.

Среди целей группировки также – правительства стран СНГ, азиатских, африканских и ближневосточных государств; организации, причастные к экстремизму в Чечне, и лица, связанные с незаконным оборотом контролируемых веществ и наркотических средств.

Тактика атакующих

В последние несколько лет «Герцоги» проводят крупные атаки два раза в год. При этом в течение одной атаки нападению подвергаются сотни и в некоторых случаях даже тысячи организаций, утверждают авторы доклада.

Атаки происходят «налетом» – быстро и в то же время открыто. После взлома хакеры стараются как можно быстрее собрать столько данных, сколько удастся. Если выясняется, что атакуемый объект представляет серьезный интерес, атакующие переключаются на менее заметные методы, позволяющие скрытно выкачивать информацию в течение длительных периодов времени.

Аналитики добавили, что по времени некоторые атаки совпадают с важными событиями в политике России, предшествуя принятию новых решений.

Вредоносный узел Tor и спам во «ВКонтакте»

Исследователи F-Secure утверждают, что хакеры группировки «Герцоги» использовали вредоносный выходной узел анонимной сети Tor для заражения передаваемых через него бинарных файлов. Речь идет об узле, существование которого в октябре 2014 г. обнаружила компания Leviathan Security Group. По словам представителей F-Secure, узел Tor был использован не для того, чтобы проводить атаки, а для формирования ботнета из зараженных компьютеров. Данный ботнет использовался для проведения DDoS-атак (атак типа «отказ в обслуживании»).

Кроме того, один из используемых хакерами вредоносных модулей был предназначен для автоматического постинга сообщений и рассылки спама в социальной сети «ВКонтакте» ***(«Российские хакеры» шпионят за западными правительствами 7 лет // InternetUA (http://internetua.com/rossiiskie-hakeri--shpionyat-za-zapadnimi-pravitelstvami-7-let). – 2015. – 18.09).***

***

Активісти «Правого сектору» зламали сайт студії М. Михалкова «ТРІТЕ».

На головній сторінці сайту розміщено логотип червоного павука і «Правого сектору», – інформує Газета.ру.

Хакерській атаці також піддалися сайти онлайн-кінотеатру студії «Мосфільм», В. Соловйова і С. П'єхи.

На момент написання матеріалу ці сайти були недоступні до перегляду ***(Правий сектор зламав сайт російської студії Михалкова // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2015/09/18/pravyy_sektor_zlamav_sayt_rosiyskoi_studii_myhalkova_625474). – 2015. – 18.09).***