СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(1–14.02)

2016 № 3

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(1–14.02)
№ 3

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 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

4.02.2016
Миллиардная посещаемость: как набрать популярность

Обычно, задумавшись о том, как проекты-миллиардеры по количеству аудитории находят своих фанатов, люди первым делом вспоминают о рекламе. Потом в ход идет такой аргумент как «идея» и «полезность» или, еще лучше – «инновационность». Практически никто не задумывается о том, что все это было и есть, к примеру у такого продукта как Instagram, за пять лет своего существования едва приблизившегося к отметке в 500 млн пользователей, пишет IGate.

Проектом «на миллиард» люди должны пользоваться не менее двух раз в день, это должно стать одной из сотен привычек, управляющих человеком на протяжении его дня. Этот проект должен быть удобен и понятен – ничего лишнего, ничего сложного для понимания. Этот проект должен быть надежен. Вот основные примеры «победы с разгромным счетом на рынке IT».

2013 – YouTube

В 2013 г., спустя восемь лет после запуска, самый известный видеохостинг мира – YouTube – смог перешагнуть желанную веху пользовательского интереса. Месячная аудитория ресурса составила более 1 млрд пользователей. На тот момент это приравнивалось к тому, что каждый второй интернет-пользователь мира посещает YouTube.

На сегодняшний день активная аудитория ресурса крепко удерживает позиции свыше 1 млрд пользователей в месяц, однако по охвату интернет-аудитории YouTube все же немного «сдал» – сейчас его аудитория составляет около трети всех пользователей мировой паутины.

Однако нельзя сказать, что ресурс не развивается – в течение 2015 г. общее время просмотра увеличилось на 60 %, показав самый высокий прирост за двухлетний период, а ежедневная посещаемость увеличилась практически на 40 %.

Нельзя также не отметить прекрасную локализацию видеохостинга: интерфейс YouTube переведен на 76 языков мира, что составляет лингвистический охват более 95 % пользователей Интернета.

2014 – Facebook

В отчетности 2015 г. самая популярная социальная сеть в мире – Facebook – сообщила о достижении порога в 1,5 млрд пользователей за год, а ежедневно в соцсеть заходят более 864 млн пользователей.

При этом первое упоминание о достижении миллиардного порога ежемесячно появилось в далеком 2012 г. Тогда же, когда был зарегистрирован миллиардный пользователь Facebook, и этот факт слегка поколебал

уверенность аналитиков в достижении компанией миллиардного месячного порога именно в 2012 г.

Стоит также отметить, что в конце августа 2015 г. Facebook воспользовались более 1 млрд человек за сутки, что, по сути, является мировым рекордом.

«Сообщество нашей сети продолжает расти, и наш бизнес процветает. 2015 г. был прекрасным годом для Facebook», – заявил по этому поводу основатель соцсети М. Цукерберг.

2016 – WhatsApp

В начале текущего года миллиардную веху удалось перешагнуть еще одному революционному (в прошлом) и весьма удобному (в настоящее время) продукту. Через семь лет после старта сервис WhatsApp присоединился к рекордсменам по посещаемости. А в январе этого года стало известно, что собственник продукта, компания Facebook, решила сделать мессенджер полностью бесплатным.

По данным компании, ежедневно через WhatsApp отправляется 42 млрд сообщений и 250 млн видео.

Нелетающая птичка

Если смотреть на статистику достижения миллиардного порога – то следующей компанией, перешагнувшей за благословенный «миллиард», могла бы стать Twitter.

Однако по итогам III квартала 2015 г. Twitter едва смог набрать 312 млн пользователей.

Если быть честным, следует отметить, что миллиардной отметки по общему количеству пользователей сервису все же удалось достичь, однако удержать и сделать их активными – не получилось.

Нельзя отрицать очевидное

Глядя на историю побед и поражений, следует отметить, что несомненным фактором успеха является своевременность запуска того или иного сервиса. Для примера – вспомните о таком проекте как Friendster. Не вспоминается?.. А жаль.

Friendster – одна из первых социальных сетей в мире, запущенная в далеком 2002 г. Проект не смог завоевать достаточной аудитории, хоть был и вполне хорош для своего времени. Ему банально не хватило пользователей – у слишком малого количества людей были компьютеры.

***

1.02.2016

Facebook добавит возможность поиска попутчиков

Компания Facebook получила новый патент, описывающий систему райдшеринга для пользователей, планирующих посетить одно и то же место, пишет IGate. Такую информацию опубликовало издание Business Insider, ссылаясь на сайт американского Бюро патентов.

Технология предполагает добавление функции поиска попутчиков в Facebook на странице «Мероприятия». Она позволит подписчикам искать попутчиков, для совместной поездки на выбранное событие. Новая опция должна появиться в привычном формате вроде «Собираюсь пойти». По замыслу авторов рядом появятся кнопки «Собираюсь идти и за рулем» и «Собираюсь пойти, но не за рулем».

Если у пользователя имеется автомобиль, он сможет описать подробности – какое количество пассажиров он хочет взять, место и время отправления, а также категорию пользователей, которых он предпочел бы взять с собой – к примеру, только друзья или же друзья друзей.

Издание отмечает, что скоординировавшиеся подобным образом пользователи получат шанс сэкономить средства, уменьшить вред, наносимый окружающей среде, а также познакомиться с новыми людьми.

Функционал сможет подбирать попутчиков, основываясь на их личной информации, образовании, интересах.

Заявку на данный патент Facebook подала 25 июля 2014 г.

***

2.02.2016

В «Одноклассниках» появилась функция перевода денег между пользователями

Российская социальная сеть «Одноклассники» в партнёрстве с банком ВТБ24 запустила сервис денежных переводов между своими пользователями. Пока пользователи могут перевести не более 8 тыс. р., пишет HiTech-News.ru.

Как сообщает «Коммерсантъ», первый перевод на сумму до 500 р. пользователь сможет совершить без комиссии. Затем в течение первых трёх месяцев работы сервиса комиссия за перевод на сумму менее 500 р. составит 30 р. За более крупные транзакции сервис будет снимать комиссию в размере 60 р.

***

2.02.2016

Фейсбук меняет ленту новостей

В администрации Facebook рассказали, что теперь будут учитывать все жалобы и пожелания пользователей, и в ближайшее время изменят настройки для ленты новостей. Как передает replyua.net, в компании заявили, что теперь изменения коснутся обновлений – некоторые из них будут видны только в конце новостной ленты, другие – в самом начале, информирует Экономические известия.

Недавно Facebook проводила опрос среди всех пользователей и попросила оценить содержание новостной ленты. В администрации поинтересовались, как юзеры относятся к рекламе, а также к просьбам

пользователей «лайкнуть» их посты. По словам представителей компании, лента скоро изменится, и у пользователей появятся новые возможности.

В администрации пообещали, что все новости теперь будут классифицироваться, и каждый пользователь сможет увидеть наверху ленты только то, что ему действительно интересно. Представители Facebook рассказали, что без изменений останутся только те настройки, которые позволяли пользователям подписываться на обновления людей, интересующих этих пользователей.

***

3.02.2016

Facebook запустила новую социальную сеть

Компания Facebook открыла доступ к бета-версии социальной сети Facebook at Work. Чтобы создать аккаунт организации в новой соцсети, достаточно будет оставить заявку в специальной форме и пройти процедуру регистрации. Ожидается, что официальный релиз новой социальной сети состоится в ближайшее время, пишет InternetUA.

Корпоративный аккаунт можно будет соответствующим образом стилизовать, например, разместить логотип компании в верхнем левом углу, или выбрать корпоративные цвета в качестве оформления. Ежемесячная плата за доступ к дополнительным функциям составит несколько долларов.

Каждому сотруднику, желающему присоединиться к корпоративному профилю, будет выдан специальный логин и пароль. Возможность импортировать данные из собственной страницы на Facebook не предусмотрена, поскольку разработчики позаботились об отсутствии утечек производственной информации и исключили возможность синхронизации.

Пользователей по-прежнему ожидает лента новостей, возможность ставить лайки, создавать группы для совместных проектов и делиться ссылками. Но, например, игры в Facebook at Work уже не предусмотрены.

Информация о запуске Facebook at Work появилась в начале декабря 2015 г., однако бета-тестирование соцсети ведется уже с января 2015 г. В течение пробного периода доступ к сервису можно было получить только по специальному приглашению. Возможности новой социальной сети протестировали такие компании, как Maximum, Heineken, Royal Bank of Scotland и др.

Корпоративные социальные сети уже давно пользуются популярностью у крупных компаний. Так, в 2012 г. Microsoft приобрела соцсеть Yammer за 1,2 млрд дол. Сетью пользовались более 200 тыс. компаний, включая таких гигантов, как eBay и Groupon.

***

4.02.2016

Facebook в честь своего 12-летия предложил вспомнить о друзьях

Facebook запустила новую функцию, которая автоматически создает персонифицированные видеоподборки о друзьях пользователя. Об этом говорится в сообщении компании. Таким образом соцсеть отметила свое 12-летие, которое наступило 4 февраля 2016 г., пишет InternetUA.

Опция получила название «День друзей». Предложение воспользоваться ею, как правило, появляется вверху новостной ленты. Можно выбрать автоматическое создание клипа из фотографий с друзьями либо вручную подобрать снимки.

Новая услуга схожа с функцией «Обзор года» (Year in Review), которая формирует видеоролики о самых важных событиях пользователя на основе записей на его странице, опубликованных за ушедший год.

***

4.02.2016

Twitter тестує кнопку для вставки GIF зображень

Twitter почала тестувати нову кнопку в мобільному додатку, яка відповідає за вставку gif-анімації, передає портал BUBLBE.COM.

Кнопка GIF була розміщена праворуч від значка камери в мобільному додатку Twitter, що працює на операційній системі Android. Нова кнопка з'явилася на деякий час і не у всіх користувачів програми.

Один з користувачів Twitter Ф. Перлман розповів, що натискання на кнопку GIF дає можливість вибрати або свою gif-картинку, або шаблонну. Ф. Перлман розмістив скріншот на своїй сторінці, проте незабаром кнопка зникла з його додатку. Він не єдиний, у кого з'явилася кнопка gif-анімації, а потім зникла.

У листопаді минулого року сервіс мікроблогів Twitter відважився на зміну дизайну програми. Twitter відмовилася від кнопки «Додати в обране» і замінила її кнопкою «лайку». Представники компанії відзначили, що кнопка «Додати в обране» бентежила нових користувачів, які звикли до «лайків» в інших соціальних мережах.

***

5.02.2016

Глава Facebook рассчитывает увеличить аудиторию соцсети до 5 млрд к 2030 году

Глава и основатель Facebook М. Цукерберг объявил о намерении увеличить аудиторию своей соцсети до 5 млрд человек к 2030 г. Об этом пишет IGate со ссылкой на USA Today.

«Мы хотим подключить всех [к соцсети], мы собираемся сделать это при помощи властей и компаний по всему миру», – заявил М. Цукерберг во время

мероприятия, посвященного 12-летию компании. По его словам, цель Facebook – «подключить 5 млрд из 7 млрд людей на планете».

По оценке ООН, население Земли к 2030 г. возрастет до 8,5 млрд человек.

***

5.02.2016

Количество сообщений в соцсети «ВКонтакте» впервые превысило 5 млрд в сутки

Количество личных сообщений в социальной сети «ВКонтакте» превысило 5 млрд в сутки. Об этом сообщил операционный директор компании А. Рогозов, пишет IGate.

«“ВКонтакте” традиционно лидирует среди мобильных приложений в России, опережая все известные социальные сети и мессенджеры. Это подтверждается как нашими собственными данными, так и независимым измерителем – компанией TNS», – отметил А. Рогозов.

Согласно исследованию TNS, на которое ссылается А. Рогозов, по состоянию на декабрь 2015 г. «ВКонтакте» лидировала среди мобильных приложений в городах с населением более 700 тыс. человек. Средняя дневная аудитория приложения «ВКонтакте» составила 6,8 млн пользователей. Вторую строчку занял мессенджер WhatsApp с 4,4 млн, на третьей строчке расположился фотосервис Instagram с аудиторией в 3,5 млн человек.

По данным исследовательской компании J’son & Partners Consulting, которая проводила онлайн-опрос среди пользователей смартфонов в городах-миллионниках в июне 2015 г., самым популярным мессенджером является Viber (доля 61 %). Вторым по популярности стал WhatsApp (49 %). Третью строчку занял лидировавший в 2013 г. Skype.

В пятерку мессенджеров-лидеров, по версии J’son & Partners Consulting, также вошли соцсети «Одноклассники», «ВКонтакте» и Facebook Messenger.

***

6.02.2016

Instagram позволит переключаться между аккаунтами

В Instagram появится функция переключения между несколькими аккаунтами. Об этом сообщает Tech Insider, пишет InternetUA.

Пользователь сможет получать уведомления о подписках, лайках и комментариях сразу со всех учетных записей. Пока опция доступна некоторым пользователям в тестовом режиме. Возможность переключаться между несколькими аккаунтами без выхода из них в первую очередь необходима владельцам рекламных и профессиональных страничек в соцсети.

***

10.02.2016

Twitter сделал ленту новостей похожей на Facebook

Twitter поменяла алгоритмы ленты новостей, говорится в блоге компании. Теперь твиты отображаются не в хронологическом порядке, а исходя из интересов пользователя. Похожий принцип использует Facebook, пишет InternetUA.

Компания не поясняет, по каким именно параметрам проходит отбор лучших твитов, которые должны отображаться в самом верху новостной ленты. Однако отмечается, что это будут «самые важные сообщения тех людей, на которые вы подписаны». Остальные сообщения будут располагаться ниже.

Пока что нововведение опционально: функция «Показывать сначала лучшие твиты» включается в настройках аккаунта. Ожидается, что в ближайшие недели эту возможность выбора уберут.

Twitter приступила к тестированию нового формата ленты новостей в начале декабря 2015 г. После появления слухов о возможном нововведении пользователи сервиса вывели в мировой топ хештег #RIPTwitter. Основное недовольство вызвал тот факт, что сервис станет похож на Facebook, использующий схожий алгоритм.

Для сравнения, Facebook при построении ленты ставит в приоритет посты ближайших друзей и наиболее интересующие пользователя страницы, которые можно указать в настройках.

***

11.02.2016

Twitter впервые за два года потерял аудиторию

Число активных пользователей Twitter в IV квартале 2015 г. снизилось на 2 млн. Это первое сокращение аудитории сервиса с 2013 г., сообщает CNN Money со ссылкой на данные компании, пишет InternetUA.

В октябре – декабре предыдущего года число пользователей соцсети в среднем составляло 305 млн человек в месяц, в то время как в предыдущем квартале оно равнялось 307 млн. Число пользователей, хотя бы раз в месяц заходящих в Twitter, составило порядка 320 млн, что соизмеримо с показателями III квартала (на 9 % выше показателей того же периода 2014 г.).

***

12.02.2016

MySpace стал собственностью издательского дома Time Inc.

94-летний издательский дом приобрел социальную сеть MySpace. Приобретение позволит Time Inc получить доступ к данным пользователей, нарастить рекламные технологии и «качество» контента. Социальная сеть

MySpace была обновлена в 2013 г., чтобы сфокусироваться на музыке, получив инвесторов-знаменитостей, таких как Д. Тимберлейк. В январе 2015 г. платформа насчитывала 50 млн ежемесячных пользователей, пишет Marketing Media Review.

***

13.02.2016

В мессенджер Facebook встроят поддержку СМС

Компания Facebook сделала еще один шаг на пути превращения Messenger в универсальное средство коммуникации, способного подменить собой все прочие сервисы для общения. Как сообщает VentureBeat, инженеры соцсети тестируют новую функцию в Android-версии мессенджера, которая позволит читать и отправлять СМС, пишет InternetUA.

Однажды Messenger уже был интегрирован с СМС, однако эта возможность была убрана в ноябре 2013 г. Тогда представители Facebook пояснили, что новая функция «просто не взлетела».

В настоящее время чтение и отправка СМС в Messenger доступна очень ограниченному кругу пользователей Android-смартфонов в США. На наличие этой функции указывает новый пункт Change SMS App («Изменить приложение для СМС») в настройках приложения.

Помимо этого, компания тестирует возможность добавления нескольких учетных записей к Messenger. Между ними можно будет легко переключаться, не выходя из программы. Новая функция облегчит жизнь людям, вынужденным пользоваться одним устройством, а также крупным брендам и SMM-специалистам, которым приходится поддерживать множество аккаунтов

***

13.02.2016

В Instagram появилась еще одна полезная функция

В ближайшем будущем пользователи Instagram получат доступ к еще одной полезной функции – им станет доступна информация о количестве просмотров опубликованных ими видеороликов. Сообщение об этом опубликовано в официальном блоге фотосервиса, пишет InternetUA.

По словам разработчиков, новая возможность будет развернута для всех пользователей Instagram в течение ближайших нескольких недель.

Информация о числе просмотров видео будет видна на том месте, где раньше размещалось поле информации о количестве поставленных зрителями лайков. Для того чтобы узнать, сколько человек нажали кнопку «нравится», пользователю нужно будет нажать кнопку View.

***

14.02.2016

В Facebook добавили кнопку для отправки сообщений-валентинок

В честь Дня святого Валентина в Facebook появилась специальная кнопка для отправки сообщений-валентинок. Об этом сообщают пользователи Reddit, пишет InternetUA.

По их утверждениям, в мобильном приложении Messenger появилась кнопка с пронзенным стрелой сердцем. Нажав на нее, можно написать сообщение и красиво оформить его с помощью анимации. Получателю оно придет в виде конверта с подарочной ленточкой, который он может открыть при нажатии на послание.

Судя по отзывам пользователей Reddit, опция работает в версиях Messenger для iOS и Android. Сообщения также можно открыть и на десктопной версии Facebook.

***

14.02.2016

Twitter упростит систему ответов и другие функции в сервисе

Сервис Twitter, как недавно стало известно, в финансовом плане переживает не самые лучшие времена. Поэтому компания заявила инвесторам, что одна из ключевых особенностей социальной сети – возможность вести диалог с другим пользователем – неудобна и будет переосмыслена, пишет InternetUA.

«Мы собираемся починить разбитые окна и запутанные детали вроде синтаксиса .@имён и @правил ответа, которые, как мы знаем, тормозят использование сервиса и отталкивают людей», – говорится в письме, адресованном инвесторам Twitter. Также компания собирается улучшить процесс приспособления к сервису новых пользователей, ускорить процесс создания «твитов», а также позволить людям быть более выразительными в плане текста, фотографий и видео. «Беспрестанное обновление Twitter позволит большему количеству людей получать из Twitter больше и быстрее».

Позже генеральный директор Twitter Д. Дорси подтвердил намерение компании доработать систему ответов в сервисе. «В плане диалогов у нас какие-то на самом деле странные правила, – заявил он. – Никто ничего не понимает, и нам просто нужно исправить это». Он также упомянул процесс адаптации к социальной сети, назвав его «неидеальным» и пообещав изменить то, как люди будут приспосабливаться к платформе в первые несколько недель.

Пока не ясно, как именно изменится система ответов в Twitter, особенно если учесть, как она уже укоренилась в сервисе. Тем не менее о реорганизации ленты компания уже говорила неоднократно, поэтому все намеченные планы тем или иным образом в любом случае должны быть реализованы.

***

12.02.2016

Кисіль К. Соціальні мережі для читачів – право на власну територію

Віртуальні книжкові полиці, каталогізація прочитаного й «букчеленджі» – читацькі соціальні мережі стають не лише корисним практичним інструментом, а й майданчиком для популяризації молодих авторів і читання загалом, пише MediaSapiens.

Чимдалі менше наше життя можна уявити без участі соціальних мереж. Це стосується й читання. Панацеєю та затишним майданчиком для профільного спілкування стали нішеві соцмережі. Попри те, що Facebook намагається замінити все: від медійних видань до форумів, – популярність таких майданчиків не зменшується.

Читацькі соціальні мережі умовно поділяються на соцмережі-каталоги з активними соціальними функціями, тобто спілкуванням читачів між собою та авторами, та на соцмережі-бібліотеки, які пропонують безкоштовно або за фіксовану плату доступ до книжок на сайті.

Однією з найбільш відвідуваних соцмереж (40 млн користувачів) для читачів залишається ***Goodreads***. Існування такого майданчика дало читачам те, чого вони не мали раніше, – окремої платформи.

Г. Ткачук, письменниця: «Я використовую сервіс Goodreads, по-перше, для систематизації прочитаного. Це моя електронна книжкова полиця, на якій збираю всі прочитані книжки, оскільки таку аналогову полицю-шафу-кімнату мати неможливо. Різні полички й теги допомагають швидко зорієнтуватися в тому, що я читала з певної теми, для певної вікової категорії чи з певної національної літератури. Я читаю паперові книжки, електронні з kindle, із ноутбука, крім того – слухаю аудіокниги. Тож дуже зручно мати на смартфоні додаток, який організовує моє читання, не дає забути, що я читаю зараз (бо це завжди кілька книжок паралельно) і що планую прочитати згодом. Як автору мені цікаво і приємно, коли читачі ставлять оцінки моїм книжкам, діляться враженнями. Однак найбільше мене дивують теги, надані моїм книжкам, і добірки, у котрі вони (книжки) потрапляють. Наприклад, минулого року я нагуглила таке: на російському читацькому сервісі LiveLib, де чималий сегмент української літератури, мою книжку “Вечірні крамниці вулиці Волоської” додано до підбірки “А мені фіолетово” (за кольором обкладинки), а також їй надано тег “Місто зсередини”».

Майже повною копією американської мережі Goodreads є російська мережа ***LiveLib.ru***. Перша виграє в естетичній та функціональних категоріях. Друга – за відсутності знання англійської. Сайт Goodreads повністю англомовний. Проте базового рівня мови для зручного користування має вистачити з головою. У LiveLib.ru серед учасників розігрують подарункові книжки. У Goodreads є окрема поличками з безкоштовними електронними книжками, на які відкривають доступ на певний період. Тобто ці соцмережі також частково стають бібліотеками.

Однією з базових функцій першої категорії читацьких соцмереж є каталогізація прочитаного. На перший погляд не така важлива річ. Але для людини, яка читає багато, стає істотним фіксування прочитаних книжок, щоб не загубити, не забути прочитаної інформації. Goodreads надає можливість до наявної бази, яка переважно складається з англомовної літератури, додавати нові книжки. Так, база за останні роки помітно поповнилася україномовними виданнями та перекладами. Процес не займає багато часу й не потребує особливих зусиль.

Така мережа може виступати в ролі й однієї з найбільших мрій книголюбів – заснування власної домашньої бібліотеки. Дарма що віртуальної. На сайтах можна створювати категорії-полички на власний смак – за жанрами, мовою видання чи перекладу, специфічними вподобаннями й інтересами. Така функція присутня майже в кожній соціальній мережі для читачів. Обов'язковими є зазвичай три полички – та, на якій розташовано книжки, які наразі читаєш, поличка з прочитаними книжками і з книжками, які хочеш прочитати.

Прочитаним книжкам можна ставити оцінки-зірочки та писати на них відгуки, за оцінками яких будується загальний рейтинг читача. Туди ж зараховуємо й участь у форумах, обговореннях, онлайн-зустрічах із авторами, участь в опитуваннях та вікторинах.

Як і в будь-який соціальній мережі, у читацькій можна (і треба) відстежувати діяльність друзів – тим самим стежачи за їхніми відгуками на книжки, беручи участь в обговореннях. Система соцмережі налаштована так, щоб радити учасникам книжки, базуючись на вмісті їхніх поличок.

Але такі соцмережі є не лише читацьким простором, а й у ширшому розумінні літературним майданчиком. Не так давно в Goodreads відкрили окрему рубрику для публікування творів молодих авторів. Усі охочі можуть опублікувати для читання й отримати схвалення у вигляді лайків чи коментарів.

Для письменників є окрема база, де можна завести власну сторінку з біографією та виданими книжками. Через неї надається можливість спілкуватися з читачами, започатковувати дискусії та організовувати онлайн-чати.

Орієнтованою саме на молодих авторів є мережа ***WattPad***. Засновники на початку надали доступ до 17 тис. класичних книг, а також зробили платформу для публікації коротких творів початківців. Тепер на сайті у відкритому доступі близько 10 млн книжок. Учасники обговорюють роботи одне одного та спілкуються з письменниками.

Ще одним прикладом соцмережі-бібліотеки є російська мережа ***Bookmate***. Платформа є фактично електронною приватною бібліотекою. Доступ до книжок платний. Є дві пропозиції – стандартна й розширена. Читачі, купуючи абонемент на місяць або рік, отримують доступ до класики й новинок. Переважна більшість книжок російською мовою. Є також книжки англійською, іспанською, індонезійською, данською та іншими мовами. Але асортимент

бідний. Проте саме такий вид бібліотеки є найбільш реальною альтернативою класичним бібліотекам. А також дієвим способом боротьби з піратством.

Bookmate від самого початку запрограмований на читання через пристрої (смартфони й планшети). Має багато рубрик, на кшталт поради від відомих критиків для читання або добірки оповідань для швидкого читання у транспорті. Тематичну добірку може створити кожен учасник мережі.

З кінця минулого року і в українському соцмедійному просторі стартував процес «розкручування» читання. Активно на нього вплинув проект письменників К. Бабкіної та М. Лівіна ***Bookchalleng_ua***. Так звані букчелендж-виклики щороку проводять і соцмережі для читачів. Тут кожен собі сам може обрати ту кількість книг, які він хоче прочитати за рік. Система періодично нагадуватиме про плани, демонструватиме у відсотках його виконання. А в кінці можна буде отримати інфографіку всього прочитаного за минулий рік. Дуже зручна річ, беручи до уваги, що візуальна інформація набагато краще сприймається та запам'ятовується. Крім приводу похизуватися, це також і привід замислитися, скільки, а головне що ти читаєш. Цього року читацькі челенджі в мережі Goodreads встановили більш як мільйон читачів.

Однією із суттєвих і ще повністю не зауважених видавництвами функцій соціальних мереж для читання є промоція книжок. Масовий читач не завжди орієнтується на високочолих критиків чи поважні видання, йому важливіше цілковитий збіг у смаках. Тож ми часто звертаємося з проханням про поради до друзів і людей, яким довіряємо. Саме цю функцію соцмережі можуть задовольнити на найвищому рівні.

Соціальні мережі для читання є дуже комфортним місцем для читачів, які не шукають професійної критики, не надто пильно стежать за літературним процесом, проте багато читають і люблять говорити про книжки. Тут можна знайти й однодумців, і близькі до власних інтересів книжки, і власне той читацький простір, якого не вистачає, нарешті, соціальних майданчиків.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

8.02.2016

Новости Верховной Рады: парламент заявил, что «с головой» уходит в соцсети, чтобы быть ближе к народу

Верховная Рада Украины зарегистрировала официальные страницы в социальных сетях, пишут Украинские реалии.

Верховная Рада Украины завела официальные аккаунты в социальных сетях, передает Joinfo.ua со ссылкой на пресс-службу Аппарата парламента.

«В рамках программы модернизации парламента Верховная Рада Украины активизирует свое присутствие в мировых социальных сетях – Facebook, Twitter, Google+ и Instagram», – сказано в сообщении.

«Наша цель – превратить официальные страницы парламента в социальных сетях в площадки информирования, общения и обмена мнениями между гражданами и высшим законодательным органом страны», – объяснили в Верховной Раде.

Теперь оперативные, актуальные и достоверные новости о работе Верховной Рады доступны каждому пользователю социальных сетей. «Это информационные сообщения о ходе пленарных заседаний, анализ важнейших законодательных актов, позиции ведущих политических сил, международные отношения парламента, освещение происходящих в организации его работы, актуальные интервью», – говорится в пресс-релизе.

«Новый формат общения поможет журналистам, общественным активистам и всем гражданам Украины лучше сориентироваться в повседневной деятельности Верховной Рады и получить необходимую информацию.

Широкий выход украинского парламента в социальные сети – важный шаг к открытости и публичности власти, что является непременным условием возврата им доверия со стороны общества. Присоединяйтесь!» – призывают в парламенте.

***

11.02.2016

Голова Печерської райдержадміністрації відкрив для жителів групу у Viber зі своїм номером телефону

Відтепер печеряни зможуть особисто звернутися до голови Печерської районної в місті Києві державної адміністрації С. Мартинчука через створену мобільну групу в популярному месенджері Viber, пише MediaSapiens.

«Фактично я створив для своїх мешканців цілодобову і оперативну “гарячу лінію”, використовуючи свій мобільний номер телефону в месенджері Viber, за допомогою якої печеряни зможуть залишати свої звернення з описом конкретної проблеми або побажання, додавати фото- та відеоматеріали. Всі звернення я буду розглядати особисто та гарантую миттєву реакцію і зворотний зв’язок», – повідомив С. Мартинчук.

Також представник Президента України в Печерському районі міста Києва повідомив, що це вже не перший досвід створення інтерактивних проектів для зворотних зв’язків з жителями Печерського району.

Нагадаємо, що в соціальній мережі Facebook створена офіційна сторінка Печерської районної в місті Києві державної адміністрації, на якій розміщена інформація про діяльність райдержадміністрації, про заходи та події, що відбуваються на території району та ін.

Також у мережі Instagram діє акаунт очільника Печерського району (@sergey_martynchuk), через який С. Мартинчук нещодавно оголосив флешмоб: «Оціни роботу комунальних служб з прибирання снігу у центрі Києва».

Для того, щоб приєднатися до публічного чату в месенджері Viber, необхідно залишити повідомлення на офіційній сторінці Печерської РДА в соціальній мережі Facebook із зазначенням свого мобільного номеру телефону та фактичного місця проживання, а також можна залишити своє повідомлення або коментар в акаунті голови Печерської райдержадміністрації С. Мартинчука в мережі Instagram (@sergey_martynchuk).

***

6.02.2016

У США досліджують активність українців у соцмережах під час Майдану

Дослідники з Університету Сан-Дієго (США) проводять ґрунтовне опитування, щоб вивчити активність українців у соціальних мережах під час і після подій Євромайдану, передає Persha.kr.ua з посиланням на VIDIA.

Опитування має на меті дослідити онлайн-активність українців, що проживають за кордоном, під час подій Революції гідності. А також – як вона змінилась у постмайданний період.

Одна з дослідниць С. Красинська в коментарі VIDIA зазначила, що важливо, аби якомога більше людей взяли участь у дослідженні – тоді його результати були ґрунтовнішими.

У сфері наукових інтересів С. Красинської – громадянське суспільство України, а особливо його неформальні організації та ініціативи, неприбуткові організації у Східній Європі, зокрема й Україні. На її рахунку – чималий список публікацій на цю тематику.

Дослідниця каже, що університет постійно підтримує усі суспільні і наукові починання, які пов’язані з українською тематикою.

За підсумками дослідження будуть підготовані наукові статті. Результати буде представлено на різноманітних наукових платформах.

***

5.02.2016

Байден створив аккаунт у Facebook

Віце-президент США Д. Байден обзавівся акаунтом у соціальній мережі Facebook і опублікував свій перший відеозапис.

Про це повідомляє LB.ua з посиланням на ТАСС.

«Ласкаво прошу на мою сторінку у Facebook, – привітав він користувачів. – Віце-президент США вперше обзавівся нею. Я хотів би, щоб вона стала місцем, де ми можемо говорити безпосередньо про проблеми, які мають значення для нас усіх».

Соцмережу Д. Байден назвав «вражаючим форумом для конструктивних дебатів, який потрібно використовувати з ентузіазмом».

Віце-президент приурочив реєстрацію в соцмережі до Всесвітнього дня боротьби проти раку. Д. Байден очолює спеціальну робочу групу боротьби з раковими захворюваннями.

***

11.02.2016

Папа Римский обратился к пастве через Telegram

Приход церкви в городе Помпеи (Италия) запустил канал в Telegram, в котором публикуются сообщения от Папы Римского Франциска. Об этом пишет InternetUA.

Канал в Telegram можно найти под аккаунтом @pgpompei, а сам блог Папы Римского озаглавлен Keep Lent («Соблюдай пост»). Помимо различных сообщений от главы католической церкви, в чате также появляются аудиозаписи, на которых Франциск зачитывает вслух стихи из Евангелия. Подписчиками канала стали уже более 3600 человек, отмечает портал.

В первом посте Папа Римский призвал совершать хорошие поступки и не ждать одобрения со стороны, так как «это заставляет нас концентрироваться на том, что думают о нас другие».

Открытие канала в мессенджере приурочено к Пепельной среде, которая отмечается 10 февраля и знаменует начало поста перед Пасхой.

В 2015 г. сообщения от Папы Римского распространялись через WhatsApp. Подписчиков прошлогоднего чата организаторы призвали переходить на Telegram, отметив, что он «как WhatsApp, но только лучше»

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

5.02.2016

Instagram запускает видеорекламу длительностью 60 секунд

Instagram представляет новый формат рекламы – промовидео длительностью 60 секунд, сообщает МедиаБизнес.

Сам по себе формат не стал новинкой: в социальном сервисе и ранее существовала возможность запускать видеорекламу длиной 15 и 30 секунд. Однако партнёры Instagram не раз жаловались на издержки функционала, который не позволяет им транслировать полноценное видео. В результате, представители социального сервиса приняли решение увеличить длительность ролика до 1 минуты.

Первыми рекламодателями, пожелавшими протестировать новый формат, стали T-Mobile и Warner Brothers. Предполагается также, что новый рекламный формат будет востребован среди продавцов популярных потребительских товаров.

Запуск нового формата стал ответным шагом Instagram на решение ближайшего конкурента Twitter'а расширить доступ к видеорекламе формата pre-roll. Продукт позволяет рекламодателям, издателям и брендам показывать пользователям сервиса микроблогов видеоклипы событий практически в режиме реального времени. Буквально неделю назад в Twitter'е появились 30-секундные видеоролики формата pre-roll. Через 6 секунд просмотра рекламу можно пропустить.

***

6.02.2016
Western Union внедряет переводы через Viber

Один из самых известный сервисов по переводу денежных средств, компания Western Union сообщила о партнерстве с мессенджером Viber. Данная сделка позволит переводить средства прямо в чате во время переписки, пишет IGate.

Пользователей Viber по всему миру насчитывается более 664 млн, так что соглашение будет выгодно обеим сторонам. В ближайшее время приложение на API-платформе Western Union Connect, позволяющее переводить деньги через мессенджер, будет доступно жителям США.

С проблемой переводов денежных средств сталкивается много людей, оказавшись за границей. Ведь банки чужих стран берут немалые комиссии за международные денежные переводы. Создание такого приложения позволит сэкномить, находясь в другой стране.

Американская компания Western Union является самой большой в своем роде и имеет более 500 тыс. отделений во всем мире. Однако в последнее время у нее появилось немало конкурентов, таких как Azimo, WorldRemit и TransferWise, предлагающих лояльные условия и более низкие проценты. Вероятно, в связи с этим WU и решили сделать «ход конем» и заключить партнёрскую сделку с одним из самых крупных месенджеров.

На начальном этапе проекта только пользователи Viber в Соединенных Штатах Америки смогут использовать такой вариант денежных переводов, отправляя до 499 дол. в любую страну мира.

Также существует ряд нюансов при переводе денежных средств, на которых компания Western Union не акцентирует внимания. Например, при переводе курс будет отличаться от реального, а в интерфейсе программы курс перевода нигде не указывается. В самой компании такую ситуацию объяснили отсутствием места в интерфейсе программы, хотя место для размещения можно найти.

Ну а насколько такой сервис приживется и как будут реагировать конкуренты, покажет только время.

***

10.02.2016

Эра персональности: как использовать мессенджеры в бизнесе?

Сегодня мессенджеры называют «новыми социальными сетями». Развитие мобильного Интернета прибавило популярности подзабытым чатам в новом формате. Сегодня через них прокачиваются огромные объемы трафика, люди делятся ссылками, смотрят видео, общаются в группах по интересам. Основатель агентства контент-маркетинга CMdigital С. Коноплицкий рассказывает, для чего брендам мессенджеры и как их использовать, пишет AIN.UA.

Несмотря на разнообразие социальных сетей – прекрасных площадок, чтобы общаться, узнавать что-то новое и убивать время – у пользователей остается потребность делиться информацией с небольшой группой знакомых людей. Эту нишу занимают мессенджеры, которые уже совершили маленькую мобильную революцию, постепенно вытесняя привычные смс-сервисы мобильных операторов. Сегодня на телефонах украинцев можно видеть WhatsApp, Facebook Messenger, Google Hangouts, Skype, Line, Viber, ICQ и другие, более редкие приложения.

По данным аналитической компании eMarketer, мессенджеры используют три четверти всех пользователей смартфонов. Рост за 2015 г. составил 31,6 %. В 2018 г. пользоваться мессенджерами будут уже 2 млрд человек (80 % обладателей смартфонов).

Другие исследования говорят, что пользователи заглядывают в смартфон около 220 раз в день, а сообщения занимают у них первое место по популярности, обгоняя карты и соцсети.

По результатам iVOX Ukraine, самый высокий уровень проникновения у Skype. Им пользуются 78 % украинцев, для 46 % это любимый мессенджер. На втором месте Viber: 56 % респондентов отметили, что время от времени общаются с его помощью, 32 % являются приверженцами этого приложения. Messenger от Facebook занимает третью позицию. Среди юзеров приложения 29 % украинских интернет-пользователей, 8 % выбирают его в качестве основного приложения для обмена сообщениями через Интернет.

Естественно, что маркетологи по всему миру ищут варианты «достучаться» до аудитории мессенджеров, ведь канал связи в непосредственной близости к потребителю круглые сутки.

Mobile chat poster

На Западе использование мессенджеров в маркетинге более развито. Заметив этот тренд, Facebook в прошлом году «отвязал» Facebook Messenger от социальной сети и позволил новым пользователям регистрироваться с помощью номера телефона. М. Цукерберг тогда заявил, что хочет соединить

пользователей с магазинами, ресторанами и другими услугами. Еще ранее в мессенджер добавили такие полезные для работы с клиентами функции, как возможность перечислять деньги друзьям, делиться местоположением, обмениваться видео и изображениями, а также видеозвонки.

Как же использовать этот инструмент персонального маркетинга?

Реклама

Если отключить фантазию, то первое, что приходит на ум – это бомбардировка несчастных пользователей рекламными сообщениями. На выходе получаем обычный спам, но с более низкой эффективностью. Более того, уровень раздражения у пользователя от такой рекламы существенно выше, ведь происходит «несанкционированное вторжение» практически в личное пространство.

Для 40 % опрошенных iVOX Ukraine реклама в мессенджерах – раздражающий фактор, который отвлекает от общения. Не приемлют рекламу в любых ее проявлениях 16 % респондентов. 23 % относятся к коммерческим сообщениям положительно, если информация полезна и актуальна. 12 % опрошенных готовы терпеть рекламу, если это залог бесплатного пользования приложениями. 60 % участников исследования отметили, что вовсе не обращают внимания на рекламу в мессенджерах.

Но стоимость рекламы в мессенджерах – 6–8 коп. за одно сообщение и находятся немало желающих экспериментировать.

Чтобы использование такого канала, как мессенджеры было эффективным, нужно подойти к нему со стороны пользователя. Что человек ожидает от коммуникации с брендом, и почему потребителю будет интересно поддерживать общение с ним таким образом?

Зачем?

Это главный вопрос при планировании чего угодно в мире интернет-маркетинга. Вопрос, который обозначает цели и задачи. Вопрос, на который можно получить неожиданный ответ – «не знаю». Зачем использовать инструмент, если он не нужен? Но если все-таки нужен, тогда пусть на этот вопрос ответит потребитель. «Зачем мне связь с брендом через мой любимый мессенджер?»

Если обобщить все возможные варианты ответов, то основными будут два: получение информации и поддержка.

Теперь посмотрим, как бренд может использовать эти ожидания клиентов.

Предложение информации

Основной инструмент для инициации общения в мессенджерах, со стороны бренда – это push-оповещения. Для передачи сообщений, необходимо согласие клиента, его желание получать требуемую информацию по этому каналу. Иначе компания рискует получить негативное отношение и репутацию спамера. Также не стоит использовать этот канал слишком часто и по пустяковым поводам. Это может вызвать раздражение. При отправке сообщений нужно учитывать, что это, прежде всего, мобильный канал.

Возможно, что ваша CRM имеет большой объем данных о клиенте, и вы можете прогнозировать, что по выходным хозяин этого смартофна часто бывает в торговых центрах или ресторанах, а может быть сейчас он заграницей. Отправлять сообщения, в соответствии с поведением пользователя – это та заветная персонализация, способная максимально сблизить бренд с потребителем.

Поддержка

Боязнь говорить по телефону – одна из самых распространенных социофобий. В век Интернета все меньше причин бороться с ней, а значит, количество людей, предпочитающих альтернативные способы связи, в том числе и мессенджеры, будет расти.

Кроме того, очень удобно узнать, например, информацию о заказе, статус покупки, данные о новинках продукции в режиме чата. Короткий и лаконичный стиль чат-общения прекрасно подходит для нашего быстрого века.

Скажем, один из популярных мессенджеров, Telegram, созданный основателем социальной сети «ВКонтакте» П. Дуровым, предлагает API для компаний, многие из которых уже реализовали интересные решения для клиентской поддержки. Например, виртуальная АТС передает бесплатные «уведомления о пропущенных звонках» в приложение. В прошлом году в Telegram была открыта платформа ботов. Боты – обычные аккаунты Telegram, которыми управляют не люди, а программы. Они могут преподавать, играть, искать информацию, транслировать сообщения на широкую аудиторию, напоминать о событиях, подключаться к другим сервисам, даже передавать команды в интернет вещей. Клиент может добавить в свой аккаунт бота, чтобы получать полезную информацию.

Сегодня мессенджеры отлично используются в продажах малого бизнеса, салонов одежды, красоты, СТО и пр. Потребитель может запросить фото товара, информацию о времени работы, поучаствовать в конкурсе.

Чтобы поддержка была идеальной, нужны идеальные скрипты для менеджеров, с учетом того, что это мобильная технология и человек может находиться где угодно и, как правило, рассчитывает не на долгие вовлекающие разговоры, а на четкий и быстрый ответ.

Главный принцип использования мессенджеров в маркетинге – удовлетворять потребности клиентов и ничего не навязывать. Тогда у вас будет канал с уникальной персонализацией.

***

11.02.2016

В видеорекламе на Facebook появится возможность автоматического добавления субтитров

Facebook представила несколько нововведений, призванных повысить эффективность видеорекламы в социальной сети, пишет Состав.ua.

В их числе:

Автоматическое добавление субтитров к видео

Ранее такая возможность уже была доступна рекламодателям, но им приходилось встраивать субтитры в видео или же загружать их отдельным файлом.

В скором времени можно будет выбрать опцию автоматического добавления субтитров. Новый инструмент сгенерирует субтитры во время создания видеообъявления, после чего рекламодатели смогут их отредактировать и сохранить.

В ближайшие недели эта функция будет запущена по всему миру в Ads Manager и Power Editor. На первых порах субтитры будут доступны только на английском языке.

Завершена интеграция с Moat

В сентябре Facebook объявила о сотрудничестве с аналитической компанией Moat с целью получения сторонней статистики для видеорекламы. Теперь интеграция запущена в мировом масштабе. Moat будет производить измерения просмотров и их длительности для рекламных видео в Facebook.

Facebook также работает с Millward Brown и Nielsen над получением сторонней статистики измерений не только для видеорекламы, но и брендовых кампаний.

Оплата за фактические просмотры видеорекламы

Рекламодатели теперь смогут платить только за фактические просмотры видеорекламы. Данные о просмотрах будут предоставляться Moat. Эта возможность появилась в сентябре 2015 г., теперь она доступна всем рекламодателям.

Советы по улучшению эффективности мобильных видео

Компания также поделилась рекомендациями, как получить максимальную отдачу от мобильных видеокампаний. Советы основаны на внешних и внутренних исследованиях того, как пользователи потребляют видеоконтент социальной сети.

Ниже – основные результаты этих исследований:

– более 100 млн часов видео пользователи смотрят ежедневно;

– на мобильных устройствах люди потребляют контент быстрее, чем на десктопах;

– 47 % стоимости видеообъявления приходится на первые три секунды просмотра;

– 74 % – на первые 10 %;

– 80 % пользователей негативно реагируют на видеорекламу, которая запускается со звуком;

– 41 % видеороликов не имеет смысла без звука;

– время просмотра видео с субтитрами возросло в среднем на 12 %.

Рекомендации:

– устанавливайте контакт сразу же, чтобы захватить внимание зрителя в первые секунды просмотра;

– создавайте видео, которые можно смотреть без звука;

– продолжайте экспериментировать, поскольку единого эффективного решения для всех компаний не существует.

Напомним, что в ноябре 2015 г. количество просмотров видео в Facebook достигло 8 млрд в день. Число рекламодателей компании на конец года составило 2,5 млрд. Количество предприятий малого бизнеса, представленных в социальной сети, достигло 50 млн.

***

11.02.2016

Twitter запустил премиум-формат видеорекламы First View

Twitter представила новый рекламный формат First View, который позволяет разместить промовидео компании вверху новостной ленты пользователей. Ролик будет виден при первом открытии сервиса в течение 24 часов после его публикации. Новая опция премиум-размещения призвана дать компаниям возможность выделиться среди других объявлений и сделать свою рекламу заметнее в ленте, сообщает МедиаБизнес со ссылкой на searchengines.ru.

Оплата с рекламодателей будет взиматься, начиная с третьей секунды просмотра ролика. Видео проигрывается автоматически. Показ рекламы будет производиться как на десктопах, так и на мобильных устройствах.

Партнёрами по запуску выступили киностудия 20th Century Fox и телекоммуникационная компания Verizon. Они первыми получили возможность воспользоваться преимуществами нового формата.

Пока First View запускается только для рекламодателей в США. Когда он станет доступным в других странах, в компании не уточнили.

***

12.02.2016

Новая лента Twitter поможет брендам привлечь наиболее заинтересованную аудиторию

По мнению экспертов и специалистов отрасли, новая лента Twitter открывает больше возможностей перед брендами. Теперь они смогут привлечь более заинтересованную и вовлечённую аудиторию, сообщает МедиаБизнес со ссылкой на searchengines.ru.

Для брендов, цель – повысить видимость их органического контента в Twitter и побудить пользователей к взаимодействию с ним. Это, в свою очередь, может способствовать увеличению бюджетов компаний на продвижение в сервисе микроблогов. Показ рекламы в новой ленте будет производиться так же, как и в традиционном варианте.

Одной из основных возможностей роста для брендов в Twitter будет создание вовлекающего и интересного контента. У компаний, привлекающих

пользователей качественными материалами, будет больше шансов на то, что алгоритм Twitter выберет их контент для показа в лентах подписчиков.

Нововведение не повлияет на показ продвигаемых твитов и аккаунтов. Однако теперь компании смогут лучше понимать, какой контент больше всего резонирует с их аудиторией и учитывать эту информацию при создании рекламного креатива.

***

13.02.2016

Профессиональная сеть: как с помощью LinkedIn найти работу

LinkedIn – это социальная сеть для инсайдеров бизнеса и профессионалов. Сайт помогает расширять сеть деловых контактов, узнавать о новостях коллег или индустрии в целом, а также собрать в одном месте информацию о собственном карьерном пути и профессиональных достижениях, пишет UBR.

Другими словами, профиль в LinkedIn легко может стать вашим портфолио и дополнить ваше резюме. К тому же, все чаще HR-агенты просят потенциальных кандидатов указывать ссылку на свой профиль в этой сети или же самостоятельно находят там страницы соискателей. Именно поэтому к информации, которая там указывается, необходимо относиться так же ответственно, как и к собственному профилю в других социальных сетях, которые используются в рабочих целях, пишет rabota.ua.

Важность LinkedIn не стоит недооценивать: в настоящее время в этой соцсети более 400 млн пользователей из более чем 200 стран. Сайт доступен на 24 языках.

С чего начать?

Загрузите фотографию. Статистика показывает, что профили с фото просматривают чаще. Это должна быть ваша настоящая фотография в деловом стиле хорошего качества.

Заполните свой профиль. Страница в LinkedIn имеет очень четкую структуру, поэтому соцсеть сама подсказывает, какой еще информации не хватает и какие поля необходимо заполнить.

Информация станет более эффективной и начнет сразу работать в вашу пользу, если снабдить описание краткой информации о себе и своего профессионального опыта наиболее важными ключевыми словами и навыками, которые относятся к указанной специальности. Именно ключевые слова помогают потенциальным работодателям найти ваш профиль в поиске. Чтобы выделить нужные «ключи» и правильно ими распорядиться, посмотрите, как заполнены профили у других специалистов вашей сферы. Это поможет сориентироваться.

Уделите время и внимание заполнению Summary – это краткая характеристика вас как профи в самом начале вашего профиля. Это мини-презентация, которая сразу бросается в глаза и определяет характер общения с

вами. Написанное в Summary должно привлекать. Указывать в нем информацию можно по такому шаблону:

1) кто вы и чем занимаетесь, ваши ключевые навыки и компетенции;

2) профессиональные цели, интересы и достижения;

3) в какой занятости вы заинтересованы и какие предложения для вас интересны.

Найдите коллег и друзей. LinkedIn позволяет воспользоваться импортом из адресных книг, ручным поиском людей с помощью настраиваемых фильтров, а также сеть сама предлагает контакты на основе уже имеющейся сети. Интересных вам людей можно искать через поиск с помощью ключевых слов. Например, по названию должности, если вы ищите эйчаров компаний или рекрутинговых агентств, руководителей или топ-менеджеров.

Что еще здесь есть?

Компании. Многие компании, особенно международные, ведут корпоративную страницу на LinkedIn, где публикуют важные корпоративные новости и вакансии. Подписываясь на страницы, вы можете отслеживать ключевых игроков индустрии. Новости компаний появятся у вас в ленте, причем это могут быть не только обновления, размещаемые самой компанией, но и упоминания о ней на сторонних ресурсах. Также очень часто о поиске специалистов делают объявление в виде обычного поста с целью расшарить его и получить отклики, поэтому внимательно следите за своей лентой.

Вакансии. На LinkedIn есть отдельный раздел для поиска работы – Jobs. Однако для поиска работы можно использовать и обыкновенный поиск, вписывая туда необходимые ключевые слова, которые могут быть в описании вакансии, название должности, название компании и т. д.

Группы. Группы могут объединять людей как по интересам, так и по принадлежности к какой-либо компании. Например, может быть группа блогеров, группы пользователей определенного сайта или группа работников модной индустрии. Иногда по тематике групп, которые отображаются в профиле того или иного человека, можно судить о его интересах и сфере увлечений.

Личности. В LinkedIn легко можно найти профиль CEO крупной международной компании и подписаться на его обновления. Вы сможете видеть инициируемые этим человеком дискуссии, его рекомендации и ссылки. Отличный способ учиться у лучших.

Как использовать LinkedIn с максимальной пользой?

Регулярно публикуйте обновления. Это могут быть полезные ссылки на другие ресурсы, ссылки на ваш сайт или продукт, опубликованные вами статьи и т. д. Но помните, что LinkedIn – это сеть для профессионалов, поэтому не стоит захламлять ленту или наполнять ее ненужным, не относящимся к теме материалом.

Участвуйте в дискуссиях. Любая статья или обновление статуса подразумевает возможность комментирования. Это отличный повод обсудить

свежую новость с коллегами, продемонстрировать свою осведомленность в вопросе, быть в курсе новостей отрасли или завести новые знакомства.

Сообщайте об изменениях в карьере вовремя. Если даже вам кажется, что это мелочи, может оказаться, что человек просто увидит, что вы уволились с работы (LinkedIn присылает оповещения о происходящем в сети контактов) или завершили проект – и сделает вам выгодное предложение. Более того, сайт активно используют рекрутеры, для которых ваши успехи, продвижения и события тоже могут нести информативную ценность.

Используйте рекомендации. После успешного сотрудничества не стесняйтесь просить довольных клиентов или коллег оставить отзыв в вашем профиле. Это хороший знак для потенциальных работодателей и отличная возможность продемонстрировать свои выгоды и сильные стороны.

Подтверждайте навыки других. В профилях всех пользователей LinkedIn отображается список их навыков. Их можно подтвердить, нажимая кнопку Endorse возле каждого. Не скупитесь на такие подтверждения: оно занимает всего пару кликов, но правилом хорошего тона считается отправить подтверждение в ответ. Таким образом вы получите активность на своей странице .

Будьте на связи. Обязательно отвечайте на все личные сообщения и не бойтесь инициировать общение сами. Например, если рекрутер или HR-агент той или иной компании сам добавил вас в контакты, есть смысл написать ему личное сообщение в целях знакомства, спросить, нужна ли какая-то дополнительная информация и т. д. Даже если сразу не поступит предложения о сотрудничестве, вас заметят и запомнят.

В чем следует проявлять осторожность?

Не злоупотребляйте большим количеством групп. Вы можете состоять не более чем в 50 группах. Это ограничение соцсети. Выбирайте группы с наибольшим количеством участников и только те, которые действительно интересны для вас.

Не злоупотребляйте рассылками. За жалобы на спам могут заблокировать.

Не злоупотребляйте большим количеством контактов. LinkedIn позволяет отправлять запросы в друзья другим людям и рекомендует при этом составлять текстовое сообщение, если есть вероятность, что человек вас не вспомнит или может лично не знать (но при этом вы хотите добавить его в друзья). Рекомендуем так и делать. Ведь при получении заявки на добавление через интерфейс сайта другой пользователь можно указать «Я не знаю этого человека». Если таких случаев в ответ на ваши заявки будет слишком много, это может привести к заморозке аккаунта.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

9.02.2016
Недостаток сна приводит к зависимости от социальных сетей

Ученые университета Питтсбурга выявили закономерность между ростом интереса к социальным сетям и накопленной усталостью в организме. Ими было установлено, что недостаток сна влияет на желание людей пользоваться той же Facebook, и чем больше недосыпание, тем сильнее желание открыть этот сайт, пишет InternetUA.

Исследование, проведенное специалистами, главным образом затрагивало студентов, которые уже не могут представить жизнь без смартфонов и мобильного Интернета, передает портал Slash Gear. В отчете ученых говорится, что социальная сеть Facebook абсолютно не виновата в недостатке сна у студентов – это касается в равной степени всех существующих социальных сетей, и самая крупная из них была взята лишь в качестве наглядного примера.

Закономерность между недосыпом и стремлением как можно больше времени провести в социальной сети, проста: отсутствие сна одаривает людей постоянным чувством усталости, которое постепенно приводит к сильной раздражительности и резко снижает работоспособность, что тоже не лучшим образом отражается на настроении. Facebook и другие социальные сети не требуют от пользователей умственной или физической деятельности, позволяя расслабиться за чтением постов и просмотром фотографий, что и делает их популярными среди тех, кто испытывает проблемы со сном. Для них это просто способ расслабиться и снять стресс при нехватке сил на что-либо другое.

Все данные взяты на основе эксперимента, в котором приняли участие 34 студента и 42 студентки (итого, 76 человек). Находившиеся под наблюдением в течение недели, они специально недосыпали и каждое утро отвечали на вопросы о своем состоянии после сна. Вечером того же дня они передавали ученым данные о своих делах в течение светлого времени суток, а датчики на них фиксировали уровень стресса.

Согласно результатам исследования, зависимость от социальных сетей, вызванная повышенной отвлекаемостью на фоне хронической усталости, не связана ни с возрастом, ни с полом людей – в равной степени это касается и взрослых, и детей, и мужчин, и женщин.

***

5.02.2016

Facebook спростував теорію шести рукостискань

Facebook перевірила теорію шести рукостискань на базі 1,6 млрд користувачів. Компанія з'ясувала, що двох людей розділяють у середньому 3,57 людини, пише RegioNews-Суми з посиланням на Meduza.

Повідомляється, що дослідження показало тенденцію до скорочення відстані між двома будь-якими людьми зі зростанням кількості користувачів.

Facebook довела, що якщо у вас 250 друзів у соціальній мережі, а у них теж по 250, то тільки кількість друзів буде більше 62 тис.

У 2011 р. Корнельский університет і Університет Мілана перевірили теорію шести рукостискань на 721 млн користувачів Facebook. Тоді виявилося, що відстань між людьми становить 3,74.

Маніпулятивні технології

12.02.2016

Facebook стрімко втрачає користувачів інтернету через неадекватну політику

З приводу політики Facebook є моменти, які вказують на відмирання соцмережі, принаймні в Україні, приводить Інформатор статтю С. Вакули.

«Неадекватна "політика Facebook" викликає все більше невдоволення адмінами соцмережі, які таки сидять під Пітером в адмінцентрі (чи не в Ольгіно?). "Правила Facebook", на які вони посилаються, адекватно не пояснюють дії адмінів, і тим більше не дають змоги апелювати до тих чи інших положень. Адміни банять на свій розсуд, а не через якісь конкретні правила.

– Адміни Facebook за два роки війни проявили себе як антиукраїнська соцмережа, банячи користувачів за посити із символікою добробатів.

– На Facebook без відома користувача додають у сотні груп, і якщо на них хтось наскаржиться – банять усіх учасників груп.

– У порівнянні з іншими соцмережами, на Facebook запроваджена неадекватна цензура. Зокрема – пропаганда "цінностей" ЛГБТ та інших меншин, які, на думку М. Цукерберга і його оточення, є "демократичиними" і "істиними". Якщо хтось не поділяє цю думку – нещадний бан, навіть за конструктивну критику.

Ці, та інші фактори спричинили суттєву "міграцію" користувачів з Facebook на інші соцмережі. Зокрема – в Instagram».

***

13.02.2016
Владельцы iPhone оказались жертвами розыгрыша в соцсетях

Ряд владельцев iPhone оказались жертвами розыгрыша в соцсетях, в результате которого их смартфон временно переставал работать. В нескольких сообществах «ВКонтакте» была опубликована запись, где говорилось о возможности получить «новый хиппи-дизайн стандартных приложений, новый хиппи-шрифт и пару новых обоев», пишет InternetUA.

Для этого пользователям предлагалось вручную поменять дату в настройках устройства на 1 января 1970 г. и перезагрузить iPhone.

В реальности владельцы гаджетов становились жертвами ошибки, из-за которой смартфон зависал во время отображения логотипа и больше не включался. 11 февраля о ней впервые сообщили пользователи Reddit. Решить проблему помогает только ручное отсоединение аккумулятора, которое производят в профессиональном сервисе.

Зарубіжні спецслужби і технології «соціального контролю»

6.02.2016
Twitter провела кампанию по борьбе с терроризмом в соцсети

Социальная сеть Twitter заблокировала более 125 тыс. учетных записей пользователей из-за террористических угроз или за пропаганду терроризма. Об этом говорится в заявлении, опубликованном в официальном блоге компании, пишет InternetUA.

«Только с середины 2015 г. мы закрыли более 125 тыс. аккаунтов, в первую очередь связанных с “Исламским государством”», – отмечается в документе.

8 января Белый дом, правоохранительные органы и спецслужбы США провели встречу с главами крупнейших американских интернет-компаний. На встрече с представителями Microsoft, Apple, Facebook, Google, Twitter, Yahoo и LinkedIn чиновники обсудили вопрос противодействия террористам во всемирной сети.

***

9.02.2016
Twitter создаст совет по борьбе с троллями

Руководство Twitter приняло решение учредить совет, который займется вопросами борьбы с оскорблениями и запугиваниями в соцсети (Twitter Trust and Safety Council). Об этом сообщает InternetUA ссылаясь на Engadget.

По словам главы по глобальной политике Twitter П. Картес, компания наймет специалистов почти из 40 правозащитных организаций. Среди них GLAAD, которая занимается интересами ЛГБТ-сообщества, Национальная сеть противодействия насилию в семье и британская благотворительная организация the Samaritans («Самаритяне»), оказывающая психологической помощь по телефону.

Компания также хочет заполучить в свой совет специалистов из организации по защите прав женщин Feminist Frequency. Ее руководитель А. Саркисян ранее поднимала вопрос о том, как женщины изображаются в видеоиграх.

Обезопасить платформу руководство соцсети подтолкнул поток жалоб от пользователей, которые требовали ужесточить правила в отношении оскорблений и посягательств одних людей на других, особенно направленных на женщин.

Ранее в феврале 2015 г. гендиректор Twitter Д. Костоло признал, что компания испытывает затруднения в борьбе с интернет-нарушителями на своей платформе. «Мы плохо справляемся с троллями на нашей платформе и это продолжается годами. Это не секрет, и весь мир говорит об этом каждый день. Мы теряем ядро нашей аудитории просто потому, что не можем эффективно бороться с троллингом», – сказал он.

***

7.02.2016

«Твіттер-поліція» Малайзії заборонила критикувати прем'єра в соцмережах

У малайзійській поліції створено спеціальний кіберпідрозділ по боротьбі з користувачами, які критикують дії прем'єр-міністра Малайзії Н. Разака, повідомляє BUBLBE.COM з посиланням на портал asiaone.com.

Нагадаємо, Міністерство юстиції США розслідує платежі на 681 млн дол. і угоди з елітною нерухомістю в Нью-Йорку, які можуть бути пов'язані з корупційним скандалом навколо прем'єр-міністра Малайзії Н. Разака і суверенного фонду 1Malaysia Development Berhad (1MDB). Ця справа спровокувала політичну кризу в азіатській країні, уже ведуться розслідування у Швейцарії, Гонконгу і самій Малайзії.

Минулого тижня генпрокурор Малайзії заявив про те, що розслідування по трансферту сотень мільйонів доларів на особисті рахунки Н. Разака закрито, оскільки жоден із законів не порушено. За його словами, 681 млн дол. – це «особисте пожертвування» від королівської сім'ї із Саудівської Аравії, і більшу частина цієї суми було повернуто.

Незважаючи на це, жителі Малайзії активно критикують прем'єра, зокрема в соціальних медіа. Так, поширення набула карикатура, на якій Н. Разак зображений з обличчям клоуна і власною цитатою: «У країні, де процвітає корупція, ми всі під підозрою».

Буквально за кілька годин після появи малюнка поліцейські надіслали його авторові Ф. Резі інтернет-попередження про те, що його Twitter-акаунт перебуває під наглядом і повинен використовуватися «розумно і відповідно до закону».

Ф. Резі – далеко не єдиний користувач, переслідуваний поліцією. «Стосовно осіб, які розповсюджують неправдиву інформацію, будуть вжиті заходи», – таке попередження правоохоронці розсилають усім користувачам, які дозволяють собі критикувати прем'єра.

***

12.02.2016

В США готовят законопроект против антишифровальных законов

В США готовится новый законопроект, направленный на запрет создания антишифровальных законов на уровне штатов. Об этом сообщает Gazeta со ссылкой на Wired, пишет InternetUA.

Калифорнийский конгрессмен Т. Лью представил законопроект «Обеспечение национальных конституционных прав для частных телекоммуникаций – 2016», сокращенно ENCRYPT. В нем Т. Лью предлагает отказаться от введения антишифровальных законов на уровне штатов, которые часто дублируют друг друга.

«Невозможно создать бэкдор, которым смогут пользоваться только хорошие парни, потому что рано или поздно хакеры найдут его», – рассказал конгрессмен.

Т. Лью также отметил, что законы США распространяются только на американские компании, а значит, принудительное дешифрование коснется Apple, но не затронет Samsung или LG. Конгрессмен объяснил, что какие-либо доказательства того, что благодаря антишифровальным бэкдорам могут быть предотвращены террористические атаки, отсутствуют.

Ранее стало известно, что власти американского штата Калифорния рассматривают законопроект, который может привести к приостановке продаж продуктов Apple в родном штате компании.

Согласно тексту рассматриваемого законопроекта, производитель или поставщик операционной системы должен иметь право разблокировать и получить доступ к информации любого смартфона, изготовленного на момент 1 января 2017 г. или позднее и поступившего в продажу на территории Калифорнии.

Если законопроект вступит в силу, то за каждый телефон без возможности стороннего разблокирования Apple будет вынуждена заплатить штраф в 2,5 тыс. дол.

***

12.02.2016

В России заговорили о вечной блокировке «ВКонтакте»

Глава российской службы по надзору в сфере связи (Роскомнадзор) А. Жаров заявил, что социальная сеть «ВКонтакте» за год-полтора обязана полностью избавиться от нелицензионного контента. Компании необходимо перейти на легальную схему работы, иначе ее ждет печальная участь Rutracker, пишет IGate.

«Я уверен в том, что в ближайшее время – год-полтора – «ВКонтакте» станет полностью легальным сервисом», – сообщил А. Жаров.

Он отметил, что с момента вступления в силу антипиратского закона в РФ поведение местных социальных сетей заметно изменилось. Однако «ВКонтакте» продолжает оставаться в списке главных пиратских ресурсов США. «Мы продолжаем работать, над исключением ее из списка», – сказал А. Жаров. Он уточнил, что в настоящее время владельцы социальной сети начали сотрудничество с площадкой дистрибуции легального медиа-контента Pladform. Это поможет легализировать трафик фильмов и музыки. Кроме того, представители «ВК» ведут переговоры с местными зарубежными правообладателями.

Глава Роскомнадзора подчеркнул, что основной проблемой в России остается слишком высокая стоимость контента. Он объяснил такое положение дел длительной неравной конкуренцией между легальными ресурсами и «пиратами».

***

11.02.2016

В России хотят взять под контроль интернет-трафик

Минкомсвязи России разработало законопроект о государственном контроле над прохождением интернет-трафика на территории РФ.

Об этом сообщают «Ведомости» со ссылкой на пояснительную записку к документу, пишет InternetUA.

Это проект поправок в законы «О связи» и «Об информации, информационных технологиях и защите информации».

Законопроект реализует поручения президента РФ В. Путина по итогам заседания Совета безопасности, состоявшегося осенью 2014 г. Совет обсуждал итоги учений по устойчивости российского Интернета и вопросы его автономной работы: речь шла о минимизации рисков для рунета в случае его временного отключения от внешнего мира при чрезвычайных ситуациях.

В законопроекте Минкомсвязи описаны несколько способов, которые помогут органам государственной власти следить за маршрутами интернет-трафика по сетям связи. Во-первых, министерство предлагает создать

государственную систему мониторинга «использования ресурсов глобальной адресации и глобальных идентификаторов сети интернет (DNS и IP-адресов)». Эта система также должна отслеживать работу критических элементов инфраструктуры рунета, говорится в записке. В рамках этой системы будет создан реестр адресов рунета.

Также законопроект предлагает сделать зарубежные каналы связи и точки обмена трафиком более контролируемыми. Во-первых, организовывать международные каналы связи смогут только операторы, имеющие лицензию на трансграничную передачу данных. Источник издания объясняет: сейчас в России сложно подсчитать количество каналов связи, пересекающих границу, и среди них есть серые каналы, не учтенные профильными ведомствами. Собеседник «Ведомостей» рассчитывает, что им придется выйти из тени и полностью выполнять российские законы. С другой стороны, государство могло бы предложить им защиту и резервные каналы на случай чрезвычайных ситуаций.

***

13.02.2016

Черный Р. Роскомнадзор пытается запретить людям обсуждать методы обхода блокировок

Роскомнадзор одобрил законопроект, согласно которому пользователи могут быть оштрафованы за один лишь факт обсуждения способов блокировок сайтов. Несмотря на очевидную абсурдность подобного законопроекта, в ближайшее время его текст будет передан руководству организации для внесения на рассмотрение в Госдуму, пишет IGate.

Законопроект предполагает, что «реклама, пропаганда или иной призыв к использованию специальных технических средств и способов, позволяющих получить беспрепятственный доступ» к заблокированным сайтам, наказывается штрафом. Сумма штрафа составляет от 10 тыс. до 50 тыс. р. для простых граждан; от 50 тыс. до 100 тыс. р. для должностных лиц; от 100 тыс. до 300 тыс. р. для организаций и компаний.

Впрочем, в этой ситуации можно усмотреть и положительные аспекты. В частности, сама попытка Роскомнадзора протащить подобное «художество» в ранг закона указывает на отчаяние и неспособность этой организации сколь-нибудь серьезно навредить свободе Интернета.

***

12.02.2016

Турецкую журналистку приговорили к 28 месяцам тюрьмы за твит

В Турции 24-летнюю журналистку Х. Калафат приговорили к 2 годам и 4 месяцам тюрьмы за сообщение на ее странице в Twitter, в котором, по мнению

суда, содержатся оскорбления в адрес президента Турции Т. Эрдогана, передает InternetUA со ссылкой на Hurriyet.

Отмечается, что в своем сообщении, которое журналистка опубликовала в марте 2015 г., она раскритиковала действующего президента страны, а также правящую Партию справедливости и развития. Х. Калафат вскоре удалила свое сообщение, однако прокуратура к тому времени уже начала расследование против нее.

В суде Х. Калафат раскаялась, после чего суд принял решение об отсрочке исполнения приговора на пять лет.

***

13.02.2016

Індія vs Цукерберг, або чому мережевий нейтралітет – це не абстракція

8 лютого Індія заборонила реалізацію на своїй території проекту М. Цукерберга Free Basics (internet.org). Платформа Free Basics («Вільні основи») покликана надати мобільним користувачам 30 країн безкоштовний доступ до спрощеної версії соцмережі, новинних сайтів, ресурсів для пошуку роботи тощо. Сервіс дає користувачам доступ лише до обмеженого кола ресурсів, а не до всього Інтернету, що і викликало бурхливу суперечку в Індії щодо мережевого нейтралітету – принципу, згідно з яким всі мережеві дані повинні оброблятися однаково. Критики ж стверджують, що Facebook класифікує користувачів, створивши обмежену версію Всесвітньої павутини для бідняків.

MediaSapiens пропонує переклад статті автора The Atlantic А. Лафренс Not Another Net-Neutrality Story («Не чергова історія про мереживий нейтралітет»), у якій журналістка пояснює, що принцип мережевої нейтральності таки відіграє роль у реальному світі.

Facebook зазнає удару з боку регулюючих органів в Індії, що доводить: боротьба за відкритий Інтернет – це більш ніж абстракція.

Інтернет може бути прекрасним, темним та глибоким, проте більшість із нас надто не занурюється в його нетрі. Ще у 2013 р. провідна американська соціологічна компанія повідомила, що в середньому американці відвідують по 90 доменів на місяць кожен. Цей вкрай низький показник – еквівалент трьом доменам на день – знижувався з року в рік, хоча люди усе більше й більше часу проводять онлайн. Я підозрюю, що середньостатистична людина нині відвідує навіть менше доменів, оскільки такі компанії-гіганти як Facebook, Amazon та Google у конструюванні своїх платформ намагаються зробити користувача максимально залученим та знеохотити його відвідувати інші сайти.

І це, зокрема, є дуже цікавим у контексті нещодавнього рішення регулюючих органів в Індії заблокувати те, що називають zero-rating чи sponsored data – практику звільнення користувача від оплати за Інтернет у випадку використання конкретного набору веб-ресурсів. Цей крок ефективно

блокує фейсбукову програму Free Basics, пакет спрощених версій популярних сайтів, звичайно ж включно з Facebook, що не «з'їдають» трафік на противагу іншим мобільним сайтам. Ідея полягає в тому, щоби дати людям можливість отримати доступ до Інтернету, проте вона вже давно критикується з боку прихильників мережевого нейтралітету, оскільки вони розглядають її як спосіб надавати несправедливу перевагу певним сайтам.

Якщо ти пропонуєш лише певний набір сайтів безкоштовно, стверджують вони, чи не надає це нечесну перевагу цим сайтам? Вам не треба активно блокувати своїх конкурентів, аби знищити їх. (Free Basics позиціонується як відкритий проект – тобто кожен може додавати свої веб-сайти до платформи, але Facebook все ще встановлює основні принципи, які диктують правила використання).

Знову ж таки, якщо у вас є вибір поміж організованим Facebook міні-інтернетом, або між його відсутністю узагалі, чи не ліпше хоча би щось за нічого? Можливо, і ні. Деякі критики проводять паралелі між роллю Facebook як «воротаря» (що управляє чи конструює потік інформації) та британською колонізацією Індії.

«Я прошу вибачення за незручності, створені нами, індійцями, через неприйняття чогось, що кричуще суперечить свободі слова та відкритому Інтернету…», – зауважив один користувач Reddit минулого року в AMA (Ask Me Anything – «спитай мене що завгодно») з К. Деніелсом, віце-президентом Facebook, який працює над проектом internet.org, що включає в себе Free Basics. «Ми скоїли дурницю з EastIndiaCompany. Більше ніколи, брате, більше ніколи!».

На доступ до величезних «покладів» інформації та знань для мільярдів людей. Ось як незалежний регулятор телекомунікаційного бізнесу в Індії (Telecom Regulatory Authority of India) підсумував своє рішення цього тижня:

«Ці диференційовані тарифні пропозиції мають як позитивний, так і негативний вплив. З одного боку, у цьому можна вбачати спосіб зробити загальний доступ до Інтернету ще більш доступним – за рахунок скорочення витрат на певні види контенту і надання можливості людям, які до цих пір не в змозі використовувати інтернет-сервіси та контент, доступу до частини Інтернету. Це може мати перевагу розширення та прискорення доступу до Інтернету, оскільки ці користувачі зможуть вперше випробувати його переваги та почати платити за повний доступ.

З іншого боку, диференційовані тарифи призводять до класифікації абонентів залежно від контенту, до якого вони хочуть мати доступ (тими, хто хоче отримати доступ до безкоштовного контенту, і тими, хто бажає отримати доступ до повного пакета)».

Тепер же ми переходимо до другої частини пояснення, чому те, що відбувається в Індії, є настільки захоплюючим. Концепція мережевого нейтралітету така непевна і хитка, тому що надто часто описується теоретичними термінами.

Не буде помилкою сказати, що засновник Facebook М. Цукерберг сприймає мережевий нейтралітет як абстракцію, якщо він почав просувати Free Basics минулого року. «Більшість людей, що наполягають на мережевій нейтральності, уже мають доступ до Інтернету, – сказав він на Q&A-сесії зі студентами в Делі, як повідомили у місцевій пресі. – Я бачу ці петиції щодо мережевого нейтралітету, і вважаю, що це чудово. Нам слід мобілізуватися в Інтернеті, аби просувати ідею. Та люди, що не мають доступу до Інтернету, не можуть підписати онлайн-петицію, наполягаючи на розширенні доступу до мережі».

Рішення Індії демонструє, що мережевий нейтралітет має значення в реальному світі і має потенціал, аби впливати на мільярди людей. Як минулого року зазначив Tech Crunch, Facebook бачить себе як трамплін, але все ще діє як воротар: «Одна сторона вважає, що допомагає знедоленим. А інша вважає, що допомога занадто небезпечна, аби її прийняти».

Це рішення також має масштабні наслідки для бізнесу Facebook. Його мета не лише допомогти 4,9 млрд людям отримати надійний і доступний Інтернет; Facebook хоче стати ключовим порталом, через який дві третини населення земної кулі відчує Інтернет. Це може звучати як цинічний спосіб інтерпретації амбіцій та цінностей проекту, який М. Цукерберг назвав способом задоволення фундаментального соціального та економічного права людей на доступ до мережі. («Мова не йде про якусь комерційну вигоду для Facebook – немає навіть жодної реклами у версії Facebook для FreeBasic», – писав він на сторінці однієї з найавторитетніших газет в Індії The Times of India минулого року.)

Але це також було би нерозумно для Facebook – не бачити потенціалу для зростання у випадку, коли кількість підключеного до Інтернету населення разюче збільшується. А М. Цукерберг зовсім не дурний.

Також є наслідки для інших країн. Частина фейсбукової стратегії глобальної експансії щойно провалилася, або принаймні Facebook було завдано серйозного удару в ключовій країні. Ось що пише автор Fusion Ке. Руз: «Якщо групі активістів вдалося успішно змінити сприйняття FreeBasics як акту корпоративної щедрості на підступе захоплення земель і мобілізувати країну проти нього, що завадить їм перешкодити вчинити так в іншому місці?»

І як І. Баррінгтон писав для The Atlantic у грудні, різні мобільні оператори у США пропонують «безкоштовний» відеострімінг як спосіб залучення нових клієнтів для платформ. «Це аж надто очевидно виходить за рамки, аби бути правдою, – пише І. Баррінгтон. – Оператори мобільного зв’язку буквально у партнерстві з великими медіа-компаніями субсидують відеострімінгові сервіси, у той час як те, що можна сприйняти за “відкритий Інтернет” усе ще залишається платним сервісом».

У понеділок М. Цукерберг у своєму пості у Facebook написав, що він «розчарований», але продовжить працювати в напрямі досягнення мети підключення в Індії. У своєму попередньому матеріалі для Times of India він був менш стриманий: «Хто взагалі може виступати проти цього?».

2.02.2016

В 2015 году было создано более 304 млн новых видов вредоносного ПО

По данным специалистов Panda Security, в прошлом году появилось более 304 млн новых видов вредоносов. Как сообщается в отчете компании, вирусописатели побили своеобразный рекорд, за один год создав более четверти (27,63 %) всего существующего в мире вредоносного ПО, пишет InternetUA.

В прошлом году специалисты Panda Security обнаружили 84 млн образцов вредоносного ПО – порядка 28 % всех созданных в 2015 г. вирусов. Для сравнения, в 2014 г. сотрудники компании выявили примерно 75 млн вредоносов.

Как заявил технический директор компании Л. Корронс в интервью изданию Infosecurity Magazine, компаниям необходимо инвестировать в технологии по обнаружению и устранению угроз на рабочих станциях (endpoint detection and response, EDR). «Как заявили специалисты Gartner, EDR позволяет улучшить безопасность компании и быстрее реагировать на атаки, обходящие существующие меры антивирусной защиты», – сообщил Л. Корронс.

Самыми популярными категориями вредоносного ПО в 2015 г. стали трояны (52 % от всех обнаруженных вредоносов), обычные вирусы (23 %) и черви (13 %). Реже всего обнаруживали новые виды потенциально нежелательных приложений (11 %) и шпионского ПО (2 %). В кибератаках чаще всего использовалось вымогательское ПО CryptoLocker.

Лидером по количеству инфекций вновь оказался Китай – 57 % компьютеров в Поднебесной оказались заражены тем или иным видом вредоносного ПО. Также в списке оказались Тайвань (49 %), Турция (43 %), Колумбия (33 %), Уругвай (33 %) и Испания (32 %).

***

1.02.2016

Неправильно настроенные серверы Apache раскрывают данные Tor-трафика

Инженер Facebook А. Маффлет привлек всеобщее внимание к проблеме, о которой ранее уже писали на Reddit и сообщали Tor Project. Дело в том, что неправильная конфигурация веб-сервера Apache, на котором работает Tor hidden service, может привести к компрометации анонимного трафика, пишет InternetUA.

Сам А. Маффлет никаких исследований не проводил, вместо этого он перепостил у себя в Twitter статью никому неизвестного студента, который прекрасно описал как саму проблему, так и ее возможные последствия.

Пожелавший остаться безымянным студент начал свой текст с простой рекомендации: все, у кого Tor работает под Apache, должны отключить mod_status ($ a2dismod status), так как в большинстве версий Apache mod_status включен по умолчанию. Из-за этого страница, расположенная по адресу http://sitename.com/server-status/ отображает статистику: аптайм сервера, использование ресурсов, данные о трафике, доступные виртуальные хосты, а также активные HTTP-запросы.

С одной стороны, по умолчанию страница /server-status доступна только локально, с другой – Tor тоже работает на localhost. То есть все скрытые сервисы, которые полагаются в работе на дефолтную конфигурацию Apache, подвергаются огромному риску.

Опираясь на данные со страницы /server-status, злоумышленник может вычислить часовой пояс сервера, его географическую позицию, языковые настройки, а также IP-адреса, если повезет с неверно настроенными виртуальными хостами.

Однако это еще не самое страшное. Студент долго разбирался в данной проблеме и искал уязвимые сайты почти полгода. В конце 2015 г. он обнаружил, что уязвимости подвержен популярный поисковик в зоне .onion. Просматривая активные HTTP-запросы сервера, он получил возможность видеть, что именно ищут люди. Исследователь сообщил о проблеме всем сайтам, где заметил уязвимость. Все администраторы, включая держателей .onion-поисковика, уже устранили проблему. Однако другие уязвимые ресурсы по-прежнему продолжают работать, и для их компрометации не нужны 0day, анализ трафика и криптоатаки. Хватит и просто включенного mod_status.

***

1.02.2016

Вымогательское ПО становится основным элементом кибератак на предприятия

Киберпреступники активно используют вымогательское ПО в атаках на частные предприятия, и требования злоумышленников становятся все более специфичными. Об этом сообщается в отчете организации Online Trust Alliance (OTA), пишет InternetUA.

Согласно данным организации, киберпреступники стали чаще инфицировать вымогательским ПО компьютерные сети предприятий, хранящих важные данные. Злоумышленники на свое усмотрение устанавливают сумму выкупа в зависимости от ряда факторов, включая конфиденциальность информации и размер компании.

«В то время как компании собирают все больше диверсифицированной информации и увеличивают зависимость от сторонних поставщиков услуг,

каждому предприятию необходимо ввести необходимые меры безопасности и иметь возможность быстро отреагировать на взлом или утечку данных. Киберпреступники не просто атакуют компании, собирающие данные о потребителях, а осуществляют целевые атаки на предприятия, хранящие конфиденциальные высокопрофильные сведения», – заявил директор отдела IT-безопасности компании LifeLock Н. Дасуани.

Одним из основных видов оружия в арсенале киберпреступников стало вымогательское ПО. По словам исполнительного директора и президента OTA К. Спизель, злоумышленники теперь самостоятельно определяют размер выкупа, основываясь на ряде факторов. Учитывается размер компании, рыночная стоимость данных и прочая информация.

Согласно приведенным в отчете данным, 91 % всех утечек данных, произошедших в январе – августе 2015 г., можно было предотвратить путем установки исправлений безопасности, шифрования данных или проведения специальных инструктажей среди пользователей.

***

2.02.2016
У шпионского трояна для Linux есть Windows-версия

Специалисты «Лаборатории Касперского» сообщили об обнаружении «брата-близнеца» трояна Linux.Ekocms, который ранее был найден экспертами компании «Доктор Веб». В классификации «Лаборатории Касперского» малварь, ориентированная на Linux системы, получила имя Backdoor.Linux.Mokes.a. Но согласно новому отчету, у вредоноса также имеется и версия для Windows, пишет Украинский телекоммуникационный портал.

В конце января сотрудники компании «Доктор Веб» сообщили об обнаружении трояна Linux.Ekoms.1. Малварь не только делает снимки экрана жертвы с определенной периодичностью, но способна загружать на зараженную машину различные файлы.

Чуть позже компании Sophos и «Лаборатория Касперского» также идентифицировали новую угрозу, дав ей названия Linux/Mokes-A и Backdoor.Linux.Mokes.a, соответственно. Но оказалось, что атаками на пользователей Linux дело не ограничивается. В новом аналитическом отчете «Лаборатории Касперского» сообщается, что специалисты компании обнаружили 32-битную Windows-версию трояна.

В целом, принцип работы Windows-версии трояна схож с работой его Linux-двойника. Разумеется, в коде есть некоторые модификации, отражающие специфику работы ОС, но их нельзя назвать существенными. Принцип работы остался прежним: троян случайным образом выбирает для установки одну из девяти локаций в %AppData %, связывается с командным сервером через определенные промежутки времени и шпионит за своей жертвой, сохраняя все собранные данные локально, для последующей передачи на сервер злоумышленников.

Основных отличий от версии для Linux два: в Windows-версии малвари включена функция кейлоггера, то есть все нажатия клавиш протоколируются и сохраняются в лог. Напомню, что Linux-версия трояна тоже содержала данный компонент, но он был отключен в обнаруженных специалистами образцах. Второе отличие, делающее версию для Windows более опасной: вредонос использует украденные сертификаты Comodo, чтобы заставить систему поверить, что он является легитимным и безопасным приложением из доверенного источника.

Чуть позже в отчете появилось дополнение, гласящее, что компания обнаружила еще одну разновидность трояна: Backdoor.Win32.Mokes.imw. Этот образец может похвастаться еще и включенной функцией звукозаписи, которая тоже неактивна в версии для Linux. Каждые пять минут малварь создает новый аудиофайл.

Троян написан на C++ и Qt, так что, теоретически, где-то может существовать и версия для Mac OS X, ведь операционная система компании Apple тоже поддерживается.

***

2.02.2016

Электроэнергетическая сеть Украины вновь пострадала от кибератаки

Электроэнергетическая сеть Украины вновь подверглась кибератаке спустя всего месяц после того, как в результате аналогичного инцидента часть системы вышла из строя, оставив миллионы жителей без света, пишет ЗапорожьеИнфо.

Ситуация усугубляется тем, что, по словам специалистов, исследующих вредоносную программу, предположительно послужившую причиной сбоя, – новую версию так называемого трояна BlackEnergy – она могла распространиться на многочисленные электросети Европы и грозит поразить многие другие.

Кибератаки и распространение вредоносного программного обеспечения (ПО) поставили перед аналитиками в области кибербезопасности задачу не только установить, какие из систем подвержены наибольшему риску, но и кто может нести за это ответственность.

«Необходимо исходить из предположения, что это ПО уже распространяется по Европе, – считает сооснователь и директор по безопасности компании SentinelOne У. Шамир. – Это кибервойна. Пора осознать, что это война».

У. Шамир и его коллеги недавно завершили полную обратную разработку нового трояна BlackEnergy3. Этой технологией аналитики часто пользуются, чтобы понять, как работает вредоносное ПО и кто его создал.

В ходе исследования аналитики выяснили, что BlackEnergy3 использует для распространения ту же слабость в программе Microsoft Office, что и более

ранние версии трояна, BE1 и BE2. По словам У. Шамира, это весьма необычно, поскольку разработчики Microsoft устранили проблему в 2014 г. «Есть несколько возможных объяснений, – рассказал эксперт “Голосу Америки”. – Во-первых, это могут быть просто старые системы, которые никогда не обновлялись. Во-вторых, кто-то может намеренно распространять вредоносное ПО изнутри. В-третьих, есть вероятность, что трояны находились в системах в спящем режиме на протяжении нескольких месяцев, и только сейчас пришли в действие».

Определить происхождение вредоносного ПО всегда крайне сложно, в связи с чем сложно наверняка установить, кто стоит за атаками. Однако специалисты из компании iSight ранее обнаружили сходства между более ранними версиями BlackEnergy и хакерской программой Sandworm предположительно российского происхождения, которая использовалась для атак на инфраструктуру НАТО в 2014 г.

У. Шамир выявил аналогичные сходства с BlackEnergy3, что позволило его команде предположить причастность российских хакеров. «Стиль кода, кластеры напоминают российское ПО, – отмечает У. Шамир. – Я практически уверен, что программа была разработана в России, но у меня нет неопровержимых доказательств».

Большее беспокойство, по словам У. Шамира, вызывает тот факт, что последняя версия BlackEnergy имеет модульную структуру, в связи с чем хакерам гораздо проще быстро вносить изменения в работу ПО, а аналитикам гораздо сложнее найти и искоренить его. «Это ПО можно обновлять, заменять, изменять, даже менять весь его функционал, – поясняет У. Шамир. – Так что если в одной промышленной сети есть спящий троян, он может получить совершенно новый командный модуль и заразить другие системы».

Именно из-за изменчивой структуры ПО так сложно определить, как именно оно работает, и какие системы поражены.

Самое страшное, по словам У. Шамира, состоит в том, что большая часть кода BlackEnergy3 не касается заражения промышленных командных систем, управляющих работой электросетей и других объектов тяжелой промышленности, а также вмешательства в их работу. Судя по всему, код создан для проведения тщательного мониторинга и сбора данных, так называемого «сниффинга».

«Это ПО способно выявлять сетевой трафик и делать записи о нем, похищать учетные данные пользователей и документы, если они работают в незашифрованном режиме, а также просачиваться в эти данные, – поясняет У. Шамир. – Это может позволить хакерам вносить поправки в BlackEnergy3 на ходу. Очевидно, программа нацелена скорее на шпионаж, и это нас беспокоит, поскольку мы не знаем, где она сейчас».

Обычно коммунальные предприятия и государства избегают публично признавать, что их ключевая инфраструктура подвержена кибератакам, из-за чего исследователям сложнее отслеживать распространение и работу BlackEnergy3.

Впрочем, У. Шамир, как и многие эксперты в сфере кибербезопасности, не сомневается в том, что троян будет распространяться и дальше, приводя к дальнейшим перебоям с электроэнергией и «загадочным» сбоям в работе электроэнергетических систем, транспорта и другой промышленной инфраструктуры.

***

3.02.2016

В промышленных коммутаторах Westermo обнаружена опасная уязвимость

В промышленных коммутаторах Westermo используются одни и те же неизменяемые закрытые ключи для SSL-сертификатов. Злоумышленник может осуществить атаку «человек посередине» и получить неавторизованный доступ к устройствам, пишет InternetUA.

Westermo – шведская компания, занимающаяся производством средств связи для критически важных систем. Решения от Westermo широко используются по всему миру в таких отраслях, как транспорт, водоснабжение, электроэнергетика, горнодобывающая и нефтяная промышленность.

По данным эксперта Команды экстренного реагирования на киберугрозы промышленных систем управления (ICS-CERT) Н. Смита, компания использует в продуктах одни и те же неизменяемые ключи шифрования. Поскольку ключи невозможно изменить, с их помощью злоумышленник может расшифровать передаваемую информацию, похитить учетные данные и получить контроль над устройствами.

Уязвимость получила идентификатор CVE-2015-7923 и оценку 9.0 из максимальных 10.0 по стандарту CVSS. Проблема затрагивает версию операционной системы WeOS 4.18 и ниже. В список уязвимых продуктов Westermo входят Falcon, Wolverine, Lynx, Viper и RedFox.

Компания выпустила обновление, позволяющее изменить проблемный SSL-сертификат, и в настоящее время работает над исправлением, автоматизирующим процесс изменения ключа. В качестве временной меры безопасности рекомендуется обновить WeOS до последней версии и загрузить пользовательский сертификат. От использования сертификатов с собственной подписью лучше воздержаться. Также следует отключить доступ к устройствам через Интернет.

***

3.02.2016

В SCADA-системах с поддержкой технологии WirelessHART обнаружена уязвимость

Специалисты компании Applied Risk обнаружили несколько уязвимостей в различных SCADA-продуктах, использующих технологию WirelessHART.

Как сообщает издание The Register, ошибки позволяют злоумышленникам манипулировать промышленными инструментами и нарушать целостность производственного процесса, пишет InternetUA.

WirelessHART – беспроводная сенсорная сетевая технология для систем АСУ ТП, работающая на основе протокола Highway Addressable Remote Transducer Protocol (HART). Продукты с поддержкой WirelessHART используются для мониторинга и контроля температуры, давления, влажности и прочих производственных показателей. Если в системе не используется технология активного мониторинга, злоумышленник сможет незаметно осуществить атаку.

Один из обнаруженных экспертами способов атаки существует из-за недостаточного обеспечения безопасности в так называемых «полевых устройствах 1 уровня» – различных датчиках и клапанах, используемых для наблюдения за производственными показателями. Специалисты Applied Risk в настоящее время разрабатывают набор WirelessHART Fuzzer, позволяющий обнаружить уязвимости в устройствах, работающих на основе данной технологии.

По словам основателя и главного консультанта по вопросам безопасности Applied Risk Д. Бухдады, в большинстве случаев ошибки в АСУ ТП остаются незамеченными на протяжении нескольких лет. «Атаки на SCADA-системы могут привести к огромному ущербу репутации компании. Предприятиям необходимо тщательно проверять и внедрять новые меры обеспечения безопасности», – отметил Д. Бухдада.

***

3.02.2016

Kaspersky предупреждает о новом опасном банковском трояне

«Лаборатория Касперского» сообщает, что вредоносная программа, которая была зафиксирована в середине прошлого года, представляет собой значительную угрозу для мобильного банкинга, пишет PaySpaceMagazine.

Первый вариант Asacub Trojan, обнаруженный в июне, был рассчитан на кражу информации, например, списков контактов, истории браузера, списков установленных приложений. Также вредоносная программа могла отсылать смс-сообщения и блокировать экран зараженного Android-устройства.

В новой версии появилось несколько новых, более опасных функций:

– инструменты для кражи денег – например, фишинговые страницы, которые имитируют мобильные версии банков;

– переадресация вызова и возможность рассылки USSD-сообщений.

Эти функции делают Asacub Trojan мощным инструментом для финансового мошенничества.

Троян ориентирован на клиентов украинских, российских и американских банковских мобильных приложений.

В течение одной недели антивирусная программа выявила более 6500 попыток заражения устройств пользователей. Это делает его самым популярным на сегодняшний день банковским трояном.

«Исходя из текущих тенденций, мы можем предположить, что в 2016 г., развитие и распространенность вредоносных программ для мобильного банкинга будет продолжать расти», – отметил старший аналитик «Лаборатории Касперского».

***

2.02.2016

Группировка Anonsec взломала внутренние сети NASA

Хакеры из группировки Anonsec взломали внутренние сети американского космического агентства NASA и похитили 250 ГБ данных о сотрудниках, полетах и миссиях организации. Злоумышленники также предположительно получили контроль над одним из дронов агентства, пишет InternetUA.

Похищенные данные включают имена, номера телефонов и адреса электронной почты 2414 сотрудников NASA, а также информацию о более чем 2 тыс. полетов. Хакеры также получили доступ к 600 видеозаписям агентства.

Подробную информацию о взломе злоумышленники разместили на сайте Pastebin. Участники группировки предположительно приобрели данные для доступа к одному из компьютеров агентства. В руках взломщиков оказались логин и пароль от пользовательской учетной записи.

Некоторые из компьютеров NASA работали под управлением устаревших версий Debian, подверженных нескольким уязвимостям. Взломщики смогли получить доступ к уязвимым ПК и просканировали сеть на предмет учетных записей с логином и паролем «root». Меньше чем за секунду злоумышленники смогли войти в одну из записей и создать сетевую карту IT-инфраструктуры NASA.

Используя полученные данные, участники группировки получили доступ к нескольким исследовательским центрам космического агентства, включая Исследовательский центр им. Д. Гленна, Центр космических полетов Годдарда и Летно-исследовательский центр им. Армстронга.

Злоумышленники также якобы перехватили управление дроном NASA Global Hawk, использующегося для проведения исследований на высоте и длительных полетов. На момент предположительного взлома беспилотник летел над Атлантическим океаном.

***

2.02.2016

Каждое двадцатое Android-устройство взломано

Многие пользователи и эксперты уверены, что мобильная платформа Apple iOS безопаснее, чем Android. Также считают и специалисты из Duo Security. Согласно их исследованиям, только на одном из десяти Android-устройств в компаниях и на предприятиях предустановлено шифрование, что подвергает риску их данные, пишет InternetUA.

Кроме того, каждое третье устройство не использует код на экране блокировки, позволяя легко получить доступ к ним. Для сравнения, среди айфонов пароль не используется на одном устройстве из двадцати. Каждое двадцатое Android-устройство, которые пользователи применяют на работе, рутировано, а среди аппаратов iPhone взломаны только одно из 250.

Главной проблемой продолжает оставаться фрагментация экосистемы Android, поскольку многочисленные производители и операторы связи не слишком оперативно обновляют устройства или не обновляют вовсе.

Duo Security насчитала 20 % устройств на версии Android 5.1.1, почти втрое больше чем на 6.0. Для сравнения, у Apple почти половина смартфонов iPhone работают на iOS 9.2. 32 % обладателей устройств на Android работают с версиями 4.x, где есть две уязвимости Stagefright, окончательно закрытые Google совсем недавно. 9 из 10 Android-устройств не защищены перед этой глобальной уязвимостью, что делает их не слишком привлекательными для рабочего окружения и хранения важной информации. Аппараты iPhone на предприятиях вдвое популярнее, чем Android.

***

3.02.2016

ЕС усилит контроль за передачей данных Facebook и Google

Евросоюз и Соединенные Штаты Америки заключили новое соглашение о передаче данных, сообщает podrobnosti.ua со ссылкой на Deutsche Welle.

Еврокомиссар по вопросам юстиции В. Юрова во вторник сообщила, что после длившихся несколько месяцев переговоров был подписан новый документ, предполагающий усиление контроля за передачей данных о европейских гражданах такими интернет-гигантами из США, как Facebook и Google.

Данное соглашение заменит действовавшее последние 15 лет двустороннее соглашение Safe Harbor, признанное в октябре 2015 г. европейским судом в Люксембурге неправомерным.

Предыдущий договор был отменен в результате коллективного иска, инициированного жителем Австрии против Facebook, в котором компания обвинялась в нарушении законодательства ЕС о защите личных данных.

Жалоба на Facebook возникла в ответ на информацию о том, что американские спецслужбы могут легко получить доступ к личным данным пользователей, поскольку социальная сеть хранит личные данные пользователей на серверах в США.

***

4.02.2016

Опасный вирус атаковал пользователей крупнейшего онлайн-магазина

Мошенники начали распространять опасный троян под названием Bayrob при помощи электронной рассылки. Письма приходят якобы от популярного во всем мире интернет-ритейлера Amazon, поэтому многие пользователи даже не подозревают об опасности, сообщает пресс-служба антивирусной компании Eset, пишет InternetUA.

Зараженное приложение находится во вложении под видом ZIP-архива. При попытке открыть файл пользователь получает ошибку, в которой сказано, что эта программа не совместима с действующей версией Windows. Тем не менее, в этот момент троян уже начал действовать.

После взлома компьютера Bayrob начинает сбор пользовательских данных: он находит информацию о банковских картах пользователя, его логинах и паролях от онлайн-банкинга. Затем вредоносное приложение отправляет все полученные данные мошенникам.

Чтобы получить желаемую информацию, троян обращается к удаленным серверам: для этого Bayrob генерирует различные URL-адреса. Как оказалось, один из таких адресов зарегистрирован японским представительством Amazon. Однако аналитики не обвиняют интернет-ритейлера: есть вероятность, что данный сервер был арендован третьими лицами.

Стоит отметить, что вредоносное приложение впервые заметили еще в 2007 г., однако активная деятельность трояна началась лишь в 2015 г.: тогда от заражения пострадали множество пользователей из Европы, Южной Африки, Австралии и Новой Зеландии. В новом году атаки вируса сильнее всего затронули Испанию, Австрию, Германию и Италию.

***

4.02.2016

Специалисты прогнозируют всплеск активности вредоносного ПО для Android

Количество угроз для ОС Android продолжает увеличиваться. Согласно отчету ИБ-компании Quick Heal Technologies (QHT), в III квартале 2015 г. было обнаружено 1,2 млн новых образцов вредоносного ПО для Android. За три месяца вирусописатели разработали 220 новых семейств вредоносов и модифицировали 147 существующих видов мобильных угроз. По состоянию на конец 2015 г. эксперты насчитали 600 уникальных семеств вредоносного ПО для самой популярной мобильной ОС в мире, пишет InternetUA

По словам технического директора QHT С. Каткара, рост количества угроз для Android не прекращается уже несколько кварталов. Обычным

пользователям и организациям придется уделять все большее внимание безопасности мобильной ОС.

Одной из основных проблем безопасности Android является фрагментированность операционной системы – огромное количество устройств все еще работают под управлением устаревшей версии мобильной ОС. В связи со сложившейся обстановкой вирусописатели могут создавать вредоносное ПО, эксплуатирующее неисправленные в ранних версиях системы уязвимости.

По мнению С. Каткара, в 2016 г. значительно увеличится количество рекламного ПО. Согласно данным QHT, более 66 % всего вредоносного ПО для ОС Android отображает рекламные объявления. В будущем, считает С. Каткар, данная тенденция лишь сохранится.

Не все загружаемые с Google Play приложения безопасны. Ошибки в магазине приложений позволяют злоумышленникам обходить механизмы защиты и загружать вредоносное ПО напрямую на Google Play. Некоторые виды вредоносного ПО имитируют легитимные программы – например, официальные приложения банковских клиентов.

По мнению С. Каткара, компаниям необходимо постоянно быть на страже. Злоумышленники разрабатывают все более сложные способы получения доступа к Android-устройствам и похищения персональной информации о пользователях.

***

4.02.2016

Закарпатська область найбільше заражена вірусами

За даними української антивірусної лабораторії Zillya!, абсолютним лідером вірусної активності у 2015 р. стали Adware – програми, що демонструють рекламу, пише Prozak.info.

Зараження по регіонах

У 2015 р. показники зараження за даними за минулий рік мають виражений територіальний характер.

Серед лідерів знову відзначається Закарпатська область із показником відсотка зараження в 45 одиниць.

Треба зазначити, що Закарпатська область продовжує залишатися в лідерах щодо небезпечності кіберпростору. Також до трійки лідерів увійшли Івано-Франківська область із показником у 43,02 % зараження ПК, а також Дніпропетровська – 42,03 %.

Слід наголосити, що рівень зараження в Києві наблизився до показників найнебезпечніших регіонів країни. Кількість атакованих ПК, на яких встановлено українську антивірус, у цьому регіоні становила 40,15 % від кількості всіх комп’ютерів.

Adware: порог эпідемії

Звіт вірусної активності за 2015 р., за даними антивірусної лабораторії Zillya!, підтвердив тенденцію зростання частки рекламних модулів (adware) серед загальної маси вірусних загроз.

Так, порівняно з 2014 р. активність даного виду шкідливих програм в Україні минулого року зросла на 12,8 %, становивши близько 49 % від загальної кількості загроз.

Варто зазначити, що найбільший сплеск активності припадає на IV квартал 2015 р., коли кількість Adware в загальній масі вірусних погроз в Україні зросла на 17 %, досягнувши показника в 51 % від загальної кількості виявлених шкідливих програм.

Троянці: шифрують і крадуть

Серед усіх вірусних погроз, згідно зі статистикою антивірусної лабораторії, 21 % займають троянські програми, різного характеру і виду дій. У той самий час варто відзначити, що у 2015 р. особливе зростання активності показали трояни шифрувальники, зокрема CTB.Locer.

Відзначився цей період і різким зростанням виявлення троянів-шифрувальників, орієнтованих на бухгалтерський сектор підприємств. Зловмисники використовують методи соціальної інженерії, які дають змогу переконати користувача запустити заражену програму або відкрити файл, тим самим заразивши свій ПК «вірусом», який зашифрує на ньому всі файли.

19 % всіх атак на персональні ПК українських користувачів здійснювалися за допомогою програм даного типу. Варто відзначити, що ці дані свідчать про деяке зниження активності в Україні троянських програм (у III кварталі 2014 р. – 33 % від усіх загроз) в загальній масі вірусних погроз.

«Мерзенна п’ятірка» малварі 2015

Найбільш активними у 2015 р. були такі ТОП-5 сімейств шкідливого програмного забезпечення. Варто відзначити, що два з них Adware.Agent.Win32 і Backdoor.PePatch.Win32 також входили в ТОП-5 у 2014 р.

1. Adware.Agent.Win32 – велике сімейство рекламного шкідливого ПО, яке встановлюється на комп’ютер таємно від користувача і виявляє свою активність у вигляді нав’язливих спливаючих вікон з рекламою або підміною результатів пошуку.

2. Adware.BrowseFox.Win32 – дані програми володіють приховати функціоналом, таким як показ спливаючої реклами, відкриття додаткових вікон в браузері і перенаправлення користувача на рекламні сайти і сайти із шкідливим програмним забезпеченням. Також, потай від користувача, на комп’ютер завантажуються інші рекламні модулі.

3. Adware.CrossRider.Win32 – сімейство кросплатформенних рекламного ПЗ. В основному Adware.Crossrider використовується для чорного SEO, тобто для розкрутки або підвищення рейтингу сайту, за рахунок перенаправлення на нього користувачів заразилися Adware.Crossrider.

4. Adware.ConvertAd.Win32 – нав’язливе рекламне програмне забезпечення. При перегляді веб-сторінок показує квадратні спливаючі вікна з рекламою. Крім того, на сторінках можуть з’являтися банери з рекламою, а

пошукові посилання підміняються на рекламні. Крім того, на комп'ютер користувача будуть завантажуватися інші програми рекламного характеру.

5. Backdoor.PePatch.Win32 – даний клас програм призначений для прихованого віддаленого керування чужим комп'ютером. За своєю функціональністю Backdoor багато в чому нагадують різні системи віддаленого адміністрування, що розробляються фірмами-виробниками програмних продуктів.

***

3.02.2016

Активность вирусов и червей в 4 квартале 2015 года возросла на 236 %

Компания Solutionary опубликовала отчет по угрозам безопасности за IV квартал 2015 г. В указанный период эксперты зафиксировали рост активности вредоносного ПО (вирусы и черви) на 236 %. По сравнению со второй четвертью прошлого года разведывательная деятельность злоумышленников возросла на 88 %, пишет InternetUA.

В последнем квартале предыдущего года увеличилась мощность некоторых видов атак, в том числе на уровне веб-приложений и ориентированных на конкретное приложение. За последние две недели IV квартала прошлого года злоумышленники чаще всего пытались атаковать сайты, использующие неисправленные версии Joomla!.

Злоумышленники по-прежнему продолжают активно эксплуатировать ShellShock – 77 % инцидентов безопасности, зафиксированных в IV квартале 2015 г., были связанны с даной уязвимостью.

США, Китай, Франция, Италия и Великобритания остаются главными странами-источниками вредоносного ПО. На долю данных государств пришлось 95 % от общего количества вредоносов, обнаруженных в IV квартале 2015 г.

В указанный период также был зафиксирован рост числа атак на Android-устройства. Как поясняют исследователи, злоумышленники активно эксплуатируют уязвимости в данной операционной системе. За последний год в ОС было обнаружено 130 ошибок – больше, чем за предыдущие шесть лет вместе взятые. По данным экспертов, 76 % всех Android-устройств работают под управлением значительно устаревших версий операционной системы. Порядка 37 % гаджетов используют версии ОС, выпущенные более двух лет назад.

***

5.02.2016

Детские умные часы и IoT-игрушки небезопасны для маленьких пользователей

Исследователи компании Rapid7 в очередной раз доказали, что большинство «умных» гаджетов на самом деле сложно назвать умными. Эксперты обнаружили ряд неприятных уязвимостей в игрушках компании Fisher-Price, а также детских гаджетах стартапа hereO, пишет InternetUA.

Fisher-Price

В конце 2015 г. исследователи в области информационной безопасности раскритиковали интерактивную куклу Hello Barbie, которую можно превратить в идеальный шпионский гаджет. Но, очевидно, говорящая Barbie была лишь первым тревожным звоночком. Похожее решение представила и именитая компания Fisher-Price, выпустив линейку интерактивных плюшевых игрушек. Умные медведи и обезьяны способны общаться с детьми посредством встроенного динамика и самообучаться. Чтобы ускорить процесс обучения, можно подключить плюшевого зверя к сети. Родители при этом могут контролировать происходящее через мобильное приложение.

По словам исследователей, во время общения с серверами Fisher-Price, игрушки используют очень слабый API. Сообщения не проходит должной верификации, что позволяет атакующему сформировать и отправить на сервер запрос, который, по идее, не должен быть обработан, но его обработка все равно происходит. В итоге хакер получает доступ к конфиденциальным сведениям о ребенке, в том числе доступ к его профилю в системе и информации об игрушках, которые привязаны к данному аккаунту. Личные данные включают в себя имя ребенка, дату его рождения и информацию об активном языке. Кроме того, можно видеть статус подключенных к аккаунту игрушек (то есть узнать, играют ли с ними сейчас) и менять его, отключая игрушки от профиля.

Данные проблемы были обнаружены специалистами Rapid7 еще в ноябре 2015 г. Компания Fischer-Price уже выпустила исправление для своих интерактивных игрушек, но сделано это было лишь в середине января текущего года.

hereO

Платформа компании hereO более молода: первые устройства пользователи получили всего месяц назад. В 2014 г. стартап hereO успешно собрал сумму, необходимую для начала производства детских гаджетов, на Ingiegogo.

Устройства hereO – это семейство умных часов для самых маленьких, со встроенной функцией GPS-маяка. Девайсы поставляются вместе с мобильным приложением, которое позволяет родителям всегда быть в курсе, где находится их чадо, отслеживая его перемещения.

Как и многие другие IoT-устройства, гаджеты hereO оказались далеки от совершенства. Эксперты Rapid7 обнаружили уязвимость в API веб-сервиса, которая позволяла злоумышленнику добавить себя в «круг семьи» – группу пользователей, члены которой имеют доступ к таким функциям, как геолокация, обмен сообщениями и так далее. Прописав себя в список доверенных лиц, атакующий мог не только отслеживать местонахождение

чужого ребенка в режиме реального времени и просматривать лог его перемещений. Хакер также мог отправлять членам группы сообщения и отслеживать местоположение других членов семьи, через GPS их в смартфонах.

Проблема была устранена 15 декабря прошлого года, тогда как баг исследователи Rapid7 нашли еще в октябре 2015 г.

Похоже, недавний скандал, развернувшийся вокруг другого производителя детских гаджетов – компании VTech, ничему не учит производителей. Создавая интерактивные игрушки и гаджеты для маленьких пользователей, компании, похоже, в последнюю очередь думают о безопасности.

«В последние полгода мы наблюдали раскрытие множества уязвимостей в IoT-игрушках, – рассказывает М. Станислав, специалист Rapid7. – Мы ожидаем, что эта тенденция сохранится, так как на рынке будут появляться все новые игрушки. Я не могу не подчеркнуть, что производителям IoT-игрушек (и производителям IoT-устройств в целом) сейчас крайне важно задуматься о том, что работа над безопасностью должна являться важным этапом процесса разработки».

***

4.02.2016

Злоумышленники атакуют сайты на базе WordPress с помощью нового вредоносного ПО

ИБ-специалист Sucuri Д. Синегубко обнаружил вредоносную кампанию, нацеленную на сайты на основе WordPress. Как сообщается в блоге компании, злоумышленники с помощью специального кода вставляют на ресурсы бэкдоры и повторно инфицируют даже очищенные от вредоносного ПО страницы, пишет InternetUA.

Хакеры внедряют зашифрованный вредоносный код во все JavaScript-сценарии на целевых сайтах под управлением WordPress. По словам Д. Синегубко, вредоносное ПО устанавливает множественные бэкдоры в различные файлы на веб-сервере и регулярно обновляет встроенный код. В результате сайт оказывается постоянно инфицирован вредоносом, а попытки удаления вируса оказываются тщетными.

Опасности подвержены все JavaScript-сценарии на всех доменах в пределах одной и той же учетной записи хостинга. Для устранения угрозы понадобиться изолировать все сайты на учетной записи и удалить вредоносное ПО.

Вирус использует несколько вариаций зашифрованного кода с одинаковой структурой. На зараженных ПК устанавливается рекламный файл cookie, вставляющий на посещаемые сайты модифицированные невидимые фреймы <iframe>.

По словам Д. Синегубко, злоумышленники активно используют технологию «затенения доменов». Преступники могут добавить вредоносные

поддомены к легитимным доменам второго уровня. Подобные поддомены используются для распространения вредоносного ПО – например, набора эксплоитов Angler.

***

4.02.2016

Хакеры взломали 20 млн аккаунтов «облачного» сервиса Alibaba

Китайские хакеры атаковали более 20 млн активных учетных записей пользователей «облачного» сервиса компании Alibaba Group – крупнейшей площадки Taobao. Об этом сообщает InternetUA со ссылкой на Reuters.

Представитель Alibaba заявил, что специалисты обнаружили атаку на первичной стадии и обратились к пользователям с просьбой изменить пароли. Кроме того, компания работает в тесном сотрудничестве с полицией в рамках расследования.

По данным китайского Министерства по управлению интернетом, хакеры начали применять схему с середины октября прошлого года, после чего были выявлены в ноябре. В настоящее время злоумышленники задержаны.

Предположительно, взлом мог произойти из-за уязвимости в платформе Alibaba, но пресс-секретарь утверждает, что система под надежной защитой.

***

4.02.2016

Администрация eBay не собирается исправлять опасную уязвимость

Исследователи компании Check Point обнаружили серьезную уязвимость в онлайн-платформе eBay. Техника эксплуатации бага получила имя JSF**k. Она позволяет обойти фильтры eBay. То есть злоумышленник может открыть на eBay собственный магазин, добавить в поле описания товара подготовленный определенным образом вредоносный JavaScript, а затем пожинать плоды своих трудов. Более того, 16 января текущего года представители eBay заявили, что не планируют исправлять данную уязвимость, пишет InternetUA.

15 декабря 2015 г. опасную брешь обнаружил сотрудник Check Point Р. Заикин. Прошло уже более полутора месяцев, но компания eBay держит слово и, похоже, действительно не собирается исправлять баг. В связи с этим специалисты Check Point хотя и раскрыли информацию о найденной проблеме, технические подробности пока не разглашаются полностью.

Суть проблемы заключается в следующем: был найден способ, позволяющий обмануть фильтры eBay, которые отвечают за распознавание вредоносного кода. Из-за этого хакеры могут создавать на eBay якобы легитимные страницы магазинов, внедрять в них вредоносный код, и открытие этих страниц приведет к весьма неприятным последствиям.

Для обхода фильтров eBay используется техника JSF**k. Проект, давший имя этому вектору атаки, был создан не компанией Check Point, его шутки ради придумал разработчик М. Клеппе. Код здесь изменяется до неузнаваемости и состоит только из шести символов: [ ] ( ) ! и +. Записывая данные таким образом, в итоге можно получить работающий код на JavaScript, который не распознают практически никакие механизмы защиты.

Благодаря технике JSF**k, вредоносный код можно беспрепятственно внедрить в поле описания товара на eBay. Системы защиты аукциона запрещают использование iFrames и HTML тегов на страницах, но против обфускации JavaScript они бессильны. Кроме того, с помощью JSF**k злоумышленники могут создать код, который будет загружать дополнительный JS-код с их сервера.

По сути, хакеры ограничены только собственной фантазией. Попав на такую страницу, пользователь может стать жертвой фишинга и кражи личных данных. К примеру, на зараженной eBay-странице пользователю предлагают скачать мобильное приложение eBay со специальной скидкой. Все выглядит легитимно и безопасно, но если жертва подтверждает скачивание, на ее устройство загружается малварь.

Так как представители eBay официально заявили, что не считают возможность проведения подобных атак уязвимостью, специалисты Check Point могут лишь выразить надежду, что компания передумает. Помимо описания проблемы, исследователи опубликовали два proof-of-concept видео.

***

4.02.2016

Бета-версия Flyme OS содержит вредоносный код

В течение достаточно долгого времени итальянские фанаты Meizu пытались изучить код Flyme OS. В результате им удалось выяснить, что приложения в бета-версии прошивки содержат вредоносный код и вирусы. Обнаружить это удалось во время очередного тестирования системы при помощи службы VirusTotal. Ещё один тест, проведённый несколькими месяцами ранее, также обнаруживал похожие вирусы в предыдущей версии ОС, пишет InternetUA.

До настоящего времени компания Meizu ещё не сделала никаких официальных заявлений, объясняющих присутствие вредоносного кода, однако итальянский дистрибьютор компании заявил, что результаты исследований сфальсифицированы. Правда, компания AVG уже подтвердила достоверность опубликованных скриншотов тестирования.

Не исключено, что вредоносный код содержится только в бета-версиях Flyme OS и только для того, чтобы автоматически отправлять разработчикам информацию об использовании приложений и ошибках. Следует иметь в виду, что наличие этого кода может привести к повышенному использованию данных

смартфона, более быстрой разрядке аккумулятора, а также отправке персональных данных на серверы Meizu.

***

5.02.2016

В продуктах Cisco исправлен ряд опасных уязвимостей

3 февраля Cisco выпустила исправления безопасности для нескольких продуктов, устраняющие ряд уязвимостей. Ошибки позволяли злоумышленнику изменить данные на системе, осуществить DoS-атаку и изменить пароль любой учетной записи, включая аккаунт администратора, пишет Центр информационной безопасности.

Одна из уязвимостей (CVE-2016-1302) затрагивала продукт Cisco Application Policy Infrastructure Controller. Ошибка логики в механизме управления доступом на основе ролей позволяла удаленному аутентифицированному злоумышленнику изменить настройки устройства. Уязвимость затрагивала Cisco APIC с прошивкой версий до 1.0(3h) и 1.1(1j), а также коммутаторы Cisco Nexus 9000 Series ACI Mode с прошивкой версий до 11.0(3h) и 11.1(1j).

Коммутаторы Nexus 9000 также были подвергнуты уязвимости, позволяющей осуществить DoS-атаку (CVE-2015-6398). Удаленный пользователь мог вызвать перезагрузку устройства, отправив на коммутатор специально сформированные пакеты ICMP. Ошибка была исправлена в обновлении прошивки до версии 11.0(1c).

В Cisco ASA-CX и Cisco Prime Security Manager (PRSM) была обнаружена опасная уязвимость (CVE-2016-1301), позволяющая сбросить пароль к учетной записи администратора. Ошибка существовала из-за недостаточной проверки запросов на смену пароля. Удаленный аутентифицированный пользователь мог задать новый пароль для любой учетной записи с помощью специально сформированного HTTP-запроса. Ошибка была исправлена в обновлении прошивки до версии 9.3.1.1(112).

Также компания опубликовала несколько бюллетеней безопасности, описывающих менее серьезные уязвимости в других продуктах. Например, в приложении Jabber Guest было исправлено несколько ошибок, позволяющих осуществить XSS-атаку.

***

5.02.2016

Неизвестный взломал авторов трояна Dridex, заставив их распространять антивирус

Ботнет Dridex, распространяющий одноименный банковский троян, оказался взломан неизвестным доброжелателем. Анонимный шутник заставил

ботнет «заражать» пользователей антивирусом Avira, пишет Центр информационной безопасности.

Хотя в конце 2015 г. ФБР провело операцию по прекращению деятельности ботнета Dridex, сеть все равно осталась на плаву и продолжила распространять малварь. Как правило, данный ботнет используется для рассылки спама. Письма содержат вредоносные вложения, в основном в виде документов Word с нехорошими макросами. Как только жертва открывает такой файл, срабатывает макрос, и с сервера злоумышленников скачивается пейлоуд. Проникнув в систему, Dridex создает за зараженной машине кейлоггер, а также использует невидимые редиректы и веб-инъекции для банковских сайтов.

«Вредоносный контент, загружающийся по URL злоумышленников, был заменен на оригинальную, самую свежую версию инсталлятора Avira (вместо обычного загрузчика Direx)», – рассказал один из экспертов Avira.

Таким образом, жертвы ботнета в последнее время получали не банковский троян, а актуальную, подписанную копию антивируса. В компании Avira сообщают, что им неизвестно, кто провернул этот трюк, и какие цели он преследовал. Свою причастность к инциденту разработчики антивируса опровергают.

«Какой-то whitehat мог проникнуть на зараженный веб-сервер, используя те же уязвимости, которые применяют сами авторы малвари. Он мог подменить их вредоносные штуки инсталлятором Avira», – строят теории разработчики, добавляя при этом, что подобные действия считаются противозаконными во многих странах мира.

Стоит отметить, что уже не первый подобный случай. Ранее инсталлятор Avira уже добавляли в состав вымогателей CryptoLocker и Tesla.

***

5.02.2016

Android-троянцы научились внедряться в системные процессы

В феврале 2016 г. специалисты компании «Доктор Веб» выявили целый комплект вредоносных приложений для ОС Android, обладающих широчайшим спектром функциональных возможностей, пишет ITnews.

Этот набор состоит из трех действующих совместно троянцев, получивших наименования Android.Loki.1.origin, Android.Loki.2.origin и Android.Loki.3 соответственно. Первый из них загружается с помощью библиотеки liblokih.so, детектируемой Антивирусом Dr.Web для Android под именем Android.Loki.6. Эта библиотека внедряется в один из системных процессов троянцем Android.Loki.3 – в результате Android.Loki.1.origin получает возможность действовать в системе с привилегиями пользователя system. Android.Loki.1.origin представляет собой службу, обладающую широким набором функций: например, троянец может скачать из официального каталога Google Play любое приложение с помощью специальной ссылки,

содержащей указание на учетную запись той или иной партнерской программы, благодаря чему злоумышленники получают возможность извлекать доход.

Среди других возможностей Android.Loki.1.origin стоит отметить следующие:

– установка и удаление приложений;

– включение и отключение приложений, а также их компонентов;

– остановка процессов;

– демонстрация уведомлений;

– регистрация приложений как Accessibility Service (службы, отслеживающей нажатия на экран устройства);

– обновление своих компонентов, а также загрузка плагинов по команде с управляющего сервера.

Вторая вредоносная программа из обнаруженного аналитиками «Доктор Веб» комплекта – Android.Loki.2.origin – предназначена для установки на зараженное устройство различных приложений по команде с управляющего сервера, а также для демонстрации рекламы. Однако обладает этот троянец и шпионскими функциями – при запуске он собирает и отправляет злоумышленникам следующую информацию:

– IMEI инфицированного устройства;

– IMSI инфицированного устройства;

– mac-адрес инфицированного устройства;

– идентификатор MCC (Mobile Country Code) – мобильный код страны;

– идентификатор MNC (Mobile Network Code) – код мобильной сети;

– версия ОС на инфицированном устройстве;

– значение разрешения экрана;

– данные об оперативной памяти (общий объем и свободный объем);

– версия ядра ОС;

– данные о модели устройства;

– данные о производителе устройства;

– версия прошивки;

– серийный номер устройства.

После отправки этой информации на управляющий сервер троянец получает в ответ конфигурационный файл, содержащий необходимые для его работы данные. Через определенные промежутки времени Android.Loki.2.origin обращается к управляющему серверу для получения заданий и во время каждого сеанса связи дополнительно передает злоумышленникам следующие данные:

– версия конфигурационного файла;

– версия сервиса, реализованного троянцем Android.Loki.1.origin;

– язык операционной системы;

– страна, указанная в настройках операционной системы;

– информация о пользовательской учетной записи в сервисах Google.

В ответ Android.Loki.2.origin получает задание либо на установку того или иного приложения (они в том числе могут загружаться из каталога Google

Play), либо на отображение рекламы. Нажатие на демонстрируемые троянцем уведомления может привести либо к переходу на определенный сайт, либо к установке приложения.

***

7.02.2016

Раскрыты актуальные цены на кражу банковских данных и «угон» аккаунтов в соцсетях

Исследователи по безопасности из компании EMC раскрыли расценки хакеров на услуги по краже различных персональных данных. Наиболее высокую стоимость имеет информация о банковских счетах и прикрепленных к ним картах, пишет InternetUA.

Кража банковских данных

Одной из наиболее дорогих услуг в прейскуранте хакера является кража данных о дебетовой карте и прикрепленном к нему банковском счете. За это на черном рынке злоумышленники просят от 150 до 300 дол. Стоимость же поддельной пластиковой карты для обналичивания колеблется от 10 дол. за карту с магнитной полосой до 20 дол. за карту с чипом.

Если же речь идет об электронном кошельке с прикрепленной к нему кредитной картой, стоимость падает до 15 дол. плюс 10 % от баланса карты. Стоимость обналичивания с таких счетов оценивается в 25–30 % от суммы перевода. Такие цифры опубликовала корпорация EMC по результатам исследования, проведенного специалистами подразделения RSA.

«Угон» аккаунтов в соцсетях

Одна из самых дешевых услуг – кража логина и пароля от учетной записи в социальной сети. Если у жертвы не менее 500 друзей, его аккаунт оценивается в 7,5 дол. Исследователи не уточнили, как стоимость варьируется в зависимости от количества друзей.

DDoS-атаки

В EMC сообщили, сколько в среднем на черном рынке стоит проведение DDoS-атаки (Distributed Denial of Service – распределенной атаки на сайт, в результате которой он перестает реагировать на запросы пользователей). По данным исследователей, стоимость такой атаки составляет 30 дол. за один час.

Поддельные документы

Наконец, специалисты RSA также выяснили, сколько стоит купить на черном рынке идентификационные документы. Если этот документ на французском языке, стоимость составит 10 дол., на испанском – 13–15 дол., на итальянском – 10 дол., на английском – 15 дол. В компании не уточнили, о каких именно типах документов идет речь.

Черный рынок

«Черный рынок представляет собой реальный бизнес, основанный на тех же экономических принципах, на основе которых функционирует любая компания», – отметили в EMC.

Исследователи по безопасности добавили, что украденная информация имеет такое свойство, как актуальность. И спустя некоторое время она «портится», что снижает ее ценность практически до нуля. Например, если сразу после взлома информация о кредитных картах продается по цене 50–100 дол. за штуку, то затем, только лишь бы найти покупателя, злоумышленник готов отдать ее за 1 дол.

***

6.02.2016

Злоумышленники распространяют троян через макросы Microsoft Office

С недавних пор злоумышленники возродили интерес к макросам Microsoft Office, активно используемым для распространения банковских троянов, а в последнее время и вредоноса BlackEnergy. По информации исследователей из американской компании zScaler, данную технику применяют операторы трояна Kasidet, также известного как Neutrino, пишет InternetUA.

Вредоносные макросы Office распространяются в виде вложений в фишинговые письма. По наблюдениям zScaler, за последние две недели активность вредоносной спам-кампании значительно возросла. Помимо Kasidet, тот же VBA-дроппер загружает банковский троян Dridex.

Вредонос Kasidet известен с 2013 г. и до недавнего времени использовался для осуществления DDoS-атак. Предположительно, в сентябре прошлого года авторы вредоносного ПО добавили функции хищения данных.

По сравнению с более ранними версиями Kasidet, обнаруженный исследователями вариант обладает более широкими возможностями. Вредонос способен похищать конфиденциальную информацию как из браузеров (перехватом API), так и из памяти PoS-систем. Помимо прочего, Kasidet собирает сведения о названии и версии системы, наличии антивируса и т. д. Все похищенные данные вредонос отправляет на C&C-серверы из списка, содержащегося в коде в виде зашифрованных URL.

Совместная загрузка Kasidet и Dridex вовсе не указывает на взаимосвязь между двумя кампаниями. «Вредоносные документы Malicious Office – популярные у вирусописателей векторы доставки полезной нагрузки. Авторы Dridex используют данную технику уже больше года. Было интересно обнаружить кампанию с применением похожих методов для распространения Kasidet», – отметили исследователи.

***

6.02.2016

Хакеры нашли новый способ взлома iPhone и iPad

Эксперты из компании Vulnerability Lab обнаружили новый способ взломать украденные iPhone или iPad. Благодаря найденной уязвимости хакеры

могут разблокировать «запароленное» устройство в домашних условиях, пишет InternetUA.

Опасная уязвимость работает на телефонах iPhone 5 и 6, а также на планшетах iPad 2 с операционной системой iOS 8.2 или выше. «Дыра» в системе позволяет хакерам обойти пароль на устройстве путем обновления приложений и выполнения других несложных действий, из-за чего на гаджетах начинается бесконечный цикл. Для подтверждения сотрудник компании Б. Мейри выложил подробную инструкцию по взлому «айфонов» и «айпэдов» на своем YouTube-канале.

В Vulnerability Lab отметили, что известили компанию Apple о найденной уязвимости еще в октябре прошлого года, однако купертиновцы до сих пор не закрыли опасную брешь в системе.

***

6.02.2016

Google будет предупреждать о скачивании вирусов

Компания Google будет предупреждать пользователей своих браузеров о скачивании вредоносных приложений, скрытых под видом антивирусов, обновлений операционной системы и прочего полезного софта, пишет InternetUA.

Обычно уведомления о скачивании софта появляются на недобросовестных или зараженных сайтах – пользователю показывается сообщение о том, что его устройство заражено либо его операционная система устарела. Некоторые пользователи верят этим сообщениям, скачивают поддельный софт, устанавливают его, а затем сталкиваются с рядом проблем – например, с пропажей денег со счета мобильного телефона или кражей паролей, номеров банковских карт и прочей чувствительной информации. На сайте Google появилась инструкция для веб-мастеров, в которой рассказано, что нужно сделать, чтобы не попасть под блокировку этим расширением.

Начиная с этой недели, в браузере Chrome будет автоматически активировано расширение Safe Browsing, которое будет защищать пользователя от скачивания подозрительного софта на сомнительных сайтах.

Ранее подобная функция появилась в мобильной версии «Яндекс.Браузера» – это приложение предупреждает пользователя, когда тот или иной сайт пытается подписать его на платные услуги и списать деньги со счета мобильного телефона. Пользователю предлагается либо покинуть сайт, либо согласиться с оплатой.

***

6.02.2016

Инженер Google обнаружил критические уязвимости в «безопасных» браузерах

Инженер по вопросам безопасности из Google Project Zero Т. Орманди опубликовал доклад об обнаруженных не так давно критических уязвимостях в ряде браузеров, которые являются форками Google Chromium. Речь идёт о таких популярных проектах, как Avast, Chromodo и Malwarebytes. По словам Т. Орманди, обнаруженные бреши в «безопасных» браузерах предоставляли хакерам прямой доступ к системе и носили чрезвычайно угрожающий характер. К счастью, по состоянию на 3 февраля, в двух браузерах из трёх «дыры» были закрыты соответствующими патчами безопасности. С другой стороны, эта новость выявила серьёзные погрешности со стороны сторонних разработчиков в вопросе обеспечения безопасности пользователей, пишет InternetUA.

В браузере Avastium Т. Орманди обнаружил возможность удалённого получения доступа к любому файлу в системе через специально подготовленную веб-страницу с исполняемым кодом JavaScript. Потенциально такая «дыра» позволяет извлекать куки и электронную почту. Проблема была впервые озвучена 8 декабря и устранена 3 февраля.

Похожая история приключилась с браузером Chromodo от Comodo Internet Security. По словам инженера безопасности, в Chromodo не выполняется правило ограничения домена и исполняемый код с одного сайта выполняется на другом. Кроме того, при установке Chromodo последний импортирует все сохраненные данные из предустановленного Chrome, включая линки, закладки, установки, куки, настройки DNS и многое другое. Директор Comodo Ч. Цинковски заявил, что новая версия браузера была выпущена с устраненными недостатками.

В случае с Malwarebytes Т. Орманди выяснил, что браузер загружает обновления не по безопасному каналу связи, что делает его уязвимым для атак типа Man-In-The-Middle. Атакующий может подменить код во время обновления и запустить его на компьютере жертвы. Руководство утверждает, что апдейт с исправлением будет выпущен в течение четырёх недель.

Google Project Zero призван выявлять уязвимости в браузерах, созданных на базе Chromium, и повышать их безопасность для пользователей.

***

8.02.2016

В продуктах Netgear обнаружили две уязвимости и выпустили для них модули Metasploit

В системе ProSafe Network Management 300, предназначенной для управления, диагностики и оптимизации работы сетевых девайсов, были обнаружены две опасные уязвимости, позволяющие полностью скомпрометировать систему. Оба бага до сих пор не устранены, но информацию о проблемах уже обнародовал CERT. После публикации CERT, нашедший уязвимости исследователь счел возможным выпустить два модуля для Metasploit, а также опубликовать детальные данные, пишет InternetUA.

Уязвимость CVE-2016-1524 позволяет злоумышленнику осуществить закачку произвольного файла, обратившись без авторизации к определенным Java-сервлетам NMS300. В свою очередь, CVE-2016-1525 предлагает возможность обхода каталога. Эксплуатируя эти проблемы, киберпреступник способен загрузить произвольный файл в корневую директорию сервера, а также получить доступ к любым файлам.

Так как исправлений для данных брешей пока нет, специалисты CERT рекомендуют администраторам заблокировать все недоверенные источники при помощь брандмауэра.

«Отправив специальный POST-запрос сервлету, злоумышленник может загрузить произвольный файл, который будет доступен с системными привилегиями из корневой директории NMS300: http://<IP>:8080/null<filename>, – гласит официальный бюллетень CERT.

[Вторая уязвимость] позволяет прошедшему аутентификацию злоумышленнику манипулировать параметром realName, путем отправки специального POST-запроса, вида http://<IP>:8080/data/config/image.do?method=add, для загрузки произвольного файла с сервера. Данный файл может быть загружен через http://<IP>:8080/data/config/image.do?method=export&imageId=<ID>, где <ID> возрастает на единицу каждый раз, когда файл загружается подобным образом».

Исходно обе уязвимости обнаружил специалист компании Agile Information Security П. Риберио. После того как CERT обнародовал бюллетень безопасности, П. Риберио счел, что пора и ему раскрыть информацию о проблемах, невзирая на отсутствие патчей. Также исследователь обнародовал и два готовых модуля для Metasploit, которые теперь облегчат жизнь как пентестерам, так и потенциальным злоумышленникам.

Ни специалисты CERT, ни П. Риберио не обладают информацией о том, ведет ли компания Netgear работу над устранением данных проблем.

***

8.02.2016

Хакеры обнародовали личные данные 20 тысяч агентов ФБР

Хакерская группа, представленная в Twitter как DotGovs, 8 февраля опубликовала контактные данные 20 тыс. сотрудников американского Федерального бюро расследований и 9 тыс. сотрудников Министерства нацбезопасности США. Об этом сообщает InternetUA со ссылкой на Motherboard.

В обнародованных файлах содержатся имена, должностные инструкции, телефонные номера и адреса электронной почты сотрудников ведомств. Взломщики утверждают, что получили доступ к личной информации работников Министерства нацбезопасности, взломав базу данных ведомства.

Запись в микроблоге сопровождает хештег #FreePalestine. Ранее под ником DotGovs публиковались призывы к США разорвать отношения с Израилем.

Таким образом, хакеры выполнили обещание, которое дали Motherboard 7 февраля. В тот день в редакцию издания поступило анонимное уведомление о намерении обнародовать эти данные.

Факт взлома расследуют в Министерстве юстиции. Его представитель П. Карр заявил, что похищение частных данных имело место, но пока «ничто не сигнализирует о том, что произошла кража важной личной информации».

***

9.02.2016

Японским хакерам удалось украсть 20 тысяч секретных файлов

В Японии неизвестные хакеры смогли похитить 20 тыс. информационных файлов, касающиеся оборонных, технологических и политических секретов. Сделать это им удалось с помощью использования вируса Emdivi, заражающего компьютеры для последующего извлечения сведений. Об этом рассказал телеканал NHK, ссылаясь на проведенное им самостоятельное расследование, пишет InternetUA.

NHK опросил представителей руководства подвергшихся атакам компаний, исследовательских институтов и официальных организаций. Выяснилось, что жертвами нападений стали порядка тысячи различных структур. Были похищены материалы оборонных фирм по поводу поставок оборудования за рубеж, а также конфиденциальные записки и расписания действий ряда политических деятеле, сообщает ТАСС. Среди прочего, были украдены пароли для доступа в электронную почту ассоциации органов местного самоуправления Японии.

Вирусом Emdivi в мае прошлого года был заражен 31 компьютер в Национальной пенсионной системе страны, из которой злоумышленники украли 1,25 млн единиц конфиденциальной информации.

***

9.02.2016

Новый вирус ворует переписку и записывает звонки в Skype

Исследователи из компании Palo Alto Networks обнаружили вирус T9000, который способен записывать разговоры в Skype и «красть» документы. Об этом эксперты рассказали на своем сайте, пишет InternetUA.

Обнаруженный вредонос T9000 представляет собой модификацию T5000, распространенного в 2013–2014 гг. Заражение им происходит через фишинговые письма с прикрепленными файлами формата RTF.

Один из модулей вируса нацелен на сбор информации из Skype. При запуске он выводит сообщение explorer.exe wants to use Skype, заставляя

пользователя согласиться на слежку. Если разрешение получено, он начинает копировать переписку, а также аудио- и видеоразговоры.

Также вирус может «красть» с компьютера файлы в формате doc, ppt, xls, docx, pptx и xlsx, в том числе со съемных носителей. Вдобавок троян дает злоумышленникам возможность передавать на компьютер команды на создание, перемещение и удаление файлов и папок, а также копирование содержимого буфера обмена.

Исследователи отметили, что вирус использует множество уловок, чтобы антивирусы не могли его распознать. Эксперты не сообщили, кто стоит за созданием трояна. Его предшественника – T5000 – связывали с группировкой Admin@338, которую называли «неофициальной киберармией Китая».

***

9.02.2016

«Доктор Веб» предупреждает: Trojan.Dyre по-прежнему опасен

Спустя чуть более двух месяцев после масштабной операции российских правоохранительных органов по пресечению деятельности преступной группировки, стоявшей за получившим в 2015 г. печальную известность троянцем Trojan.Dyre, о нем опять заговорили СМИ, пишет ITnews.

На этот раз речь идет чуть ли не о победе над этой вредоносной программой, терроризировавшей крупнейшие финансовые организации всего мира с лета 2014 г. Однако сами правоохранительные органы пока не спешат сообщить об успехах в борьбе с очередным творением киберпреступного мира.

Специалисты компании «Доктор Веб» на протяжении всего времени существования троянской программы Trojan.Dyre пристально следили за ее распространением, изучали инфраструктуру, которая была создана злоумышленниками. Прежде всего следует отметить, что в данном случае мы увидели «классический» пример реализации модели CAAS – crime-as-a-service (преступление как услуга). «Пользователи системы» получали билдер для генерации сэмплов троянца, который позволял часто менять его сигнатуру, делая его таким образом неуязвимым для антивирусных программ. При этом все данные, которые собирались троянцем на зараженных компьютерах, отправлялись на серверы владельцев Trojan.Dyre. Там они обрабатывались и заводились в административную панель, которая была доступна тем «пользователям», которые купили к ней доступ. Сама панель была разделена на несколько функциональных частей – управление ботами, поиск по логам. Кроме того, самих групп панелей было несколько. Все входящие данные анализировались фильтрами для получения интересующей мошенников информации (логины-пароли и т. д.).

Большой интерес представляет сама инфраструктура Trojan.Dyre, которая, как считают аналитики «Доктор Веб», является намного более сложной, чем инфраструктуры многих других нашумевших банковских троянцев. Обычно данные с зараженных компьютеров отсылаются троянцами

на сервер, где и развернута панель, с помощью которой злоумышленники управляют своими ботами. В случае же с Trojan.Dyre использовался целый набор различных технологий, который свидетельствовал о том, что разработавшая и воплотившая в жизнь этот проект преступная группа располагает довольно внушительными финансовыми и человеческими ресурсами. Так, приемом и обработкой данных от ботов занимались «самописные» серверы на .Net, а панели управления ботнетом были написаны с использованием php-фреймворка Kohana. Для хранения и обработки массивов данных, поступавших практически со всех концов света, использовались базы postgres и mysql, а также система полнотекстового поиска sphinx. Все входящие данные поступали на специальные фильтры, которые служили для выделения интересующей мошенников информации (логины, пароли, номера банковских счетов, персональные данные пользователей и т. д.). Для защиты серверов от обнаружения были использованы Tor-серверы, а также proxy-серверы, объединенные в сеть посредством openvpn. Отличительной чертой атаки с использованием троянца Trojan.Dyre было размещение первичных проксирующих «прокладок» на взломанных злоумышленниками роутерах, где соответствующим образом была изменена таблица маршрутизации. Взломы роутеров производились рутинным подбором паролей, с учетом того факта, что многие пользователи не заботятся о смене заводских настроек защиты роутеров, а некоторые вообще не рассматривают их как точку возможного проникновения во внутреннюю сеть.

Тем не менее, аналитики «Доктор Веб» смогли определить целый ряд конечных серверов, которые использовались злоумышленниками. Были вскрыты элементы инфраструктуры Trojan.Dyre, удалось реализовать синкхол некоторых серверов. Это позволило получать важную информацию, которую специалисты компании оперативно предоставляли ряду европейских банков, а также правоохранительным органам нескольких стран.

Несмотря на опубликованную в СМИ информацию, в «Доктор Веб» считают, что по поводу Trojan.Dyre еще не пришло время расслабляться. До сих пор аналитиками компании фиксируются спам-рассылки с сэмплами троянца, и имеются основания полагать, что не все серверы инфраструктуры прекратили свою работу. Скорее всего, в этой истории «продолжение следует».

***

10.02.2016

Франция запретила Facebook следить за незалогиненными пользователями

Франция потребовала от Facebook прекратить собирать сведения о поведении в Интернете европейских граждан, которые не являются пользователями соцсети, а также пересылать их личные данные в США. На выполнение требований компании дано три месяца. В противном случае она будет оштрафована, пишет InternetUA со ссылкой на Reuters.

Ранее аналогичные претензии администрации Facebook выдвинули Голландия и Бельгия. Недовольство политикой соцсети уже спровоцировало расследования в 28 странах Евросоюза.

Ультиматум французских регуляторов – первый конкретный шаг по приведению в действие решения Европейского суда, который в октябре прошлого года отменил прежнее соглашение о «безопасной гавани» между IT-компаниями, которые вынуждены хранить персональные данные пользователей и используют для этой цели США (The transatlantic Safe Harbour pact). Именно на него ссылается Facebook и тысячи других компаний, объясняя правомерность своих действий.

Три месяца, данные на выработку новых правовых механизмов регулирования обмена данными между США и Евросоюзом, истекли на прошлой неделе. Стороны подготовили альтернативный пакт, однако документ не был принят и, возможно, будет доработан в сторону ужесточения правил.

Как заявили во французской Национальной комиссии по информатике и гражданским свободам (CNIL), практика Facebook по внедрению файлов cookie без предупреждения пользователя о том, что он заходит на страницу соцсети, противоречит законодательству Франции. Регулятор также отметил, что у юзеров должна быть возможность запретить сбор их личных данных, которые затем используются для предложения им контекстной рекламы.

***

11.02.2016

От бэкдора Adwind пострадало более 440 тыс. пользователей по всему миру

От деятельности многофункционального вредоносного ПО Adwind, также известного как AlienSpy, Frutas, Unrecom, Sockrat, JSocket и jRat, пострадало в общей сложности 443 тыс. организаций и частных лиц по всему миру. Троян до сих пор активен и распространяется в формате «вредоносное ПО как услуга», сообщают эксперты «Лаборатории Касперского», пишет InternetUA.

Как показало расследование ряда инцидентов с участием Adwind, вредоносная программа используется преимущественно в целях кибершпионажа. Готовый инструмент для слежки доступен любому желающему – достаточно просто заплатить за пользование вредоносным ПО. В отличие от остальных вредоносов, Adwind распространяется открыто в рамках единой платформы. В данном случае «клиент» платит за троян как за сервис. По данным «Лаборатории Касперского», по состоянию на конец 2015 г. количество пользователей данной «сервисной» системы насчитывало порядка 1,8 тыс.

Adwind написан целиком на Java, поэтому может работать практически на всех распространенных платформах, в частности Windows, OS X, Linux и Android. Функционал трояна включает возможность собирать и извлекать данные из системы, удаленно контролировать инфицированное устройство,

запоминать нажатия клавиш, делать снимки экрана, собирать общие данные о системе, передавать файлы, записывать аудио, похищать ключи от криптовалютных кошельков, красть VPN-сертификаты и пр.

Проанализировав порядка 200 целевых фишинговых атак, эксперты составили общую картину интересов злоумышленников. Большинство потенциальных жертв вредоноса работают в следующих сферах: производство, финансы, строительство и проектирование, разработка ПО, образование, производство продуктов питания, энергетика и пр. Почти половина (49 %) пострадавших от Adwind находятся в 10 странах: ОАЭ, Германии, Италии, России, Индии, США, Вьетнаме, Гонконге, Турции и на Тайване.

***

8.02.2016

«Одесский форум» активно DDoS'ят

«Одесский форум» активно DDoS'ят. Об этом сообщил администратор «Одесского форума» Д. Козин. Это уже не первая подобная атака на сайт за последний месяц, пишет Таймер.

«Кто-то очень сильно не жалеет денег. Пошли третьи сутки DDoS-атак на сервер http://forumodua.com», – отмечает он.

Причину такого нападения на сайт Д. Козин видит в проукраинской позиции «Одесского форума». «Всё из-за того же, из-за чего и Крым и Донбасс», – подчеркнул он.

***

9.02.2016

Мерія Чернівців просить СБУ розслідувати втручання у роботу системи електронних петицій

Мерія Чернівців просить СБУ, прокуратуру і поліцію розслідувати факт втручання в роботу системи електронних петицій із фальсифікацією підписів, пише Західна інформаційна корпорація.

Про це IA ZIK повідомили в міськраді.

Зокрема, ідеться про петицію про звільнення начальника міського управління охорони здоров'я І. Незборецького, яка за два дні набрала необхідні для розгляду 252 голоси.

Як розповіли чиновники, петицію було зареєстровано 20 січня, але вона зібрала лише кілька підписів. Аж раптом за 4–5 лютого з'явилися решта підписів.

Петицію, згідно із затвердженим положенням, було передано на розгляд мера. Однак відділ звернень почав отримувати листи від чернівчан із заявами про те, що їхні прізвища були використані під петицією без їхнього відома. Зокрема, було використано прізвища людей, які підписали іншу петицію на сайті. «Ми проаналізували підписи і дійшли висновку, що дійсних підписів – не

більше 10, а решта сфальшовані, – розповів начальник відділу комп'ютерно-технічного забезпечення міськради В. Маніліч. – Наприклад, приходили по десятку підписів з електронних адрес, які відрізнялися одна від одної лише буквою чи цифрою. Також дивним є те, що петицію підписали – судячи з IP – мешканці Білорусі та Бразилії».

Отож більшість підписів було скасовано, петиція залишається на сайті, збір підписів під нею триває.

Тим часом міський голова О. Каспрук звернувся до поліції, СБУ та прокуратури з листом про проведення розслідування факту зовнішнього втручання.

Надалі міська рада планує ускладнити верифікацію при голосуванні за петиції – для цього доведеться вказувати номер однієї зі своїх банківських карток чи картки чернівчанина.

***

10.02.2016

Эксперты вышли на след «богов кибершпионажа»

Компания «Лаборатория Касперского» вышла на след кибергруппировки, которая как минимум с 2005 г. крадет конфиденциальные данные у компаний по всему миру. Затем злоумышленники под угрозой перепродажи информации требуют заключить с ними контракт на предоставление консалтинговых услуг по IT-безопасности. Группировка получила название Poseidon, пишет InternetUA.

Жертвами атак становятся финансовые, телекоммуникационные, промышленные и энергетические компании, государственные учреждения, СМИ, PR-агентства и даже кейтеринговые службы, клиентами которых являются топ-менеджеры корпораций, говорится на сайте «Лаборатории Касперского».

В качестве основного языка группировка использует бразильский вариант португальского. Уже пострадали как минимум 35 организаций в России, Казахстане, США, Франции, ОАЭ и Индии, затронута и Бразилия. Особый интерес злоумышленники проявляют к внутрикорпоративным сетям на основе доменов.

Для атак используется вредоносное ПО, подписанное поддельными цифровыми сертификатами. Чаще оно проникает в систему с помощью фишинговых писем с RTF- и DOC-вложениями, которые приходят обычно в виде уведомлений от HR-служб. Попав в систему, это ПО собирает большое количество конфиденциальных данных, в том числе финансовых. Атакующие используют их для шантажа, принуждая пострадавшие компании к сотрудничеству, или же перепродают их третьим лицам.

«Мы обнаружили ряд командных серверов Poseidon в инфраструктуре интернет-провайдеров, обслуживающих морские суда, – рассказал Д. Бестужев, руководитель латиноамериканского исследовательского центра "Лаборатории

Касперского". – Для сокрытия следов своей деятельности злоумышленники использовали целый ряд хитроумных инструментов, включая обнаруженные нами зловреды с очень коротким жизненным циклом».

***

11.02.2016

Хакеры «угнали» аккаунт «бога» в Twitter

Злоумышленники воспользовались уязвимостью в Twitter, «угнав» целый ряд считающихся ценными учетных записей. Среди них оказался и аккаунт @God, зарегистрированный в 2007 г. Как сообщает Business Insider, уязвимость проявлялась в алгоритме восстановления пароля: при попытке восстановить его выводился полный электронный адрес, а не частично скрытый звездочками, как обычно, пишет InternetUA.

При некоторых обстоятельствах, когда срок регистрации адреса истек, злоумышленники могут перерегистрировать его, сбросить пароль и получить контроль над учетной записью. Не исключен и вариант с так называемой социальной инженерией, когда преступники выясняют всю необходимую им информацию о жертве обходными путями.

Отмечается, что пользователь @God обычно публикует шутки и юмористические картинки, однако сейчас изменил стиль. Помимо «Бога», оказались украдены и другие аккаунты, в частности @Emoji, @miracles, @Vagina, @nudes, @3o и ряд других. К настоящему времени уязвимость исправлена, однако администрация Twitter пока не прокомментировала инцидент.

***

10.02.2016

Приложения для Mac оказались под угрозой атаки злоумышленников

Компьютеры на OS X уязвимы, и это не раз подтверждалось. Новая уязвимость, найденная исследователем в области безопасности под именем Radek, может позволить злоумышленникам получить доступ к огромному количеству приложений, установленных на нашем Mac, и с их помощью атаковать другие компьютеры, находящиеся в одной сети. Атаке подвержены приложения как для OS X Yosemite, так и для OS X El Capitan, пишет InternetUA.

Уязвимость кроется в Sparkle. Sparkle – это инструмент, который активно используется разработчиками сторонних приложений для обновления продукта на свежую версию. Это касается только тех приложений, которые устанавливаются и обновляются без помощи Mac App Store. Механизм обновления приложений в OS X не использует Sparkle Update для приложений из магазина Apple.

Уязвимость существует благодаря тому, что среда Sparkle Update подключается с помощью HTTP вместо защищенного протокола HTTPS. Разумеется, в первую очередь информацию об уязвимости получили разработчики. Sparkle уже обновили свою среду и закрыли уязвимость. Многие разработчики уже работают над обновлением, а некоторые, например создатели популярного проигрывателя VLC, уже выпустили обновленное приложение, использующее новую среду Sparkle Update.

***

11.02.2016

Хакеры обнаружили новый способ похищения средств с банкоматов

Исследователи «Лаборатории Касперского» А. Гостев и В. Камлюк обнаружили две преступные группировки, использующие вредоносное ПО для изъятия денежных средств из банкоматов, компрометирования банковских сетей и отмены финансовых транзакций. Злоумышленникам удалось взломать более 30 российских банков. В атаках использовалось вредоносное ПО Metel (также известно как Corkow), пишет InternetUA.

«Вредоносное ПО, используемое группировкой Metel, инфицировало корпоративную сеть банка через электронную почту и получило доступ к компьютерам в IT-системах финучреждения. Получив доступ к процессинговой системе, злоумышленники смогли отменять транзакции через банкоматы. Преступники могли получать в банкоматах наличные и сразу отменять платеж. Баланс на дебетовых картах не менялся», – сообщают исследователи.

Вначале хакеры осуществляли целевые фишинг-атаки с применением наборов эксплоитов Niteris или Cotton Castle. Как только жертва устанавливала на компьютер вредоносное ПО, злоумышленники сканировали корпоративные сети банка в поисках процессинговой системы. Получив доступ к системе обработки платежей, преступники начинали снимать деньги с банковских карт и моментально отменять транзакции. В ходе одной из операций злоумышленники смогли похитить несколько миллионов рублей.

К аналогичной схеме прибегла группировка GCMAN. Хакеры также осуществляли фишинг-атаки, проникали в корпоративные системы банков и похищали денежные средства. В отличие от Metel, злоумышленники внедрили в сервер банка cron-сценарий, ежеминутно осуществлявший денежные переводы размером в 200 дол.

***

12.02.2016

Количество входящих в ботнет Wifatch маршрутизаторов достигло 70 тысяч

В октябре прошлого года SecurityLab.ru сообщал об обнаружении нового ботнета, исправляющего уязвимости на инфицированных устройствах

(преимущественно домашних маршрутизаторах). Как выяснилось, за несколько месяцев размер сети возрос до 70 тыс. сетевых устройств. Группировка, ответственная за создание и поддержку работоспособности ботнета, получила название White Team, пишет InternetUA.

Ботнет представлен в виде p2p-сети. Хакеры получают доступ к уязвимым устройствам и устраняют наиболее распространенные проблемы, включая слабые пароли, отключенные межсетевые экраны и бэкдоры.

Для инфицирования уязвимых маршрутизаторов используется вредоносное ПО Wifatch. Исходный код проекта был размещен на портале GitLab. Wifatch регулярно обновляется для добавления поддержки большего количества сетевого оборудования.

Впервые Wifatch попал в поле зрения исследователей в 2014 г. Тогда исследователь безопасности с псевдонимом Loot Myself обнаружил и проанализировал работу вредоноса. После обнаружения специалистами Symantec в 2015 г. Wifatch пришел к известности. Легальность действий хакеров до сих пор обсуждается ИБ-экспертами – по мнению некоторых специалистов, насколько бы благородными не были цели создателей Wifatch, существование ботнета незаконно.

***

11.02.2016

В библиотеке Libgraphite обнаружено 4 опасные уязвимости

Специалисты подразделения компании Cisco по ИБ-исследованиям Talos обнаружили несколько уязвимостей в библиотеке libgraphite, ответственной за обработку и отображение шрифтов во многих приложениях в Linux и Windows. Ошибки затрагивают работу клиентских и серверных компьютеров и позволяют удаленному злоумышленнику выполнить произвольный код, пишет InternetUA.

Уязвимости могут быть проэксплуатированы в любом приложении, использующем библиотеку libgraphite версии 2-1.2.4 для загрузки шрифтов TrueType (формат .ttf). Для успешной эксплуатации программа должна обработать страницу со специально сформированным вредоносным шрифтом.

В библиотеке существуют четыре уязвимости: CVE-2016-1521, CVE-2016-1522, CVE-2016-1523 и CVE-2016-1526. Ошибки позволяют выполнить произвольный код на целевой системе, осуществить DoS-атаку и раскрыть данные.

Наиболее опасная уязвимость (CVE-2016-1521) позволяет скомпрометировать систему. Ошибка существует из-за выхода за пределы памяти, вызванного отсутствием проверки значения goto в коде библиотеки.

Уязвимость CVE-2016-1522 также позволяет выполнить на системе произвольный код. Для эксплуатации ошибки необходимо обработать страницу со специально сформированным вредоносным шрифтом. Операция приведет к переполнению буфера.

Менее опасные уязвимости (CVE-2016-1523 и CVE-2016-1526) позволяют осуществить DoS-атаку и раскрыть данные.

***

11.02.2016

Мошенники используют WhatsApp для хищения личных данных пользователей

Пользователи популярного сервиса WhatsApp оказались под прицелом новой мошеннической кампании, направленной на инфицирование устройств жертв и хищение персональных данных, пишет InternetUA со ссылкой на издание This is Money.

Действуют мошенники следующим образом: на гаджет пользователя приходит сообщение с фразой «Look» («Смотри») якобы от доверенного контакта с легитимной по виду ссылкой. Данная ссылка ведет на подложный веб-сайт, завлекающий пользователей скидочными купонами на продукцию известных торговых марок.

Для получения ваучера жертве необходимо предоставить свои имя, адрес электронной почты, номер мобильного телефона и физический адрес. В результате устройство оказывается инфицированным вредоносным ПО, а злоумышленники получают доступ к персональным данным его владельца.

По словам ведущего аналитика «Лаборатории Касперского» Д. Эмма, злоумышленники убеждают жертву перенаправить сообщение с вредоносной ссылкой 10 контактам, иначе пользователь не сможет получить вожделенный купон. Как отметил Д. Эмм, мошенническая кампания продолжается уже некоторое время и охватывает несколько стран, о чем свидетельствует использование в сообщениях различных языков.

***

12.02.2016

Новый троянец обманывает клиентов банков

Одной из наиболее опасных угроз информационной безопасности принято считать банковских троянцев, представляющих собой довольно сложные вредоносные программы с широкими функциональными возможностями, пишет HiTech.Expert.

Однако в своих попытках обмануть клиентов различных кредитных организаций злоумышленники не брезгуют и более тривиальными решениями – к таковым относится троянская программа Trojan.Proxy2.102, исследованная специалистами компании «Доктор Веб».

Trojan.Proxy2.102 предназначен для кражи денег с банковских счетов и использует для этого достаточно простой метод. Запустившись на атакуемом устройстве, троянец устанавливает в системе корневой цифровой сертификат и

изменяет настройки соединения с Интернетом, прописывая в них адрес принадлежащего злоумышленникам прокси-сервера.

С этого момента любые обращения браузера к веб-страницам системы интернет-банкинга нескольких ведущих российских кредитных организаций осуществляются через прокси-сервер киберпреступников. С его помощью в страницы систем «банк-клиент» при открытии на инфицированном компьютере встраивается постороннее содержимое, позволяющее злоумышленникам похищать деньги с банковских счетов жертвы. В настоящее время установлено, что Trojan.Proxy2.102 способен подменять содержимое следующих банковских интернет-ресурсов: online.sberbank.ru, online.vtb24.ru и online.rsb.ru. Поскольку троянец предварительно устанавливает на зараженном компьютере поддельный цифровой сертификат, с использованием которого подписывает соответствующие веб-страницы, пользователь вряд ли сможет вовремя заметить подмену.

После успешной установки троянец отправляет сообщение об этом событии на управляющий сервер. Поскольку он никак не регистрирует себя в автозагрузке, после выполнения своих вредоносных действий троянец переходит в бесконечный спящий режим.

Антивирус Dr.Web успешно обнаруживает и удаляет вредоносную программу Trojan.Proxy2.102, поэтому она не представляет опасности для наших пользователей.

***

12.02.2016

Android-троян для похищения SMS-сообщений маскируется под функцию безопасности AliPay

ИБ-эксперты компании Zscaler предупредили пользователей Android-устройств о новой угрозе. Вредоносное ПО маскируется под функцию безопасности популярного приложения для осуществления online-платежей AliPay, но на самом деле представляет собой троян для перехвата смс-сообщений, пишет InternetUA.

Пользователи загружают вредонос в полной уверенности, будто скачивают приложение, усиливающее защиту AliPay. Через три секунды после установки трояна его иконка удаляется, однако сама программа никуда не исчезает.

Незаметно для жертвы вредонос регистрирует сервисы Android, способные работать в фоновом режиме и выполнять задачи с длительным временем реализации. Если точнее, троян использует MyService, DealService и TestService, а также несколько приемников широковещательных сообщений (System Boot Receiver, Massage Receiver и Screen-On Receiver). Главная задача вредоноса – похищение и передача на подконтрольный злоумышленникам C&C-сервер смс-сообщений жертвы.

Поскольку ПО не запрашивает права администратора, удалить его достаточно просто. Троян можно деинсталлировать с помощью соответствующих настроек Android.

AliPay (так называемый «восточный PayPal») – китайская online-платформа для осуществления платежей без комиссионных, поддерживающая свыше 65 финансовых институтов, в том числе Visa и MasterCard, и 14 валют. Используется в порядка 300 торговых организациях.

***

12.02.2016

Ежедневные российские кибератаки

Главнокомандующий Вооруженными силами Швеции М. Бюден заявил в интервью газете Sydsvenska Dagbladet, что Россия ежедневно производит кибератаки и информационные операции против Швеции, пишет 24news.

«Это комплексная гибридная война с целью посеять неуверенность. Мы отслеживаем российские действия, для этого есть основания», – сказал главнокомандующий. Он также рассказал, что число кибератак против Швеции и шведских интересов резко возросло в последнее время. Нападающие пытаются внедрять коды-вредители в компьютеры вооруженных сил и промышленности, выкрадывая с их помощью информацию из этих систем или с помощью рассылки фальшивых сообщений от чужого имени.

Тем не менее, М. Бюден не согласен со словами генерала армии А. Брэнрстрема о том, что «Швеция может вступить в войну через несколько лет». «Я бы избегал таких выражений, но общая угроза ныне совсем другого порядка чем прежде, – сказал главнокомандующий. – Прямой и непосредственной военной угрозы нападения на нашу страну нет. То, что мы видим, это комплексные гибридные военные действия, в которых пытаются использовать наши слабые места, где на нас нападают не только военными средствами, но используя и другие инструменты».

М. Бюден не верит, что Россия планирует вторжение в Швецию. Но считает, что российское агрессивное поведение может привести к непредсказуемому кризису.

***

14.02.2016

Злоумышленники выдают троян Remtasu за инструмент для взлома Facebook

ИБ-эксперты компании ESET сообщили о трояне, замаскированном под новый инструмент для компрометации учетных записей в Facebook. Решив с помощью данного ПО взломать чужой аккаунт, пользователь сам становится жертвой хакеров. Исследователи предупреждали о Remtasu еще несколько лет назад, однако количество его жертв продолжает расти, пишет InternetUA.

Варианты Win32/Remtasu.Y чаще всего обнаруживаются в странах Южной Америки, в большинстве случаев в Колумбии, а также в Таиланде и Турции. В рамках недавно зафиксированной кампании вредонос выдается за инструмент для взлома чужих учетных записей в Facebook. В отличие от других представителей семейства, данный образец Remtasu распространяется не посредством фишинговых писем, а через загрузки с сайта. Пользователь сам добровольно загружает и выполняет вредоносный файл.

Троян способен фиксировать нажатия на клавиатуре и похищать информацию из буфера обмена. Все полученные с инфицированной системы данные сохраняются локально в файле и затем отправляются на FTP-сервер. В отдельной папке внутри папки system32 создается копия вредоноса, благодаря чему он остается на системе даже после перезагрузки. Папка InstallDir скрывается в системных файлах, поэтому пользователю сложно получить к ней доступ.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Касаткіна** Тетяна

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

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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

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