СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(23.05–5.06)

№ 8 2016

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(23.05–5.06)
№ 8 2016

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

3.06.2016

Новий інструмент Facebook навчиться розуміти все, що пишуть користувачі

Компанія Facebook розробила штучний інтелект, який розпізнаватиме, про що пишуть користувачі соцмережі з «майже людською точністю», пише MediaSapiens.

Про це компанія повідомила у своєму блозі.

Ціль Deep Text – аналізувати текстові повідомлення людей у соцмережі та рекомендувати їм відповідні пости та сервіси. Також інструмент допомагатиме у відсіюванні спаму та небажаних повідомлень.

Deep Text випробовується у Facebook Messenger і генерує відповіді на певні пошукові запити. Наприклад, якщо хтось переписується в Messenger про підготовку до подорожі, система може запропонувати замовити таксі, виходячи з контексту переписки. За цим же принципом, якщо користувач пише про намір щось продати, боти Deep Text опрацюють цей текст і запропонують використати один з інструментів для продажів у соцмережі. При цьому вони врахують специфіку товару та цільову аудиторію, якій він може бути цікавим.

Наразі Deep Text може аналізувати кілька тисяч повідомлень у секунду і працювати з більш ніж 20 мовами.

У майбутньому компанія планує розвивати Deep Text, щоб він міг краще розпізнавати людей, місця і події в постах. Наприклад, розуміти зв'язки між словами, будувати концептуальну карту, як використовуються різні слова. У Facebook вважають, що так рекомендації можуть стати ще більш персоналізованими.

Оглядач технологічних новинок М. Мерфі зазначив у своєму пості для Quartz, що таке використання Deep Text несе певні загрози. Надто персоналізовані рекомендації можуть замкнути користувачів у межах певної локації, інтересів, вірувань. «Google також робить це, певною мірою, але принаймні він перш за все виконує пошук по всьому Інтернету. А не тільки в межах якогось закритого простору», – зазначив М. Мерфі.

***

25.05.2016

Twitter рассказал о ближайших новшествах

Социальная сеть Twitter перестанет учитывать имена пользователей, опросы, изображения, видео и другие медиафайлы в лимите 140 символов, сообщает vc.ru, пишет Телекритика.

Вместе с тем компания не стала отказываться от учета ссылок, о чем ранее говорили источники агентства Bloomberg.

Также, согласно сообщению в официальном блоге Twitter, у пользователей появится возможность ретвитить и цитировать собственные твиты. В компании отмечают, что это позволит выражать свое отношение или чувства к старым записям.

Кроме того, соцсеть отменит правило, согласно которому твит, начинавшийся с имени пользователя, считался перепиской и был виден только подписчикам обоих собеседников. Чтобы обойти это ограничение и показать ответ всем подписчикам, раньше приходилось начинать твиты с точки (в формате «.@username»). Теперь же, чтобы сделать свой ответ видимым для всех, нужно будет лишь ретвитнуть свой твит.

Как уточнили в Twitter, все эти изменения вступят в силу в ближайшие месяцы в веб-версии, мобильных приложениях сервиса, а также в Tweetdeck.

***

26.05.2016

LiveJournal перетворився на медіа

Платформа блогів LiveJournal провела масштабний перезапуск. Тепер головна сторінка LiveJournal виглядає як медіа, створене на основі авторських блогів, а при її формуванні редактори сайту орієнтуються на правила та закони, які використовуються в ЗМІ.

Про це повідомив головний редактор LiveJournal В. Гулін, пише Media Sapiens.

«Відійти від тизерних заголовків, провокацій та погоні за ілюзорними показниками популярності. Писати цікаві, повноцінні тексти, а не перебиватися недогризками у сподіваннях на довгі гілки коментарів. Працювати з аудиторією всієї платформи, стати частиною LiveJournal, вийти за межі “ЖЖ” [LiveJournal – “Живой Журнал”], свого затишного, але все ж маленького світу», – написав В. Гулін.

На головну сторінку LiveJournal потраплятимуть як тексти популярних блогерів, так і матеріали, написані невідомими авторами. За словами В. Гуліна, LiveJournal має стати цікавим і багатостороннім ресурсом, у якому є «і новини, і вічні теми, і огляди, тести».

LiveJournal, або «Живой Журнал», – найбільша блог-платформа у Росії. Розвитком її кириличного сегмента займається група компаній Rambler&Co. Платформа була запущена в 1999 р. За даними TNS Web Index, щомісячна аудиторія сервісу в Росії становить16 млн людей.

***

25.05.2016

Twitter тестирует ночной режим для мобильной версии сервиса

Twitter добавит ночной режим интерфейса в официальном приложении для мобильных платформ. Как стало известно, компания проводит тестирование альфа-версии (5.112.0-alpha.423) Android-приложения социальной сети с подобным функционалом, пишет InternetUA.

Одним из нововведений мобильного Twitter станет появление специального ночного режима, который будет включаться автоматически в ночное время суток. При этом пользовательский интерфейс будет меняться.

Стоит отметить, белый текст на темном фоне для многих пользователей является не самым комфортным сочетанием. Пользователям остается надеяться, что в финальной версии появится отдельный переключатель дневного и ночного режимов работы, которого нет в текущей альфа-версии.

По последним данным, пользовательская база Twitter превышает 310 млн человек.

***

25.05.2016

Facebook купила компанию по виртуальному звуку Two Big Ears

Социальная сеть Facebook приобрела компанию Two Big Ears, занимающуюся звуком виртуальной реальности, и будет использовать её платформу для продвижения высококачественного VR-звука. Facebook выпустила программное обеспечение купленной компании Spatial Workstation под обновлённым названием Facebook 360 Spatial Workstation. Согласно официальному сайту, ПО предназначено для распространения виртуального звука на различных устройствах и платформах. Улучшать его будут работники Two Big Ears и Oculus, владельцем которой также является Facebook, пишет InternetUA.

Релиз Spatial Workstation состоялся прошлой осенью: изначально это была платформа для создания аудио, которое могло бы звучать реалистично в трёхмерном пространстве. Так называемое пространственное аудио является важным элементом при работе с виртуальной реальностью – Oculus также работала над ним некоторое время. Однако в отличие от ряда нескольких других VR-компаний, эта покупка была совершена именно Facebook, а не Oculus – поэтому и в названии проекта присутствует слово Facebook. Нацелен продукт как на виртуальную реальность в целом, так и на 360-градусное видео в частности.

Следующие 12 месяцев Two Big Ears будет обеспечивать техподдержку тем, кто оплатил лицензию на старую версию её продукта. Сама программа будет продолжать работать – в ней почти ничего не изменится. Однако некоторые опции новым пользователям доступны не будут: это, в частности, касается возможности использовать плагины для игрового движка Unity и звуковых движков Wwise и FMOD. Несмотря на это, компания продолжит быть «агностиком» по отношению к устройствам и платформам – это означает, что она не будет концентрироваться исключительно на Rift или Gear VR.

***

24.05.2016
Facebook изменит алгоритм показа новостей

Изменения вызваны обвинениями сети в политической предвзятости, отмечает slon.ru. В блоге компании отмечается, что проведенное внутреннее расследование не подтвердило слухи о том, что в лентах чаще показываются новости с «либеральной» точкой зрения, нежели с «консервативной». Тем не менее, в Facebook решили пойти на ряд мер, чтобы исключить даже теоретическую возможность этого.

Компания заявила, что принятые меры будут включать в себя переобучение сотрудников, работающих с алгоритмом, и разработки новых инструкций для них. Помимо этого, будет отключена функция сравнения популярных постов с материалами крупнейших изданий США, пишет Marketing Media Review.

***

26.05.2016
Viber – самый популярный мессенджер в Украине

Аналитическая компания SimilarWeb на основе статистических данных, собранных с Android-устройств по всему миру, определила самые популярные мессенджеры, пишет IGate.

Вполне ожидаемо, первое место, с большим отрывом от конкурентов, занимает WhatsApp, являющийся наиболее популярным в 109 странах из 187 учувствовавших в исследовании. WhatsApp оказался номером один в Индии, Бразилии, Мексике, России и других странах.

На втором месте расположился Facebook Messenger, лидирующий в 49 странах, среди которых отметим США, Канаду, Австралию.

С учетом того, что оба эти сервиса принадлежат Facebook, можно сказать, что компания захватила 80 % мирового рынка мессенджеров.

Из остальных участников только Viber является наиболее популярным в 10 или более странах. Особенно любят мессенджер в Восточной Европе. В Украине, к примеру, этот сервис не только самый распространенный, но и установлен на 65 % всех Android-устройств. Также Viber лидирует в Молдове и Беларуси и других странах.

***

28.05.2016
Foursquare анонсировала рекомендательного бота

Социальная сеть геолокационных данных Foursquare анонсировала Marsbot – приложение для iOS, в реальном времени предлагающее места, где можно пообедать и выпить. «Наша цель – создать продукт, который говорит

вам, где поесть и выпить, ещё до того, как вы подумаете об этом спросить», – говорят разработчики. «Он может давать контекстуально подходящие, упреждающие рекомендации по отличной еде и местам ночной жизни через самый простой коммуникационный канал: текст», пишет InternetUA.

На скриншотах приложения можно увидеть интерфейс чата. Тем не менее, Foursquare уверяет, что Marsbot – это не чат-бот. «С помощью чат-бота вы задаёте конкретные вопросы и даёте конкретные подсказки касательно того, что вам нужно», – говорит компания. «Цель Marsbot – дать вам ответы ещё до того, как вы спросите, основываясь на том, где вы и куда вы обычно ходите». Нечто похожее умеет и само приложение Foursquare – оно может отправлять уведомления, когда вы оказываетесь, например, в незнакомом городе. Поэтому не совсем ясно, зачем разработчикам выпускать отдельное приложение.

Однако у Foursquare есть причины экспериментировать с ботами. Сегодня немало стартапов пробует чат-интерфейсы, при этом некоторые из них полностью концентрируются на рекомендациях касательно ресторанов и ночных клубов. Такие компании, как Ozlo, Luka и Mezi, собираются потеснить Foursquare. Также можно предположить, что похожая функциональность будет и в мессенджере Allo от Google, который должен стать доступен летом.

Несмотря на то, что Foursquare позиционирует Marsbot скорее как эксперимент, нежели как полноценный новый продукт, её старания могут принести плоды – особенно если учесть, что сервисы по рекомендациям и чат-боты становятся всё популярнее.

***

28.05.2016

Uber разрешил использование баз Foursquare в работе своего сервиса

Сервис пассажирских перевозок Uber заключил соглашение о стратегическом партнерстве с компанией Foursquare. Она владеет одноименным проектом, в рамках которого пользователи пополняют базу данных о различных заведениях, расположенных в населенных пунктах разных стран. Эти точки на карте отныне можно использовать в Uber в качестве пунктов отправления и назначения, пишет InternetUA.

О факте заключения соглашения сообщили обе стороны в своих официальных блогах, передает портал CNET. В Uber уже действует подобная система, в основе которой лежит сервис Google Maps, но в ее работе есть ряд ограничений, в том числе и определенные проблемы с выбором некоторых заведений на карте. Сотрудничество с Foursquare позволит избежать всего этого.

Финансовый и временной аспекты сделки между компаниями держатся в секрете, но она уже вступила в силу. Как отметили представители Foursquare, соглашение носит глобальный и одновременно долгосрочный характер, что дает основания предположить, что интеграция базы Foursquare в сервис Uber затронет не только США.

Эксперты отметили, что стратегическое партнерство в данном случае выгодно обеим сторонам: Uber получит большее количество клиентов, которые плохо ориентируются на местности и не могут указать точный адрес (к примеру, туристы), но могут отметить расположенные поблизости заведения. Foursquare же в свою очередь может рассчитывать на усовершенствование собственной базы, поскольку каждый клиент Uber может добавить новое заведение или пометить на удаление уже закрывшееся или сменившее адрес.

Для Foursquare Uber не является первым партнером такого рода: в список клиентов компании входят Microsoft, Samsung, Apple, Yahoo, Twitter и ряд других крупных предприятий. Uber тоже является одним из крупнейших игроков в своем сегменте рынка, еженедельно расширяя географию своего присутствия. В частности, проект уже стартовал в нескольких крупных городах России, и до конца текущего года их количество, несмотря на санкции, должно увеличиться вдвое.

***

31.05.2016

В США получают информации о стране и мире из Reddit, Facebook и Twitter

Опрос общественного мнения впервые показал, что большинство американцев узнают последние новости из социальных сетей. Согласно исследованию Pew Research Center, 62 % опрошенных используют Reddit, Facebook и Twitter для получения свежей информации о стране и мире. В аналогичном опросе, проведенном четыре года назад, этот показатель составлял 49 %, пишет МедиаБизнес.

Как сообщает sostav.ru, 18 % случаев соцсети часто используются в качестве новостного источника, в 26 % – время от времени, в 18 % – очень редко. 38 % респондентов никогда не узнают новости в social media.

Самыми «преданными» читателями являются пользователи Reddit – 70 % его аудитории ищут новости на этом же сайте. У Facebook доля таких пользователей составляет 66 %, у Twitter – 59 %. Меньшим интересом к новостям отличается аудитория Tumblr (31 %), Instagram (23 %) и YouTube (21 %).

Однако в целом лидером является Facebook. Соцсеть охватывает 67 % взрослого населения США, поэтому она является источником новостей для 44 % американцев. У YouTube это соотношение составляет 48 % к 10 %, Twitter – 16 % к 9 %, Instagram – 19 % к 4 %.

Для 64 % пользователей, узнающих о новостях из соцсетей, достаточно одного-единственного сайта. 26 % предпочитают две площадки, 10 % ради новостей посещают минимум три соцсети. Аудитория Instagram, Facebook и YouTube предпочитает потреблять новости в фоновом режиме, одновременно с другими занятиями. Более целенаправленными являются пользователи Reddit, Twitter и LinkedIn.

Исследователи также обнаружили, что каждая из пяти социальных сетей вызывает интерес определенной демографической группы. Так, среди пользователей LinkedIn много (65 %) выпускников колледжей, среди пользователей сети Facebook большинство составляют белые неиспанские (65 %) женщины (57 %), а Instagram пользуется популярностью у женщин (65 %) и сторонников Демократической партии (40 %).

***

31.05.2016
Twitter ввів підтримку 3D Touch

У мобільній версії соціальної мережі Twitter з'явилася підтримка функції 3D Touch. Скористатися нею зможуть власники таких ґаджетів, як iPhone 6S і iPhone 6S Plus, пише Bublbe.com.

Функція 3D Touch дає можливість користувачам застосовувати додаток, не запускаючи при цьому самі програми. Раніше Twitter також підтримував подібні технології, однак їх можна було використовувати тільки на базовому рівні, тобто на домашньому екрані. Отже, користувач соцмережі міг залишати твіт або відповідати на повідомлення за допомогою більш сильного натискання на дисплей.

Тепер же Twitter дає можливість своїм клієнтам додати розширену версію 3D Touch. За допомогою оновленої програми вони можуть переглядати зображення, сторінки користувачів у соціальній мережі й переходити за посиланнями.

На думку авторів проекту, подібне оновлення значно скоротить час очікування підключення до різних додатків і переходу на сторінки. Крім того, це дасть можливість користувачам швидше обмінюватися повідомленнями й робити пости в соціальній мережі.

***

2.06.2016
Instagram запретил все сторонние сервисы для просмотра ленты

Компания прекратила поддержку API, позволявшего разработчикам создавать сервисы для просмотра фотографий и видеороликов, пишет InternetUA.

Instagram запретил приложения с функциями, позволяющими подписываться на других пользователей, ставить «лайки» и оставлять под фото комментарии. Решение было принято в рамках «большой чистки» сервиса в ноябре прошлого года и вступило в силу с 1 июня 2016 г.

В Instagram пояснили, что пошли на такой шаг в связи с тем, что сторонние приложения маловостребованы у пользователей, а компании приходится тратить ресурсы на поддержку API. По данным компании,

пользовательская база даже самого популярного из них составляла лишь 0,5 % от общей аудитории сервиса – порядка 2 млн человек.

Есть предположение, что закрытие соответствующего API было вызвано желанием Instagram увеличить доход от рекламы – недавние изменения должны заставить пользователей просматривать больше фотографий, содержащих маркетинговые материалы.

Новым правилам пришлось подчиниться всем сторонним приложениям, в том числе Retro, Flow, Padgram и Pictacular для iPad, а также Webbygram, Webstagram, Instagreat и Itsdagram. Доступ к постам Instagram остался только у сервиса знакомств Tinder и рекламных программ.

Iconosquare, который позволял пользоваться Instagram через браузер, запустил платный сервис аналитики. Стоимость обслуживания составляет от 5 долл. в месяц, с его помощью можно использовать фотосервис с нескольких аккаунтов, а также просматривать настраиваемые ленты. Таким же образом перезапустился веб-клиент Websta. Создатели клиента для iPad Flow объявили о закрытии проекта.

С 1 июня Instagram разрешил подключаться к своим API только приложениям для редактирования фотографий, а также аналитическим и маркетинговым сервисам. Помимо этого, в компании отключили возможность подключать к своим проектам авторизацию через Instagram без согласования с разработчиками фотосервиса.

***

2.06.2016

Instagram будет платить пользователям за популярный контент

Социальная сеть Instagram планирует начать платить пользователям за новостной контент, контент о спорте, жизни знаменитостей и т. д. Об этом сообщает Bloomberg со ссылкой на вице-президента по глобальным маркетинговым решениям в материнской компании Instagram Facebook Inc К. Эверсон, пишет InternetUA.

Администрация социальной сети считает необходимым стимулировать пользователей к созданию интересного авторского контента.

«Содержание невероятно важно в Facebook и Instagram. Мы хотим стать глобальной платформой обмена информацией и пытаемся найти различные способы, чтобы помочь производителям контента заработать. Мы изучаем модели распределения доходов», – сказала К. Эверсон в интервью Bloomberg TV.

По словам К. Эверсон, многие рекламодатели используют и Facebook, и Instagram, создавая кроссовер между двумя платформами. В любом случае, соцсеть с 400 млн активных пользователей проивлекает как крупные корпорации, так и маленькие компании в качестве площадки для продвижения.

***

3.06.2016

Руководители Twitter и Yahoo обсудили возможность слияния компаний

Поглощение Yahoo социальной сетью Twitter обсуждалось на встрече представителей компаний несколько недель назад. Переговоры длились несколько часов, однако, основатель Twitter Д. Дорси так и не появился на встрече, пишет InternetUA.

«Идея не такая безумная как может показаться», считают источники New York Post. Twitter является источником новостей, а у Yahoo обширная аудитория.

На встрече обсуждалось финансовое состояние Yahoo, а также возможности развития сервисов после завершения сделки по слиянию. Один из источников издания отметил, что отсутствие Д. Дорси на встрече говорит о несерьезном интересе со стороны Twitter.

Пока среди претендентов на активы Yahoo лидирует Verizon.

***

4.06.2016

«ВКонтакте» тестирует приложение для прямых видеотрансляций VK Live

Об этом на открытии «V НеФорума» в Казани заявил глава пресс-службы соцсети Е. Красников, пишет InternetUA.

Пользователям будут доступны такие возможности, как групповой стриминг, мгновенный обмен реакциями по поводу видео, отправление друзьям приглашений к просмотру, карта прямых включений. Таким образом VK Live призван составить конкуренцию другому сервису прямых видео-трансляций – Periscope.

По словам Е. Красникова, приложение VK Live уже использовалось для ведения некоторых трансляций, которые были показаны в соцсети. «ВКонтакте» тестирует приложение с конца апреля.

«У нас было уже много трансляций, некоторые из них тянули, чтобы попасть в Книгу рекордов Гиннеса, например, трансляция с Егором Кридом. Она прошла в вагоне Московского метрополитена. Егор проехал один круг по кольцевой», – сказал Е. Красников. Он пошутил, что певцу «накрутили» почти 400 тыс. просмотров.

В настоящее время приложение VK Live недоступно рядовым пользователям, однако видеоблогеры могут оставить заявку на получение его тестовой версии, написав разработчикам письмо по адресу live@vk.com.

Е. Красников отметил, что уже год во «ВКонтакте» существует возможность монетизация видео. «Вы просто подаёте заявку в группу поддержки, мы признаём вас видеоблогером, берём ваши видеозаписи,

добавляем туда видеорекламу и с удовольствием делимся с вами доходом с этой рекламы», – объяснил он.

Как рассказал представитель «ВКонтакте», в дальнейшем в соцсети появится функция рекомендации видео. «Они основаны на интересах пользователей, которые сейчас смотрят видео. Оно анализируется, и будут предлагаться следующие записи, чтобы пользователи не уходили из соцсети», – пояснил Е. Красников.

***

5.06.2016

«ВКонтакте» запустит собственный мессенджер для iOS и Android

Социальная сеть «ВКонтакте» намерена до конца года выпустить собственный мессенджер для мобильных платформ. О планах компании на казанском «НеФоруме блогеров» рассказал пресс-секретарь соцсети Е. Красников, пишет InternetUA.

По имеющимся сведениям, мессенджер будет доступен в двух вариантах: в качестве мобильного приложения и как клиент для ПК. При этом он не получит функцию шифрования сообщений. «Компания заинтересована в сохранении интеграции между “ВКонтакте” и отдельным мессенджером, чтобы можно было быстро переключаться к профилю, новостям и другим сервисам», – говорил ранее операционный директор соцсети А. Рогозов.

Аудитория «ВКонтакте» составляет 90 млн пользователей, из которых около 80 % – это мобильная аудитория, причем каждый четвертый заходит в соцсеть только через мобильные устройства.

47 % всей активности пользователей «ВКонтакте» приходится на обмен сообщениями и просмотр ленты новостей. При этом с помощью социальной сети ежедневно отправляются 5 млрд сообщений. Раздел «видео» и «аудио» занимает только 10 % активности пользователей. В настоящее время социальная сеть активно занимается развитием видеоконтента.

По словам Е. Красникова, «ВКонтакте» намерена договариваться с правообладателями согласно модели, которая предполагает следующие условия. Если пользователь находит видео, которое еще не было «залито» в социальную сеть, то они могут предоставить «ВКонтакте» копию хорошего качества, и видео будет заменено, туда будет встроена реклама, и компания будет делиться доходами с пользователем.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

2.06.2016
В Twitter появился официальный аккаунт Украины

В Twitter появился аккаунт Украины, он верифицирован самой компанией как официальный. Он англоязычный, здесь пока всего один пост-обращение к другим аккаунтам стран – Польше и Канаде, которые первыми признали независимость нашей страны в 1991 г. Подписчиков у аккаунта тоже пока немного, но украинский сегмент социальной сети быстро это исправит, пишет AIN.UA.

Пока ни одно ведомство не объявило о том, что ведет этот аккаунт, но по данным редакции, им занимаются SMM-щики из Администрации Президента. Редакция также ожидает комментария от пресс-службы МИД Украины о том, насколько это официальный аккаунт. Правда, верифицированный Twitter МИД уже ретвитнул первый пост Украины.

***

24.05.2016
Политики побаиваются Facebook – Леонид Швец

Свеженазначенный Генеральный прокурор и ветеран украинской политики Ю. Луценко позвал блогеров, чтобы объясниться, информирует Экономические известия.

Раньше с ними уже встречались министры финансов, экономического развития, юстиции, внутренних дел, начальник Генштаба, глава «Нафтогаза», военный прокурор, глава президентской Администрации, руководитель НАБУ, начальник Национальной полиции, на одну из встреч зашёл и премьер, правда, это был ещё тот премьер, да и министры того правительства.

Этого достаточно, чтобы уверенно утверждать: в Украине работает необычный институт коммуникации власти и общества, такого больше нет нигде.

Конечно, американский президент, который встречается вообще со всеми, встречается и с блогерами. Даже поверхностное гугление выбрасывает новости о том, что в апреле прошлого года Б. Обама в Белом доме принимал топ-пятёрку «прогрессивных блогеров», а в октябре 2010 г. в Шарлотте, штат Северная Каролина, беседовал с местными женщинами-блогерами на семейные темы. Только «прогрессивные блогеры» – при ближайшем рассмотрении ребята-демократы, когорта сетевых бойцов за идеалы Демократической партии, так что это была эдакая внутрипартийная встреча. А женская группа в

Шарлотте – обыкновенная группа интересов, блогерство её участниц – так, дополнительное украшение.

Но вот чтобы представители высшего эшелона власти регулярно встречались с людьми, объединёнными одним признаком: наличием какого-то относительно немаленького числа подписчиков в Facebook и вниманием к общественно-политической тематике, такого в мире нигде больше нет, made in Ukraine в чистом виде.

Зачем это блогерам – понятно: любопытство. Что у них там, наверху, в мозгах и в душе, как она устроена, нынешняя власть, почему сделали это и не сделали того. В конце концов, просто посмотреть, как себя ведёт и говорит кто-то из тамошних, уже нелишнее наблюдение, пригодится для понимания и последующих комментариев. А вот зачем это представителям власти? Боятся? Уважают?

В первую очередь это, конечно, признание влиятельности. Блогер – из тех, кого называют популярными, – это такая ходячая ежедневная газета с тысячами, а то и десятками тысяч читателей. Когда-то на меня глубокое впечатление произвела цифра, которую назвала О. Забужко: суммарный тираж её произведений за всю творческую жизнь составил на момент нашего с ней разговора около 30 тыс. экземпляров. Это был, если не ошибаюсь, 2005 год. Надеюсь, сейчас значительно больше, но с активными блогерами ведущие деятели культуры по числу читателей тягаться не могут. Хотя вес слова, безусловно, несопоставим, но видит это слово разное количество людей. Немаловажно, что и публика в Facebook (а наши блогеры это Facebook-блогеры) значительно более гражданski активна, чем в среднем по стране. К этой аудитории политикам и чиновникам лучше не поворачиваться спиной. Вот они и норовят показаться лицом и при этом широко улыбаться.

Конечно, за этим кроется и колоссальная недоразвитость традиционных СМИ – полное отсутствие в стране, например, респектабельных ежедневных газет, стоящих на страже общественных интересов. И слабая структурированность общества, где ощущается острый дефицит гражданских организаций. Блогеры, по сути, совмещают в себе две функции – гражданский активизм и общественно-политическое информирование, как-то затыкая эту дыру в социальной ткани. Так что для представителей власти встречи с ними убивают двух зайцев: и гражданское общество уважить, и медиа.

Это полезная практика. Пока власти хотят, чтобы их правильно поняли, и идут на разговор, они не безнадёжны, хотя самих по себе задушевных разговоров, безусловно, мало. Верный признак серьёзных проблем – несущийся сверху монолог, заглушающий крики «А поговорить?» И ведь что ещё в блогерах замечательно: каждый посмотрит-послушает, а всё равно напишет что-то своё. Или не напишет – хозяин-барин, такому не прикажешь.

Пришёл черёд Ю. Луценко. Читайте завтра в блогах.

***

24.05.2016

В Інтернеті запущено флешмоб на підтримку «закону для українських фрілансерів» #4496

В Інтернеті запущено флешмоб на підтримку «закону для українських фрілансерів» #4496Законопроект #4496 суттєво спрощує експорт послуг з України. Найбільшу користь від нього мають отримати українські фрілансери та загалом ІТ-галузь, повідомив заступник міністра економіки М. Нефьодов, пише Watcher.

«Підтримай український фріланс: законопроект #4496, в якій наша команда приймає участь, і де потрібна ваша допомога! Please share!» – написав на своїй сторінці у Facebook М. Нефьодов.

У разі прийняття закону ІТ-галузь, фрілансери та усі ті, хто постачає послуги закордон (і цим приносить валютну виручку в Україну), чекають такі нововведення:

– можливість укладати електронні, а не паперові договори;

– визнання інвойсу і відмова від актів виконаних робіт;

– лібералізація валютного регулювання при експорті послуг;

– не вимагається переклад документів з англійської мови.

У Facebook було запущено окрему сторінку Підтримай український фріланс: законопроект #4496.

На сторінці всіх небайдужих закликають до лобіювання громадськості (crowd lobbying), що має допомогти пришвидшити прийняття закону.

«Наша мета: за допомогою Facebook-спільноти привернути увагу Парламенту та допомогти прийняти законопроект #4496», – пишуть активісти.

Законопроект вже понад чотири тижні перебуває без прогресу на розгляді Верховної Ради. Ініціатори пояснюють свою активність тим, що «кожен день затягування – це не лише додаткові витрати та непотрібна бюрократія, але і втрачена можливість для України бути серед лідерів постачання послуг у світі».

На їх сторінці у Facebook планується організувати дискусію, проводити заходи на підтримку законопроекту, стежити за його статусом, ділитися думками.

***

25.05.2016

Савченко тема № 1 за кількістю згадок у світових трендах Twitter

25 травня Н. Савченко повернулася в Україну після двох років незаконного перебування в полоні у російських окупантів. Ця тема одразу стала топовою для всього українського Інтернету, і не тільки українського, пише Watcher.

Буквально за півгодини з моменту поширення новини про можливе повернення Н. Савченко, ця тема стала № 1 в українських трендах Twitter. А потім вона потрапила у світові тренди.

***

2.06.2016

Хмельничани збираються перешкодити «зібранню сепаратистів»

В обласному центрі активісти закликають людей протистояти представникам псевдогромад. У соцмережах поширюється інформація із закликами недопустити в місті сепаратистських настроїв, повідомляє Depo.Хмельницький, пише depo.ua.

«Настав час стати на захист національних інтересів нашої держави! Представники “територіальних громад” запланували в Хмельницькому провести своє збіговисько, приурочене сепаратистським ідеям створення відповідних організацій, які виконуватимуть функції держави», – пише у своєму дописі хмельничанин С. Волков.

А ще він закликає «небайдужих Хмельничан спільними зусиллями влаштувати прихильникам федералізації “гідну зустріч”».

Нагадаємо, у Хмельницькому хочуть зібратися активісти «народних громад» зі всієї України.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

23.05.2016

Instagram открыл доступ к карусельной видеорекламе для всех рекламодателей

Формат был запущен еще в марте, позволяя компаниям демонстрировать несколько фото с кнопкой призыва к действию в одном рекламном блоке. Такие кампании, по словам площадки, увеличивали эффективность рекламы на 2.5 пункта. «С сегодняшнего дня рекламодатели смогут делиться пятью единицами контента, включая видео и фото, для более богатого сторителлинга», отмечено в блоге компании. Ранее площадка разрешила загружать 60-секундные ролики, пишет Marketing Media Review.

***

26.05.2016

Facebook закроет рекламную биржу FBX

Социальная сеть намерена закрыть рекламную биржу Fasebook Exchange (FBX), которая позволяет покупать десктопную рекламу, нацеленную на пользователей, уже посетивших сайт рекламодателя, отмечает searchengines.ru, пишет Marketing Media Review.

Вице-президент Facebook по управлению продуктами М. Идема заявил, что это решение связано с переориентацией компании на мобильный сегмент. По данным финансового отчёта за I квартал 2016 г., на доход от мобильной рекламы приходится 82 % от общей выручки Facebook.

«На сегодня мобайл является необходимым компонентом эффективных маркетинговых кампаний. Facebook помогает миллионам компаний понять путь к покупке их клиентов по различным устройствам. Динамические объявления и Пользовательские аудитории – по сути, мобильные продукты, поэтому расходы на Facebook Exchange были перенаправлены на эти решения», – отметил руководитель. Рекламная биржа Facebook Exchange была запущена в 2012 г.

***

31.05.2016

Facebook начал отслеживать всех пользователей интернета

Facebook расширил рекламную сеть на всех пользователей глобальной сети. Теперь он собирает обезличенную историю веб-серфинга всех, кто попадает на сайты-партнеры его рекламной сети, даже если они не являются зарегистрированными пользователями Facebook, пишет InternetUA.

Отслеживание всех пользователей

Facebook объявил о том, что отныне предоставляет обезличенную информацию обо всех пользователях Интернета участникам своей сети рекламы на мобильных устройствах Audience Network, даже если они не имеют учетных записей в Facebook. Компания с помощью кнопок «Нравится» и различных фрагментов кода на сайтах будет запоминать историю веб-серфинга и передавать ее партнерам.

До настоящего момента Facebook делился информацией только о зарегистрированных участниках социальной сети, у которых во время веб-серфинга оставалась активной аутентификация.

Рассказывая о нововведении газете Wall Street Journal, вице-президент Facebook по рекламе Э. Босворс сказал: «Рекламодатели и разработчики приложений имеют потенциальных клиентов, не входящих в число зарегистрированных на Facebook пользователей. Мы посчитали, что мы можем предложить им более качественное обслуживание». «Теперь мы сможем лучше понять, какую рекламу стоит отображать этой категории пользователей», – добавил он.

Например, теперь при посещении веб-сайтов с кулинарными рецептами пользователем, который не зарегистрирован в Facebook, компания сможет узнать, что он увлекается готовкой и предоставить эту информацию

рекламодателям. В дальнейшем он будет видеть соответствующие объявления на всех сайтах, на которых размещены рекламные блоки Audience Network.

Такой подход используют все рекламные сети, включая Google и «Яндекса», так как он зарекомендовал себя как наиболее эффективный.

Средства настройки

В Facebook заверили, что не будут использовать тактики, которые могут вызывать раздражение или отвлекать, например, не будут позволят рекламодателям использовать звуки в объявлениях. Также в компании обещают фильтровать случайные нажатия на объявления.

Кроме того, компания предоставляет пользователям возможность настройки того, какие объявления они видеть не хотят. Но для доступа к этой функции необходимо иметь аккаунт в Facebook, так как она находится в панели управления учетной записью.

Усиление конкуренции

В марте 2016 г. Facebook сообщил, что ежемесячно этой социальной сетью пользуются 1,65 млрд человек. Это половина всего интернет-населения в мире – согласно Международному союзу электросвязи, в 2015 г. глобальной сетью пользовались 3,17 млрд жителей планеты.

С таким количеством пользователей стремление расширить охват рекламной сети – вполне объяснимое желание, так как этот шаг позволит увеличить доход от рекламы и усилить конкуренцию с лидером на этом рынке – корпорацией Google. По данным Statista, в 2015 г. поисковый гигант занимал 33,3 % мирового рынка мобильной рекламы.

***

1.06.2016

Instagram запускає бізнес-профілі і аналітику для них

Instagram дасть компаніям можливість офіційно працювати на своїй платформі.

За допомогою нового Instagram Business Tools підприємці зможуть вести рекламні кампанії, аналізувати їх ефективність та перетворювати звичайні пости на рекламні напряму в додатку, пише MediaSapiens із посиланням на Forbes.

Провівши тести з представниками бізнесу, Instagram вирішив зміцнити свої позиції як гравця на ринку мобільної реклами і запровадив безкоштовні бізнес-профілі. Серед нових важливих функцій, які дає такий профіль, – це наявність кнопки «Контакт». За допомогою неї користувачі зможуть швидко зв’язатися з компанією. Функція буде корисною, наприклад, для профілів інтернет-магазинів тощо.

Інша функція, Insights – надаватиме дані про портрет і поведінку користувачів, ефективність тих чи інших постів. Відслідкувавши найбільш ефективні публікації, можна буде змінити їх тип, перетворивши на рекламні.

При цьому можна як вручну вказати цільову аудиторію, так і залишити це налаштування за замовчуванням.

Також через тісний зв'язок Instagram та Facebook власники бізнесу зможуть використовувати інструменти для визначення цільової аудиторії на основі даних із профілів Facebook: наприклад, стать, вік і місце проживання, особисті інтереси.

Поки що бізнес-профілі доступні в США, Новій Зеландії та Австралії, однак їх планують запровадити і для інших країн. У компанії Instagram міркують і над тим, щоб надати розширені функції користувачам, які не є представниками бізнесу, однак використовують свої акаунти в комерційних цілях.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

23.05.2016

Учёные: В соцсетях в друзья добавляют популярных и активных людей

Учёные из Университета Макгилла провели исследование в сфере социальных сетей и заметили интересную тенденцию и своеобразную иерархию при использовании соцсетей. За основу они взяли популярный Facebook, пишет HiTech-News.ru.

Уже давно известно, что человеку приятно чувствовать своё превосходство среди друзей и знакомых, однако данное утверждение не действует, когда речь идёт о социальных сетях. Собрав данные и составив статистику, специалисты доказали – когда человек добавляет в друзья нового друга, у последнего список товарищей в социальной сети намного больше. Помимо этого, они более популярнее и активнее. Согласно проделанной работе, люди из списка друзей чаще опубликовывают материалы и посты, а их сообщения больше читают.

Учёные назвали такое явление «парадокс дружбы», с которым сталкиваются все пользователи социальных сетей на протяжении жизни. Специалисты отметили – вне зависимости от активности пользователя, люди всегда добавляют в друзья тех, кто более активен, чем они сами.

Другие специалисты в области науки из Университета Оксфорда ранее опубликовали свою работу, в которой отмечено, что количество друзей в соцсетях никаким образом не влияет на дружбу в реальности.

***

23.05.2016

Социальные сети становятся для людей важнее дружбы, – исследование

В США ученые провели исследование и выяснили, чем согласны жертвовать американцы ради доступа к Интернету, передает The New York Times.

Как оказалось, многие готовы пожертвовать ближайшими друзьями и ценностями ради соцсетей, информирует Экономические известия.

Кроме того, согласно результатам исследования, близость и общение вживую жители США ставят ниже Интернета.

Самые старшие участники исследования признались, что в состоянии прожить без гаджетов не более 16 часов. Если же они лишены девайсов на более продолжительное время, то люди начинают ощущать себя несчастными.

Также сообщается, что из всех опрошенных 35 % респондентов проводят свободное время за играми в Интернете. А 41 % признаются, что посещают различные мероприятия и курорты лишь для новых фотографий, которые после будут опубликованы в соцсетях.

***

30.05.2016

Ученые рассказали, как и о чем говорят люди в социальных сетях

Ученые проанализировали сообщения, которые пользователи отправляют в Facebook. Оказалось, что мужчины ведут себя агрессивнее, а женщины в переписке чаще демонстрируют положительные эмоции, сообщает PloS One, пишет InternetUA.

В рамках исследования ученые проанализировали 10 млн сообщений, которые отправляли 52 тыс. пользователей. Лексический анализ показал, что женщины обычно создают более вежливые, мягкие и душевные сообщения, чаще выражают соучастие. Для мужчин более характерны споры, жаркие дискуссии и агрессивная лексика.

Исследователи также отмечают, что мужчины чаще рассуждают об абстрактных понятиях, а не о конкретных людях и их поведении. Женщины же, напротив, описывают определенных людей и их поступки.

Мужчины чаще женщин говорят о политике, спорте, специфических увлечениях. Зато у женщин в сообщениях гораздо чаще встречаются слова, которые относятся к социальным отношениям и позитивным эмоциям, а также преувеличения.

По итогам исследования ученые сделали вывод, что «женский» язык более теплый, «мужской» – более холодный

***

31.05.2016

Подростки online: как смартфоны влияют на нервную систему

Если подростку внезапно становится скучно, у него есть целая куча способов развлечься или просто убить время. «ВКонтакте», Twitter, Facebook, Instagram, Snapchat …

Согласно статистике, опубликованной в начале года Washington Post, американские школьники проводят в соцсетях до 9 часов в день при среднем для американца времени 4,5 часа. По Украине озвучивалась цифра в 2,5 часов в среднем по всем возрастным группам, а подростки всегда более восприимчивы к новому и привязаны к технике. Это позволяет предположить, что украинские подростки сидят в сети по 4–5 часов в сутки. Исследование агентства «Социоинформ» показало, что 85 % украинских школьников ежедневно заходят во «ВКонтакте» и 57 % называют его основным источником получения новостей. Эти данные получены еще до появления 3G. С улучшением покрытия и скорости Интернета, количество времени, проводимого подростками в соцсетях, будет только увеличиваться, пишет IGate.

Если у подростка уходят на сон здоровые 10 часов, 6 часов он проводит в школе и еще 5 часов разглядывает экран мобильника, в сутках остается всего 3 свободных часа. Это все очень важно, ведь взаимодействие с экраном влияет и на мышление человека, и на организм.

Исследование, проведенное Британским Обществом Психологии, показало, что у младенцев, которых часто развлекают с помощью смартфона или планшета, падают способности к концентрации и сосредоточению, медленнее растет словарный запас. Это связано с тем, что электроника заставляет детей привыкать к постоянным раздражителям, избыточной общественности жизни и делает их зависимыми от внимания. Доктор В. Дунклей, психиатр, утверждает, что неумеренное общение с техникой приводит к сенсорной перегрузке, ухудшению качества сна и гипервозбудимости нервной системы – как она это называет, «синдрому электорнного экрана». Но все эти исследования посвящены детям. Немало есть и работ про связь депрессии и соцсетей у взрослых. А что насчет подростков?

Последнее исследование по этой тематике опубликовано в журнале «Депрессивные и тревожные состояния» в 2016 г. В нем подтверждено, что использование социальных медиа связано с увеличением количества депрессий.

Голубой свет от экрана смартфона сбивает мозг человека с толку, нарушает циркадные ритмы и мешает выработке гормона мелатонина. Этот гормон регулирует эндокринную и имунную систему организма, управляет суточными и сезонными циклами, участвует в работе кровеносной, пищеварительной систем и мозга.

В результате было установлено, что после использования гаджетов процесс засыпания занимал больше времени, а фаза быстрого сна длилась меньше. У тех, кто читал с экрана книги, суточный ритм сбивался более чем на час. Они с трудом просыпались и чувствовали себя разбитыми в первой половине дня.

Хотя в эксперименте использовались iPad, избыточное излучение в синей части спектра характерно и для других гаджетов: планшетов, ноутбуков, смартфонов и жидкокристаллических мониторов. Исключение составляют устройства для чтения электронных книг с технологией e-paper, поскольку не излучают свет.

Ученые добавили, что хроническое подавление выработки мелатонина в организме увеличивает вероятность возникновения рака груди, простаты и кишечника. А сильнее всего это влияет именно на детей и подростков, ведь их организм еще развивается, и гормональная система нестабильна.

***

5.06.2016

Ученые рассказали, как социальные сети влияют на психологию молодых мам

Американские ученые из Университета штата Огайо описали модели поведения молодых матерей в социальной сети Facebook. С деталями работы можно ознакомиться в журнале Sex Roles, пишет InternetUA.

Статистический анализ 127 профилей недавно родивших женщин показал, что особенную активность в социальной сети проявляют те, которые слишком озабочены оценкой своей личности как матери со стороны окружающих. Это влияет на то, что они постоянно размещают фотографии детей в своем профиле. Также среди молодых матерей социальными сетями постоянно пользуются те, кто полагает, что общество предъявляет к ним высокие стандарты воспитания детей. Они проводят много времени онлайн в спорах с другими пользователями.

Было замечено, что практически все молодые мамы склонны слишком эмоционально реагировать на оставленные комментарии в Facebook. Как отмечают ученые, общение молодых матерей с другими пользователями социальных сетей способно еще более усугубить послеродовую депрессию.

Маніпулятивні технології

2.06.2016

Территория ботов. Кто и как создаёт параллельную реальность в украинских соцсетях

Кто есть кто на украинском рынке политического Facebook и как читать между строк посты известных блогеров, разбирались С. Крюкова и А. Пасютина, пишет Антикор со ссылкой на Интернет-ресурс «Страна».

…Спросом у заказчиков пользуются популярные блогеры – ЛОМы (лидеры общественного мнения) с более чем 5 тыс. подписчиков. Причем чем их больше, тем «дороже» блогер. Точка определения успеха в работе – когда пост попадает в медиа-мониторинг людей, принимающих решения в этой стране, или меняет их точку зрения на резонансные события. Совсем хорошо, когда тема попадает в поле зрения журналистов влиятельных изданий, «цепляет» ведущих из них, мотивируя к дополнительному расследованию.

«Ценность блогеров для политиков еще и в том, что информация, которая распространяется без персональной ответственности, весьма сомнительна. Другое дело, когда она подается со ссылкой на реального человека, с именем, фамилией и своей аудиторией», – рассказывает «Стране» глава парламентского Комитета по свободе слова и информации, журналист в прошлом В. Сюмар.

По этой же причине иногда имеет значение не столько количество подписчиков (все же важно, чтобы их было не менее трех тысяч), сколько социальные связи. То есть не численность, а персональный состав тех, кто в друзьях. Это мнение известного блогера А. Барабошко, который помимо того, что пишет тексты в соцсетях, зарабатывает еще и как посредник. По его словам, размещение одного поста стоит 50–100 долл. (зависит от веса, то бишь авторитета блогера), сам же А. Барабошко берет не меньше, 100 долл. за публикацию. И он, пожалуй, единственный герой этого текста, который честно признался, что пишет посты за деньги. Все остальные опрошенные «Страной» авторы ответили, что «топят» якобы за идею.

…Что касается ботов, то этот институт в Украине не структурирован и не систематизирован так, как в России.

Впрочем, боты у нас тоже имеются, просто, в отличие от РФ, их в одном здании (условном Ольгино) не держат и их просто физически не так много, как в соседней стране. Но практически все политические силы, активно представленные в соцсетях, имеют свои армии ботов. Есть они и у самых крупных блогеров. Основная их задача – лайкать, оставлять комментарии, нападать на вражеских блогеров или политиков, троллить их, создавать истерику или, наоборот, восторг вокруг заданных свыше месседжей. Вбрасывать какую-то непроверенную информацию, на которую потом смогут ссылаться ЛОМы, а уже на ЛОМов – СМИ. Таким образом легализуется множество фейков. Подробнее читайте по ссылке.

…Армии ботов и ЛОМов, превратив соцсети в поле битвы за интересы своих заказчиков, порождают волны ненависти, которые охватывают огромное число обычных людей, разделяя их по линии «свой-чужой».

Наиболее распространенным способом воздействия на аудиторию у нас уже давно является технология управляемой истерики. Сначала появляются кликуши, вещающие про «распятых мальчиков» или «сепаров» в телесериале. Это подхватывают ЛОМы. За ними – журналисты и СМИ. Эмоции катятся

валом, умело подпитываемым специально обученными товарищами. Люди мобилизуются за «своих» против «чужих». Требуют мести, расправы, войны до победного конца, голосования за нужную политсилу, которая все это обеспечит.

Самое плохое, что вслед за каждой волной такой истерики следует френдоцит. Пользователи соцсетей удаляют из своих друзей тех, кто не попал в струю истерики, показав себя «чужими». В конце концов в ленте остаются только «свои». Таким образом, люди сами себя лишают доступа к альтернативной точке зрения. А это, в свою очередь, сильно облегчает задачу манипуляторам.

Как можно уберечься от этого? Как научиться думать своей головой, а не «коллективным разумом» ботов и ЛОМов, получающих за каждый пост по 100-150 долл.?

Выход только один – не принимать безальтернативную картину мира. Не закрывать для себя доступ к альтернативным точкам зрения, «поселить» в своей ленте ЛОМов из разных лагерей, с разными убеждениями. Не верить на слово никому, пока не появятся подтверждения. И, в конце концов, включать здравый смысл, прежде чем включить истерику.

***

2.06.2016

В Росії за образи в соцмережах можна буде отримати компенсацію

Російські нотаріуси стали посвідчувати факти троллінгу в Інтернеті, повідомляє MediaSapiens.

Про це пише газета «Известия» з посиланням на Федеральну нотаріальну палату (ФНП).

Протокол огляду сторінки сайту, складений нотаріусом, необхідний для позову про компенсацію моральної шкоди. Таке розширення діяльності нотаріусів у ФНП вважають логічним, враховуючи швидкий розвиток інтернету.

Згідно з аналітичними даними за доменними суперечками, у російській судовій практиці майже в 50 % випадків використовувався протокол огляду сайту, виданий нотаріусом.

Позивач може розраховувати на компенсацію мінімум в 15 тис. р. (близько 5550 грн) за образи в соцмережах. Максимальна сума позову законодавчо не закріплена – її можна встановити на будь-якому рівні.

На думку юристів ФНП, нововведення може стати популярним і серед компаній, адже тролінг може бути спрямований і на знищення ділової репутації бізнесу. Основна складність у справах даної категорії – довести, що інтернет-сторінка належить конкретній особі, і визначити коло відповідачів.

Згідно зі статистикою i-SAFE foundation, більше половини підлітків зазнали знущання в Інтернеті і приблизно стільки ж займалися кіберхуліганством. Кожен третій отримував погрози. Більше 25 % підлітків

зазнавали повторного цькування в Інтернеті або через телефонні дзвінки. Дівчата-підлітки удвічі частіше стають об'єктом для тролінгу, ніж хлопці.

Інше дослідження, проведне групою Demos, з'ясувало, що кожні 10 секунд хтось публікує сексистські висловлювання у Twitter. І майже в половині випадків автори цих постів – жінки.

American Trends Panel наводить інші дані: серед дорослих із тролінгом частіше стикаються чоловіки, аніж жінки (44 % і 37 % відповідно). Чоловіки частіше стикаються з лайкою і погрозами фізичної розправи. У той час як жінки мають справу із сексуальними домаганнями в онлайні та переслідуваннями.

Як повідомлялось, керівництво Twitter ухвалило рішення створити раду, яка займеться питаннями боротьби з образами і залякуванням у соцмережі (Twitter Trust and Safety Council). За словами керівника з питань глобальної політики Twitter П. Картес, компанія винайме спеціалістів з майже 40 правозахисних організацій.

Також The Guardian вказував на проблему залякування активістів, журналістів та правозахисників у Росії інтернет-тролями.

Видання звертало увагу і на зростання кількості онлайн-образ. The Guardian замовило дослідження 70 млн коментарів на своєму сайті, залишених користувачами з 1999 р. і дотепер. Виявилося, що з-поміж 10 авторів, які зібрали найбільше образливих коментарів, вісім жінок і двоє чорношкірих чоловіків.

***

24.05.2016

У Росії нарахували 1,5 тис. груп про суїцид «ВКонтакте»

Колективний суїцид 20 травня відбувся як мінімум в одному місті РФ

Не менш як шість закритих груп у соцмережі «ВКонтакте» потрапили в опрацювання петербурзьких слідчих, які 20 травня порушили кримінальну справу за ст. 110, ст. 33 ч. 4 КК РФ «Підбурювання до доведення до самогубства», повідомляє Нова газета, пише LB.ua.

Як з'ясували правоохоронці, домени п'яти із шести груп, які потрапили під підозру, зареєстровані в різних містах Росії: у Москві, Петербурзі, Комі, Воронежі, а один – на Карибських островах.

«Насправді подібних провокаційних груп в Інтернеті набагато більше, за нашими підрахунками, близько 1,5 тис. Але згадані шість потрапили в поле зору правоохоронних органів передовсім тому, що стосовно них вже є підозри про причетність до конкретних трагедій з дітьми в 2015–2016 рр.», – пояснили в петербурзькому Головному слідчому управлінні.

За інформацією слідчих, на 20 травня був призначений черговий груповий суїцид у декількох містах Росії. Попередній, за наявними відомостями, планувався 17 травня, а наступний – 27 травня. І якщо 17 травня груповий суїцид вдалося запобігти, то 20 травня, за даними слідства, він

відбувся, як мінімум, в одному місті. Інформація про інші нещасні випадки, що сталися з дітьми 20 травня, перевіряється.

За даними Нової газети, передплатникам закритих спільнот (так званих груп смерті) в мережі пропонується брати участь у колективному квесті. Кілька десятків дітей могли вчинити самогубство під впливом тематичних груп «ВКонтакте».

***

26.05.2016

Во «ВКонтакте» закрыли 80 групп

Кибердружинники обнаружили в соцсети 80 групп, пропагандирующих суицид, доступ к которым впоследствии был заблокирован, пишет InternetUA.

Наиболее популярное сообщество имело 20 тыс. подписчиков. В заблокированных группах участники активно распространяли психоделический контент, видеозаписи самоубийств, подробно описывали способы их осуществления, обсуждали громкие истории подростковых суицидов.

Пользователи «ВКонтакте» взаимодействуют с надзорными ведомствами и ограничивают доступ к суицидальным сообществам. На закрытых страницах администрация соцсети размещает номера телефонов экстренной психологической помощи для подростков.

«Кибердружина» – это волонтерская организация, созданная в 2011 г.

Зарубіжні спецслужби і технології «соціального контролю»

31.05.2016

Twitter, Facebook, Microsoft и YouTube будут бороться с онлайн-враждой в ЕС

Еврокомиссия и компании Facebook, Twitter, YouTube, Microsoft подписали во вторник, 31 мая, соглашение, которое предусматривает обязательства по борьбе с разжиганием ненависти в Интернете. Об этом говорится в сообщении Еврокомиссии, пишет InternetUA.

Новые правила ЕС предполагают, что при размещении пользователями онлайн-платформ агрессивных высказываний администрация ресурсов будет подробно анализировать эти записи. В случае подтверждения наличия информации, разжигающей вражду, компании будут удалять посты или деактивировать аккаунты в течение 24 часов после публикации.

Еврокомиссия и интернет-компании признают, что распространение в сети незаконной информации, порождающей агрессию, не только отрицательно влияет на те или иные социальные группы и отдельные лица, но и негативно

сказывается на тех, кто выступает за свободу, толерантность и борется с дискриминацией в открытом обществе.

«Язык ненависти оказывает сдерживающий эффект на демократический дискурс в онлайн-среде», – заявили в Еврокомиссии.

Решение разработать единые правила было принято после терактов в Брюсселе. В ЕС обратили внимание, что за последние годы в Интернете в разы увеличилось количество экстремистских публикаций. Еврокомиссары считают, что социальные сети являются одним из инструментов распространения ненависти.

***

25.05.2016

Apple закрыла в OS X уязвимости, которые использовали британские спецслужбы для слежки за пользователями

Эксперты правительственных спецслужб, как правило, неохотно делятся с производителями аппаратного и программного обеспечения информацией об обнаруженных уязвимостях и предпочитают использовать бреши для слежки за подозреваемыми. Тем не менее, иногда они идут на встречу компаниям и сообщают им о своих находках, пишет InternetUA.

Как сообщает Securitylab, о двух уязвимостях в операционной системе OS X стало известно от экспертов Группы безопасности электронных коммуникаций (Communications-Electronics Security Group, CESG) Центра правительственной связи Великобритании. Бреши в безопасности программной платформы позволяли вызвать повреждение памяти и отказ в обслуживании Mac.

Исправленные на прошлой неделе уязвимости затрагивали OS X El Capitan 10.11 и более поздние версии. CVE-2016-1829 и CVE-2016-1822 позволяли вызвать отказ в обслуживании с помощью специально сконфигурированного приложения или удаленно выполнить код.

Как рассказал профессор криптографии Университета имени Бар-Илана (Израиль) И. Линделла, CESG сообщила Apple об уязвимостях, поскольку «они больше не были нужны спецслужбе». В распоряжении правоохранителей могут быть эксплоиты для других уязвимостей, позволяющие достигнуть тех же результатов.

***

25.05.2016

Росіянина ув’язнили за репост повідомлення журналіста ЛІГА.net

Совєтський районний суд Астрахані 16 травня виніс вирок керівнику руху «Русские Астрахани» І. Стеніну у вигляді двох років позбавлення волі за репост повідомлення журналіста ЛІГА.net, пише MediaSapiens.

Громадянин Росії І. Стенін прокоментував копію цього запису, додавши: «Смерть кремлівським окупантам! Руки геть від України!», пише ЛІГА.net.

У січні 2015 р. слідчий ФСБ звинуватив І. Стеніна «в закликах до здійснення екстремістської діяльності».

16 травня 2016 р. російський суд підтвердив обвинувачення і засудив І. Стеніна до двох років колонії-поселення.

У Росії за останні два роки засудили безліч людей за відмову підтримувати війну проти України.

***

27.05.2016

Активисты сообщили о блокировке в Facebook во время визита Обамы во Вьетнам

Вьетнамские власти ограничили на несколько дней доступ к Facebook внутри страны во время визита президента США Б. Обамы, передает Reuters со ссылкой на местную оппозицию, пишет InternetUA.

Представители организаций Access Now и Viet Tan сообщили, что доступ к соцсети был ограничен, а временами и полностью заблокирован внутри Вьетнама, начиная с воскресенья 22 мая по среду 25 мая.

Активисты сообщили, что подобные шаги вьетнамские власти приняли для того, чтобы не дать выразить протест против визита Б. Обамы в соцсетях.

Отмечается, что подобные меры по блокировке применяются во время резонансных политических событий в таких странах, как Китай, Уганда и Турция.

***

31.05.2016

Власти Ирана обяжут мессенджеры хранить данные внутри страны

Верховный совет по киберпространству Исламской Республики Иран потребовал от зарубежных сервисов для общения хранить данные на серверах внутри страны. Об этом сообщает Reuters, пишет InternetUA.

Принципы основаны на предложениях верховного лидера Ирана аятоллы А. Хаменеи.

«Чтобы продолжить свою деятельность, иностранные компании, работающие в стране, обязаны передавать все данные и информацию о действиях пользователей, которые являются гражданами Ирана, внутри государства», – говорится в заявлении совета по киберпространству. Для переноса данных власти Ирана отвели зарубежным корпорациям год.

Под действие новых правил попадает и популярный в этой стране мессенджер Telegram.

***

3.06.2016
Піхут В.
Twitter відновив пародійний акаунт В. Путіна

Twitter звинуватили в поганому почутті гумору, коли соцмережа тимчасово закрила популярний акаунт пародій на президента Росії В. Путіна, передає УНН із посиланням на BBC, пишуть Українські Національні Новини.

Акаунт @DarthPutinKGB мав більше 50 тис. фоловерів.

Користувачів Twitter також на короткий час позбавили доступу до чотирьох інших акаунтів з жартами на російську тематику. Зокрема, @SovietSergey, пасквіль міністра закордонних справ Росії С. Лаврова та @AmbYakovenkoNot, який висміює посла Росії у Великій Британії О. Яковенко.

Всі призупинені акаунти, у тому числі @SovietSergey, тепер відновили. Але тимчасове закриття акаунту DarthPutinKGB зокрема викликало обурення користувачів Twitter, а також багато гумору.

Із хештегом #NoGulagforDarthPutinKGB доброзичливі користувачі Twitter постили слова підтримки дискваліфікованого @DarthPutinKGB та критикували Twitter.

«Шановний @twitter, чому це ти вирішив призупинити один з найсмішніших акаунтів @DarthPutinKGB? Це не тролінг, а жартівливий акаунт», – написав у своєму Twitter чинний президент Естонії Т. Г. Ільвес.

Колишній чемпіон світу з шахів Г. Каспаров звинуватив соцмережу у тому, що вона «бере уроки цензури у Кремля».

Коли доступ до акаунту відновили, @DarthPutinKGB жартома пообіцяли репресії на тих, хто не виявив своєї відданості, коли акаунт заслали на кібервідпочинок.

***

1.06.2016
У КНДР з'явився і одразу зник аналог Facebook

Клонована північнокорейська версія соціальної мережі Facebook на короткий час з'явилася в Інтернеті, але потім швидко зникла, пише MediaSapiens.

Про це пише російська служба BBC.

Вона була зареєстрована за адресою StarCon.net.kp в КНДР і була схожа відразу на кілька інших популярних соцмереж.

Залишається невідомим, хто саме створив портал StarCon, проте експерти вважають, що це був пробний запуск майбутнього сервісу, який збирається запропонувати користувачам єдиний оператор інтернету в Північній Кореї.

Першим сайт StarCon помітив Д. Мадор, співробітник інтернет-компанії Dyn. За його словами, відкриття сайту, зареєстрованого в Північній Кореї, –

вкрай рідкісне явище, яке відразу привертає увагу. Назва сайту дає підстави припустити, що воно пов'язане з державною компанією Star.

Сайт StarCon був створений на основі комерційного пакета ПО під назвою phpDolphin і мав багато ознак звичних нам соцмереж, у тому числі новинну стрічку, систему обміну повідомленнями та сторінки для особистих даних користувачів. Однак багато сторінок сайту були недопрацьовані і заповнені безглуздим текстом.

Через день після появи сайту він зазнав зламу і став перенаправляти всіх користувачів на перегляд одного з відеороликів, розміщених на порталі YouTube. Після цього він повністю зник з мережі.

***

3.06.2016

За сепаратистские комментарии в Интернете одессит получил 3 года условно

Приморский райсуд Одессы приговорил к трем годам лишения свободы условно одессита, который в Интернете призывал к войне и терактам, пишет InternetUA.

Также за публичные призывы к совершению террористического акта у обвиняемого конфисковали компьютер, ноутбук и роутер.

Как сообщает корреспондент Украинской Службы Информации, такое решение опубликовано в Едином реестре судебных решений Украины.

Одессита, который зарегистрирован в Facebook как С. Мамчур, а в интернет-издании «Таймер» под ником «Сепаратист», осудили за то, что с февраля по июль 2015 г. он сделал ряд публикаций с прямыми призывами к убийству сограждан.

Так, он призывал одесситов к «очищению войной» и заявлял, что «надо взрывать украинских фашистов», советуя для этого использовать бомбу с часовым механизмом.

Смягчающими факторами в суде стали положительная характеристика обвиняемого с места работы и информация о том, что он ухаживает за больной матерью.

***

26.05.2016

Жители Луганщины осуждены на 5 лет за антиукраинские «посты» в социальной сети

Жители Луганщины были осуждены за призывы к проведению акций, нацеленных на поддержку «ЛНР» «ДНР», пишет InternetUA.

Об этом сообщает пресс-служба прокуратуры Луганской области.

Северодонецкий городской суд и Кременской районный суд Луганской области утвердили обвинительные приговоры по двум уголовным делам.

Осужденные были наказаны за распространение материалов с призывами к изменению Государственной границы Украины и призывы к проведению сепаратистских акций в социальной сети «ВКонтакте».

Преступники постоянно размещали в социальной сети тексты, поддерживающие террористические бандформирования «ЛНР» и «ДНР» и признающие их республиками.

Интернет-террористы были осуждены на пять лет лишения свободы с освобождением от отбывания наказания с испытанием.

***

23.05.2016

У Таїланді жінку хочуть ув'язнити на 15 років за коментар «Ок» у Facebook

У Таїланді поліція затримала 40-річну жінку П. Чанкідж, звинуативши в образі монархії через її коментар у Facebook. Їй загрожує до 15 років в'язниці, пише MediaSapiens із посиланням на BBC.

Як зазначив її адвокат, єдиний доказ, наданий поліцією, – це обмін коментарями у Facebook між П. Чанкідж і одним політичним активістом. Вона лише відповіла «Ок» на пост активіста. Поліція назвала її начебто нешкідливий коментар наклепом. У поліції кажуть, що вона повинна була засудити слова політактівіста.

***

28.05.2016

Россия хочет взять под контроль российский сегмент Интернета

Регулирование всех критических элементов инфраструктуры российского сегмента Интернета станет исключительным правом государства, если документ станет законом, пишет InternetUA.

Минкомсвязи разработало законопроект под рабочим названием «Об автономной системе интернет», сообщила газета «Ведомости». Документ посвящен вопросам регулирования инфраструктуры российского сегмента Интернета – совокупность расположенных в стране линий и узлов связи, центров обработки данных (ЦОД), которые обеспечивают работоспособность сети, уточняет издание. Регулирование всех критических элементов инфраструктуры российского сегмента Интернета станет исключительным правом государства, если документ станет законом, пишут «Ведомости», информирует eizvestia.com.

Разработка документа пока находится в ранней стадии, с главой Минкомсвязи Н. Никифоровым он не обсуждался, сообщил «Ведомостям» федеральный чиновник. Нынешняя версия законопроекта – апрельская, и у нее пока нет статуса – нет ни внутреннего, ни межведомственного согласования, уточнил собеседник РБК, близкий к Минкомсвязи. В Координационном центре

(КЦ) национального домена сети Интернет документ не видели и комментировать его по публикациям в СМИ отказались. Представитель Роскомнадзора поступил так же. Два сотрудника Минкомсвязи отказались от комментариев, сославшись на гриф «секретно». Вице-премьеру А. Дворковичу законопроект не поступал, сказала его представитель.

Речь идет о комплексе поправок в законы «О связи» и «Об информации…», который подразумевает контроль над инфраструктурой российского Интернета со стороны государства. В частности, в документе (часть его есть в распоряжении РБК) вводится понятие так называемой автономной системы – «совокупности средств связи и других технических средств с уникальным номером, пропуск трафика между которыми осуществляется по единым правилам». Эта система идентифицируется уникальным номером, следует из документа. Под автономной системой может подразумеваться собственная сеть любой компании – оператора связи, интернет-компании и др.

Государство собирается контролировать автономные системы, созданные физическими и юридическими лицами, а также индивидуальными предпринимателями. Все получившие в такой сети IP-адрес пользователи обязаны предоставить государству сведения о себе для размещения в государственной информационной системе, следует из документа. Также предполагается, что владельцы автономной системы, которые «взаимодействуют с автономной системой иностранного государства», должны будут использовать технические средства контроля трансграничного трафика.

В документе вводится в существующее законодательство новый пункт «Регулирование российской части сети интернет», в котором, по данным издания, речь идет о регулировании критических элементов инфраструктуры сети (национальные домены в зонах .ru и .рф, точки обмена трафиком и др.). Управлять российским сегментом Интернета должен федеральный орган исполнительной власти в соответствии с Законом «О контрактной системе в сфере закупок товаров, работ, услуг для государственных и муниципальных нужд», он должен заключать отдельный контракт на управление и контракт на функционирование критических элементов сети (с национальным администратором домена (КЦ), с операторами критических элементов сети), пишут «Ведомости».

В России необходимо создать единую федеральную информационную систему «обеспечения целостности и устойчивости Рунета», следует из документа. В эту инфосистему будут включены системы маршрутно-адресной информации, мониторинга трафика, система корневых доменных имен. По сути это позволит российскому сегменту Интернета работать автономно от мировой паутины.

***

3.06.2016
Педья Калайджич (Pedja Kalajdzic)

Десятки людей в России сажают в тюрьмы за «лайки» и ссылки в соцсетях

Россия жестко подавляет обычных пользователей социальных сетей, если они выкладывают в Интернет вещи, которые могут быть истолкованы как «опасность для государства». А. Бубеева приговорили более чем к двум годам тюрьмы за картинку, которой он поделился с 12 своими друзьями в социальной сети «ВКонтакте», пишут ИноСМИ.Ru.

«Рука сжимает тюбик с зубной пастой, зубная паста вытекает. Рядом – слова о “выдавливании” страны из себя».

Это описание картинки, благодаря которой А. Бубеев оказался в тюрьме. За то, что он поделился ею с 12 друзьями в соцсетях, его приговорили к тюремному заключению сроком более двух лет, пишет информационное агентство АР в статье, опубликованной в понедельник…

Используют закон об экстремизме

По меньшей мере 54 человека в России были посажены в тюрьмы за «разжигание ненависти», большинство из них – за то, что либо сами выкладывали в сеть какие-то вещи, либо делились ими. Эта цифра почти в пять раз выше аналогичной пять лет тому назад, по данным правозащитной группы СОВА, располагающейся в Москве. Группа изучает права человека, национализм и ксенофобию в России. Количество приговоров за разжигание ненависти возросло с 92 в 2010 г. до 233 в прошлом году.

Российский закон от 2002 г. определяет экстремизм как деятельность, «подрывающую безопасность государства и конституционный порядок» или «прославляющую расизм или терроризм, а также призывающую к этому других».

Расплывчатое определение в законе делает возможным преследование самых разных людей – от тех, кто создает террористическую ячейку или расхаживает с нацистскими символами, до тех, кто чаще всего пишет в сети то, что может быть истолковано как опасность для государства. В конце концов суд сам выносит решение о том, представляет ли пост в социальных медиа опасность для государства.

Атака на тех, кто критиковал вмешательство в дела Украины

В феврале 2014 г. президент В. Путин кроме того подписал дополнение к закону, которое предусматривает более серьезное наказание за ненасильственные экстремистские преступления, такие как разжигание ненависти. В том же году, но позднее – после того как Россия аннексировала Крымский полуостров – Путин подписал закон, превративший «шаги, направленные на разрушение территориальной целостности России» в преступление, за которое можно получить до пяти лет тюрьмы.

Многие из тех, кто оказался в тюрьме за разжигание ненависти в социальных сетях в России в последние пару лет, критически относились к российскому вмешательству в Украине.

Так произошло и с картинками и статьями, которые репостил А. Бубеев.

А. Бубеев считает, что то, что его посадили в тюрьму, сделано специально: чтобы другие граждане опасались высказывать свое мнение, говорит его адвокат С. Сидоркина в беседе с АР.

Приговаривают к годам в тюрьме

Раньше в этом месяце еще один человек был приговорен к двум годам тюрьмы в Астрахани за то, что выложил призыв к украинцам «бороться против путинских оккупационных сил».

В декабре одного мужчину в Сибири осудили на пять лет тюрьмы за «разжигание ненависти» по отношению к жителям Восточной Украины в видео, которое он выложил в сеть.

В октябре суд на юге России суд приговорил политического активиста к двум годам тюрьмы за незаконную акцию протеста и посты в социальных медиа, в которых он критиковал Путина и призывал юг России присоединяться к Украине.

Сетевое сообщество принадлежит пропутински настроенному миллиардеру

По данным группы СОВА, половина постов, приведших к приговорам за разжигание ненависти, выложена в сети «ВКонтакте». Компания, которая занимается этой социальной сетью, принадлежит прокремлевски настроенному миллиардеру А. Усманову. Директор СОВА А. Верховский считает, что благодаря этому российским властям легче получать доступ к аккаунтам «ВКонтакте», чем в иностранных сетевых сообществах.

Защитник А. Бубеева утверждает, что благодаря настройкам приватности в соцсети его страница была доступна ему и 12 его друзьям. Адвокат говорит в беседе с АР, что не может объяснить, как служба безопасности обнаружила его пост – и как она вообще получила доступ к аккаунтам в этой сети.

«ВКонтакте» не захотела комментировать дело, когда информационное агентство к ней обратилось.

В начале 2000 г. Россию захлестнула волна насилия по отношению к азиатским иностранным рабочим, но количество нападений резко сократилось после того, как несколько десятков неонацистов получили длительные тюремные сроки за экстремизм.

Борцы за права человека и адвокаты, которым довелось работать с делами об экстремизме, говорят, что спад насильственных преступлений на почве ненависти заставили полицию и следственные органы перейти к уголовному преследованию за ненасильственные оскорбления, чтобы показать, что борьба с экстремизмом продолжается, утверждает АР.

Проблема захисту даних. DDOS та вірусні атаки

23.05.2015

Определены самые распространенные вирусы

Компания Check Point исследовала самые распространенные киберугрозы и выяснила, что лидерами являются программы Conficker, Sality и ZeroAccess, пишет InternetUA.

Исследователи заявили, что в настоящее время основной угрозой назван компьютерный червь Conficker. С 2008 г. вредоносная программа заразила миллионы компьютеров по всему миру, распространяясь через социальные сети, включая Facebook и Skype, а также популярные сервисы электронной почты. Вредонос эксплуатировал уязвимость Windows (CVE-2008-4250), которая не была на тот момент устранена.

Check Point также называют Conficker главной угрозой прошлого месяца, с помощью этой программы злоумышленники совершили 17 % из вредоносных атак, обнаруженных экспертами. Авторы вредоноса до сих пор не пойманы, несмотря на обещанную награду 250 тыс. долл. от Microsoft. С 2008 г. Conficker заражал не только жесткие диски и USB-накопители, но даже нательные камеры видеонаблюдения офицеров полиции США. Эксперты из британского CERT (Национальный центр реагирования на киберугрозы) обнаружили более полумиллиона инфицированных Conficker устройств в апреле этого года.

Семейство вредоносов Sality можно назвать второй наиболее распространенной угрозой для пользователей ОС Windows, поскольку с помощью вредоносных программ было совершено 12 % обнаруженных атак. Представители этого семейства были впервые выявлены в 2010 г.

Третьей из наибольших угроз можно назвать ботнет ZeroAccess. Количество атак при помощи ботнета составило 6 %. Как считается, руткит ZeroAccess находится на более миллиона устройств. Преступники все еще могут обновлять вредонос, поскольку попытка взлома C&C-серверов в 2013 г. не удалась.

Наиболее распространенными вредоносными программами для Android-устройств являются HummingBad и Lop, а для устройств на базе iOS – XcodeGhost.

***

24.05.2016

Прочитать вашу переписку в Facebook может любой работник компании в любое время

Похоже, Facebook достаточно продолжительное время читает наши личные сообщения в рекламных и многих других целях. Причем доступ к этой информации есть не просто у программного обеспечения, которое анализирует информацию для предоставления актуальных для каждого партнерских предложений, а у каждого рядового сотрудника компании, пишет InternetUA.

Многие компании анализируют переписку для таргетированной рекламы. Даже Google регулярно «читает» всю нашу почту. Тем не менее, это делает специальный софт, доступа к которому у сотрудников просто нет. И эти

действия поискового гиганта не противоречат действующему мировому законодательству.

Ситуацию с Facebook сегодня рассматривают совершенно по другому. В данном случае участие принимает человеческий ресурс, что совершенно недопустимо – по крайней мере, так сегодня видят ситуацию крупнейшие мировые IT-ресурсы.

***

24.05.2016

Дослідження: Telegram і WhatsApp погано захищені від доступу сторонніх користувачів та спецслужб до акаунтів користувачів

Такі «захищені» месенджери, як Telegram, WhatsApp та Signal виявилися вразливими через можливість доступу до акаунта користувача через викрадення SMS – про це йдеться в дослідженні українських фахівців, пише Watcher.

Причому доступ до акаунта можуть отримати як спецслужби через співпрацю з мобільними операторами, так і будь-хто за наявності достатніх ресурсів і навіть без співпраці з мобільними операторами.

Після гучних зламів Telegram-акаунтів російських опозиціонерів за допомогою російського мобільного оператора МТС (а таких зламів, насправді, значно більше) постали два закономірних запитання:

1. Чи захищені інші месенджери від такого типу атак?
2. Чи можуть користувачі якось убезпечити свої акаунти від таких зламів?

Нещодавно опубліковане дослідження експериментально встановило, що:

1. Месенджери Signal, WhatsApp та Telegram не захищені від таких атак.
2. Користувач не може вбудованими в месенджери способами убезпечити свої акаунти від таких зламів.

Коротко результати дослідження можна побачити у вигляді таблиці:

«Защищённые» мессенджеры: если злоумышленник получит доступ к SMS пользователя

	Signal	WhatsApp	Telegram
Можно ли угнать аккаунт при настройках «по умолчанию»?	Да	Да	Да
Можно ли предотвратить угон?	Нет	Нет	Нет (несмотря на 2FA)
Какую информацию получит атакующий? (контакты, содержимое переписки)	Никакой	Никакой	Все контакты и переписку из обычных не секретных чатов Никакой, если была 2FA
Узнает ли жертва, что её аккаунт угнали?	Нет (но перестают отправляться сообщения – при этом ни слова о том, почему)	Да (деактивирует приложение жертвы)	Да (код для входа и сервисное сообщение о входе с другого устройства) Если была 2FA - требование зарегистрироваться снова
Увидит ли собеседник жертвы, что «что-то не так»?	Да (в текущем чате покажет сервисное уведомление, что у собеседника «изменился код безопасности»)	Нет (Да, если собеседник включит настройку Settings => Account => Security => Show security notifications – тогда увидит сервисное уведомление)	Нет (просто новый секретный чат, никакого специального уведомления) Да, сли была 2FA - уведомление, что ваш контакт присоединился к Telegram, позже (через 12-16 часов) в старых чатах вместо имени контакта «Deleted Account»

При цьому, зверніть увагу, злам акаунта не означає, що атакуючий зможе отримати ваші минулі переписки – ні, не зможе (окрім несекретних чатів у Telegram якщо не була увімкнена двофакторна авторизація). Але зловмисник зможе залогінитися з вашим номером телефону і писати від вашого імені вашим контактам.

Звісно, для того щоб отримати доступ до акаунта користувача у вищезазначених месенджерах, доведеться отримати доступ до його SMS, але, як показує практика, це цілком реально.

Як це покроково виглядає, і що робити користувачам, ви можете прочитати на сторінці дослідження.

***

24.05.2016

НАТО и ЕС объединят усилия в борьбе с российскими хакерами

Возможность проникновения российских хакеров в компьютерные сети обе структуры считают одной из наиболее серьезных угроз, пишет «Центр информационной безопасности».

Евросоюз и НАТО подпишут соглашение о сотрудничестве в борьбе с вызовами, которые стоят перед обеими структурами. В числе угроз названы российские кибератаки, миграционный кризис и развал государств на периферии Европы, сообщило агентство РБК со ссылкой на данные Reuters.

Согласно источникам последнего, что совместные действия будут предусматривать как силовой ответ, так и мягкий подход к обеспечению безопасности, борьбу с враждебной пропагандой и консультации для стабилизации положения в сопредельных странах.

Одной из серьезных угроз обе структуры считают возможность проникновения российских хакеров в компьютерные сети. «Если Россия совершит нападение в киберпространстве, то нам не придется тратить две недели на переговоры, на которых мы будем выяснять, кто из нас что должен делать», – пояснил агентству смысл соглашения источник из оборонной сферы ЕС, тесно работающий с НАТО.

***

24.05.2016

Злоумышленники используют уникальные скрипты в атаках на банки Ближневосточного региона

Исследователи компании FireEye зафиксировали вредоносную кампанию, направленную на финансовые организации, расположенные в Ближневосточном регионе. В ходе кампании злоумышленники рассылают банкам электронные письма, содержащие вредоносные вложения. По всей видимости, пока атаки осуществляются в разведывательных целях. Как отмечают эксперты, преступники применяют уникальные скрипты, что довольно редко встречается в подобных кампаниях, пишет InternetUA.

В ходе атак злоумышленники рассылают сотрудникам целевых финучреждений электронные сообщения, содержащие XLS-файлы с вредоносным макросом. Для усыпления бдительности пользователей в темах сообщений указывается информация, связанная с IT-инфраструктурой, например, «отчет о состоянии сервера» и пр.

В одном из случаев письмо содержало настоящую переписку между несколькими служащими банка, включая контактную информацию сотрудников ряда других финучреждений. Далее это сообщение перенаправлялось другим работникам банка, но уже с прикрепленным вредоносным документом. Как отмечают специалисты, вредоносный макрос работает только на компьютерах под управлением Windows Vista.

После успешного запуска макроса на экране компьютера жертвы отображался дополнительный контент, что нехарактерно для подобных вредоносных кампаний. Однако в данном случае злоумышленники приняли дополнительные меры для усыпления подозрительности пользователей.

Активация макроса приводит к запуску скрипта, который загружает кастомизированную версию утилиты Mimikatz и BAT-файл, использующийся

для сбора важной информации о целевой системе. В том числе сведения о текущем авторизованном пользователе, имени хоста, конфигурации сети, индивидуальных и групповых учетных записях, работающих процессах и пр.

Одной из интересных особенностей вредоноса является использование DNS-запросов в качестве каналов для эксфильтрации данных. Данная техника применяется для сокрытия вредоносной активности. DNS-протокол вряд ли будет заблокирован, а его применение, скорее всего, не вызовет подозрений, полагают исследователи FireEye.

***

23.05.2016

Уязвимость в Instagram позволяла взломать 20 млн учетных записей

Консультант по безопасности А. Свиннен обнаружил уязвимости в системе авторизации Instagram. По словам эксперта, отсутствие контроля аутентификации совместно с уязвимостью, позволяющей сослаться на прямой объект в памяти, могли позволить преступникам взломать порядка 4 % существующих учетных записей (приблизительно 20 млн). Проблема безопасности заключалась в системе временной блокировки учетной записи, пишет InternetUA.

Во время проверки безопасности А. Свиннен обнаружил, что формы верификации учетных записей могут различаться. В некоторых формах не было обнаружено уязвимости, в то время как другие позволяли злоумышленнику получить доступ к учетной записи. По мнению эксперта, к 39 тыс. из всех аккаунтов можно было получить доступ, изменив соответствующий учетной записи номер телефона пользователя. Помимо этого, хакер потенциально мог поменять адрес электронной почты 1700 пользователей.

По словам А. Свиннена, злоумышленник мог получить доступ к личной информации пользователя (номеру телефона), а также легко изменить номер телефона в учетной записи Instagram. После ввода нового номера хакер мог воспользоваться функцией изменения пароля через SMS и получить полный доступ к аккаунту.

Владелец Instagram компания Facebook исправила уязвимость в течение нескольких дней после ее обнаружения.

***

23.05.2016

Вымогательское ПО теперь не только шифрует файлы, но и используется для DDoS-атак

Исследователь компании Invincea сообщает, что злоумышленники, похоже, догадались использовать зараженные шифровальщиками устройства для осуществления DDoS-атак. Так, новая версия вредоноса из семейства

Cerber демонстрирует подозрительную активность, похожую на UDP флуд, пишет InternetUA.

И. Дайк из Invincea пишет, что новая вариация Cerber, похоже, создавалась как многофункциональное решение, а не просто как еще один шифровальщик. После заражения устройства малварь вносит в систему изменения, позволяющие ей подменить пользовательский скринсейвер перманентным сообщением с требованием выкупа.

Но тогда как это достаточно стандартное поведение для вымогательского ПО, Cerber также продемонстрировал странную сетевую активность, массово обращаясь к большому пулу адресов, начиная с 85.93.0.0 и заканчивая 85.93.63.255.

Исследователь пишет, что код вредоноса прошел обфускацию, а некоторые куски, похоже, вообще были добавлены в код нарочно, чтобы сбить с толку аналитиков. Все это серьезно осложняет изучение вымогателя.

И. Дайк обнаружил, что вредонос способен создавать текстовые файлы, экспортировать их как файлы .vbs и затем выполнять. После того как скрипт был создан и запущен, появляется файл 3311.tmp, который, судя по всему, и является непосредственно шифровальщиком Cerber.

Кроме того, как уже было сказано выше, малварь подменяет скринсейвер сообщением о выкупе и обращается к подсети 255.255.192.0 (85.93.0.0 – 85.93.63.255). Вредонос создает шестнадцатеричный .tmp-файл, который постоянно запускает процесс explorer.exe. Процесс тоже создает ряд файлов .tmp и записывает их на диск. Судя по всему, эта повторяющаяся цепочка действий является дочерним процессом все того же 3311.tmp. Исследователь отмечает, что файл dnscacheugc.exe на скриншоте ниже имеет тот же хеш, что и 3311.tmp, отличается только имя. И. Дайк полагает, что эта цепочка действий привязана к оригинальному лупу в VBscript.

«Наблюдаемый сетевой трафик выглядит как направленный на подсеть флуд UDP-пакетами через порт 6892. Используя спуфинг целевого адреса, хост может направить весь ответный трафик от подсети на жертву, в результате чего та перестанет отвечать», – пишет И. Дайк.

По мнению исследователя, рассматриваемый образец малвари, возможно, не полностью завершил процесс доставки пейлоада в систему, а это означает, что вредонос может быть способен и на другую опасную активность.

***

24.05.2016

Утекшие данные LinkedIn использовались для взлома аккаунтов соучредителя Twitter и автора Minecraft

Участники хакерской группировки OurMine Team заявили о взломе ряда учетных записей известных персон, в том числе соучредителя соцсети Twitter Б. Стоуна, разработчика популярной игры Minecraft М. Перссона и актера

С. Хартмана. Единственным связующим звеном между всеми жертвами является наличие учетной записи в LinkedIn, пишет InternetUA.

Как отмечают журналисты издания Vice Motherboard, в настоящее время неясно, каким образом хакеры получили доступ к учетным записям, однако некоторые косвенные улики свидетельствуют о возможном использовании утекших в 2012 г. паролей LinkedIn, которые сейчас продаются на одном из подпольных форумов.

По словам представителя Б. Стоуна, учетная запись предпринимателя в Twitter не была взломана, скорее, речь идет о другом связанном с Twitter сервисе. Хакеры опубликовали от имени Б. Стоуна сообщение, сопровождавшееся короткой ссылкой, характерной для LinkedIn, что позволяет предполагать взлом именно учетной записи в LinkedIn.

В случаях с М. Перссоном и С. Хартманом хакеры скомпрометировали учетные записи сразу в нескольких сервисах. Как полагают журналисты Vice Motherboard, для этих целей они использовали один и тот же пароль от аккаунтов в LinkedIn.

Участники OurMine Team отрицают использование скомпрометированных данных LinkedIn для взлома учетных записей. По их словам, доступ к сервисам осуществлялся при помощи эксплоитов для уязвимостей нулевого дня, однако подробности атак хакеры не раскрывают. Свои действия группировка OurMine Team мотивирует желанием привлечь внимание общественности к проблемам безопасности.

«Мы возвращаем им [жертвам. – Прим. ред.] учетные записи. Мы просто учим их, как защитить свои аккаунты, а затем отправляем новые, более надежные пароли», – отметил один из участников группировки.

***

3.06.2016

Мошенники используют утечки данных пользователей LinkedIn и MySpace для шантажа

Федеральное бюро расследований США опубликовало предупреждение о мошенниках, пытающихся нажиться на недавно обнаруженных крупных утечках данных пользователей LinkedIn, MySpace и Tumblr. За последнее время Центр приема жалоб на интернет-преступления ФБР (Internet Crime Complaint Center, IC3) получил большое количество сообщений о вымогательстве, пишет InternetUA.

Злоумышленники рассылают жертвам письма с заявлением о том, что у них есть доступ к их электронной почте и учетным записям в соцсетях, и угрожают опубликовать компрометирующую информацию, если в короткий срок не получат определенную сумму в виртуальной валюте. Как правило, размер выкупа составляет от 250 до 1200 долл.

«У нас есть для вас две новости – плохая и хорошая. Начнем с плохой. Мы подготовили к отправке на следующие адреса электронное письмо, в

котором расписана вся ваша деятельность в Интернете, в том числе информация из соцсетей, данные об авторизации и действиях с кредитной картой. Теперь хорошая новость. Вы можете предотвратить отправку письма, если перечислите 2 биткойна на следующий кошелек», – говорится в сообщении.

В других письмах злоумышленники запугивают жертв возможным бракоразводным процессом и в случае отказа платить обещают отправить компрометирующую информацию членам семьи и друзьям.

***

24.05.2016

Хакеры используют SQL-инъекции для взлома сайтов на базе Drupal

В марте нынешнего года появились первые жертвы новой разновидности вымогательского ПО. Администраторы сайтов на базе Drupal сообщали о блокировке страниц и требовании оплаты. Как информирует Softpedia со ссылкой на эксперта по безопасности Forkbombus Labs С. Гордона, первые инфицирования веб-сайтов начались 11 марта и стали интенсивнее после 18 марта, пишет «Центр информационной безопасности».

Сперва злоумышленник сканирует веб-сайт на наличие файла CHANGELOG.txt. Сканирующий бот преступника эксплуатирует уязвимость CVE-2014-3704 для взлома сайта и изменения пароля администратора. Уязвимость CVE-2014-3704 позволяет осуществить SQL-инъекцию и затрагивает вышедшие до Drupal 7.32 версии.

Как только хакер получает контроль над сайтом, создается новая страница, содержащая форму с полем для загрузки файлов. Затем бот использует эту форму для загрузки различных скриптов, извлекающих электронные письма из базы данных Drupal, и делает их доступными в виде загружаемых файлов в /sites/default/files/. Соответственно, хакер может зайти на страницу и загрузить файлы.

Последним загруженным файлом становится бинарный код, написанный на языке программирования Go и являющийся вредоносным ПО. Вредонос удаляет форму с полем для загрузки файлов и заменяет ее сообщением: «Веб-сайт заблокирован. Пожалуйста, перечислите 1,4 биткойна на адрес 3M6SQh8Q6d2j1B4JRCe2ESRLHT4vTDbSM9, чтобы разблокировать контент». («Website is locked. Please transfer 1.4 BitCoin to address 3M6SQh8Q6d2j1B4JRCe2ESRLHT4vTDbSM9 to unlock content»). Однако вредонос не шифрует информацию. Эксперт также предположил возможное существование целой инфраструктуры C&C-сервера у злоумышленников.

Вымогателем было инфицировано около 400 веб-сайтов. На указанный биткойн-кошелек преступников не было осуществлено никаких транзакций, то есть преступникам еще никто не платил. Также исследователь безопасности заметил, что зараженные вымогателем сайты производили впечатление

заброшенных создателями, поэтому преступники не нанесли никакого существенного ущерба.

***

25.05.2016

Украинские хакеры взломали сайты властей РФ

Хакеры из украинской группы «Рух8» заблокировали официальные сайты Оренбургской области России. Об этом сообщается на сайте группы. Взломщики опубликовали на сайтах жалобы людей, пишет InternetUA.

В своем пресс-релизе они сообщили, что заблокировать ресурсы удалось 20 мая этого года. До момента написания новости официальные сайты региональной власти не работают.

Группа «Рух8» сначала разместила сообщение о том, что в области усиливаются меры безопасности из-за протестов в Казахстане, но позже сообщение было удалено. Однако участники группы направили домены, в том числе главы региона, на свой сайт.

Российским специалистам не удается разблокировать работу.

Кроме того, в сеть попали тысячи обращений жителей области. В них они просят власть помочь уничтожить вредителей, расплатиться с кредитами, разобраться с главой поселка, предоставить давно обещанное жилье участнику войны на Северном Кавказе и т. п.

***

25.05.2016

Хакеры взломали 2,5 тыс. учетных записей в Twitter и распространяют ссылки на порно-сайты

Исследователи компании Symantec предупредили о более 2,5 тыс. взломанных учетных записях в Twitter, распространяющих ссылки на порно-сайты и ресурсы для знакомств. Злоумышленники меняют названия скомпрометированных учетных записей, фотографии профиля и биографию пользователей и вместо них публикуют материалы, рекламирующие вышеупомянутые сайты, пишет InternetUA.

В ходе расследования инцидента эксперты Symantec обнаружили несколько скомпрометированных аккаунтов, принадлежащих известным личностям. К примеру, жертвами хакеров стали популярная канадская группа Chromeo и журналисты издания The Telegraph и New York Times.

Очевидно, в этой кампании главным для злоумышленников является привлечение внимания пользователей. Вместо рассылки личных сообщений и твитов они используют скомпрометированные учетные записи для того, чтобы подписываться на страницы и ставить отметки «Мне нравится» под твитами в надежде заинтересовать пользователя.

На скомпрометированных страницах предлагается бесплатно зарегистрироваться на сайтах, позволяющих общаться в видеочате с различными целями. Каждый твит сопровождается фотографией соответствующего содержания и короткими ссылками. По данным исследователей, за каждого зарегистрировавшегося на таком ресурсе пользователя хакеры получают 4 долл.

***

25.05.2016

Эксперты сообщили об увеличении числа атак на iOS

Эксперты компании Check Point обнаружили в прошлом месяце 2000 уникальных семейств вредоносного ПО, что на 50 % больше, чем в месяцем ранее. По их данным, атаки на устройства под управлением iOS впервые попали в топ-3 самых распространенных видов вредоносного мобильного ПО, пишет InternetUA.

Исследования выявили широкий спектр угроз, с которыми сталкиваются пользователи и масштаб проблем, о которых должны думать специалисты в области безопасности для предотвращения атак на критическую информацию.

Исследователи обнаружили XcodeGhost, скомпрометированную версию платформы разработки iOS Xcode. Она по-прежнему представляет неизбежную угрозу для корпоративных мобильных устройств, несмотря на удаление из App Store в сентябре 2015 г. Атаки, направленные на устройства iOS, вошли в топ-3 самых распространенных видов вредоносного мобильного ПО.

Вредоносная программа для Android HummingBad остается в топ-10 атак на платформы по всему миру. Несмотря на то, что исследователи Check Point обнаружили ее только в феврале, она стремительно набирает обороты. Это подтверждает интерес хакеров к Android-устройствам как к слабому звену корпоративной безопасности и очень прибыльной цели.

В апреле самым распространенным видом вредоносного ПО вновь стал червь Conficker, использованный в 17 % всех зарегистрированных атак. Вирус Sality отмечен в 12 % нападений, а червь Zeroaccess – в 6 %. Более половины всех атак были совершены с помощью программ из топ-10 вредоносного ПО.

– Conficker – Червь, обеспечивающий удаленное исполнение операций и загрузку вредоносного ПО. Инфицированный компьютер управляется ботом, который обращается за получением инструкций к своему командному серверу.

– Sality – Вирус, позволяющий своему оператору осуществлять удаленные действия и загрузки других вредоносных программ в зараженные системы. Главная цель Sality – как можно дольше оставаться в системе, предоставляя возможности удаленного контроля и установки других видов вредоносного ПО.

– Zeroaccess – Червь, атакующий Windows-платформы, обеспечивает удаленные операции и загрузки вредоносных программ. Использует протокол

«точка-точка» (P2P) для загрузки или обновления дополнительных вредоносных компонентов с удаленных точек.

По данным экспертов, количество атак на Россию растет второй месяц подряд: по сравнению с мартом 2016 г. она поднялась с 38 на 26 место. Кроме Conficker и Sality в топ-10 по России также вошли Kometaur, Delf, Angler ek, Blackenergy, Inject, Dorkbot, Ldpinch и FULLSTUFF.

В Топ-3 семейств мобильного вредоносного в апреле вошел XcodeGhost – компрометированная версия платформы разработчиков Xcode для Mac. Эта неофициальная версия программы для разработки Xcode изменена так, что она может внедрять вредоносный код в приложение, которое разработано и скомпелировано с ее помощью. Внедренный код отправляет информацию о приложении на командный сервер, позволяя инфицированному приложению считывать данные из буфера обмена устройства.

***

26.05.2016

Троянец-бэкдор использует TeamViewer по-новому

Специалистам в области информационной безопасности известно несколько разновидностей вредоносных программ, использующих для получения несанкционированного доступа к зараженному компьютеру популярную утилиту удаленного администрирования TeamViewer, пишет Tnews.

Новый троянец BackDoor.TeamViewer.49, обнаруженный вирусными аналитиками компании «Доктор Веб» в мае 2016 г., является исключением из этого правила, поскольку эксплуатирует данную программу с совсем иными целями.

Для распространения троянца BackDoor.TeamViewer.49 киберпреступники используют другую вредоносную программу – Trojan.MulDrop6.39120, которая реализована в виде поддельного обновления Adobe Flash Player. Исполняемый файл Trojan.MulDrop6.39120 действительно устанавливает плеер на работающий под управлением Windows компьютер, но при этом втайне от пользователя сохраняет на диск приложение TeamViewer, троянца BackDoor.TeamViewer.49 и необходимый для его работы конфигурационный файл. В процессе установки на экране демонстрируется окно настоящего инсталлятора Flash Player.

Обычно различные троянцы используют TeamViewer с целью организации несанкционированного доступа к зараженному компьютеру. Однако бэкдору BackDoor.TeamViewer.49 утилита TeamViewer нужна совсем по другой причине: он активно использует в своей работе различные внутренние функции процесса этой программы. Кроме того, при своем запуске TeamViewer автоматически помещает в память компьютера библиотеку avicap32.dll, чем и воспользовались злоумышленники: они поместили в папку, в которую Trojan.MulDrop6.39120 сохраняет это приложение, троянскую

библиотеку с таким же именем. В момент запуска TeamViewer автоматически загружает ее в память.

После запуска программы TeamViewer BackDoor.TeamViewer.49 удаляет ее значок из области уведомлений Windows и отключает в системе функцию показа сообщений об ошибках. Также троянец использует специальный механизм, призванный исключить его повторный запуск на зараженном компьютере. Необходимые для работы BackDoor.TeamViewer.49 параметры хранятся в зашифрованном конфигурационном файле.

BackDoor.TeamViewer.49 регистрирует себя в автозагрузке, а затем в непрерывном цикле, но с определенными интервалами, устанавливает атрибуты «системный» и «скрытый» для своей папки, где хранятся сам исполняемый файл, вредоносная библиотека и файл конфигурации. Если в какой-то момент времени установить эти атрибуты не удалось, вредоносная программа приступает к процедуре удаления из системного реестра всех ключей, относящихся к программе TeamViewer.

В теле троянца хранится еще одна зашифрованная библиотека, реализующая вредоносные функции BackDoor.TeamViewer.49. В ней содержится специальным образом сформированный массив с именами управляющих серверов, от которых троянец может получать различные команды. Вся информация, которой бэкдор обменивается с управляющим сервером, шифруется.

Троянец способен выполнять несколько управляющих директив, однако две основные из них – это команды на установку соединения с указанным удаленным узлом (включая возможность авторизации на нем) и на перенаправление трафика от управляющего сервера на заданный удаленный узел через инфицированный компьютер. Это позволяет злоумышленникам обеспечить собственную анонимность в Интернете, соединяясь с удаленными узлами через зараженный компьютер как через обычный прокси-сервер.

Вредоносные программы Trojan.MulDrop6.39120 и BackDoor.TeamViewer.49 распознаются и удаляются Антивирусом Dr.Web, поэтому не представляют опасности для наших пользователей.

***

27.05.2016

Разработан новый метод атаки на буфер обмена с использованием JavaScript

Метод манипуляции с содержимым буфера обмена пользователя при помощи HTML/CSS уже давно не нов. Он предполагает копирование жертвой с сайта вредоносной команды, вставляемой затем в буфер обмена. Независимый исследователь Д. Эйри предложил похожий, но более опасный метод атаки с использованием JavaScript вместо HTML/CSS, пишет InternetUA.

Эксперт назвал новую технику Pastejacking и уже опубликовал на GitHub демонстрационный пример атаки. По его словам, отличие метода заключается в

том, что текст может быть скопирован непосредственно после нажатия нажатия CTRL + C или спустя короткое время. При этом браузер не запрашивает у пользователя подтверждения операции по изменению содержимого буфера обмена.

Метод также предоставляет более простой способ подстановки в буфер обмена шестнадцатеричных символов, которые могут применяться для эксплуатации VIM. Как отмечается, для успешной атаки пользователю не требуется копировать с сайта весь вредоносный текст, достаточно нескольких символов.

Д. Эйри привел пример атаки, продемонстрировав, как злоумышленник может удаленно запустить вредоносный код на целевом устройстве, очистить консоль, а затем незаметно для пользователя добавить скопированный код. Исследователь предлагает скопировать в буфер обмена строку

echo “not evil”

На терминале она будет подменена на строку

echo «evil»\n

Для сокрытия вредоносной активности подойдет следующее решение

touch ~/.evil

clear

echo «not evil»

Данная команда создаст вредоносный файл в домашней директории и приведет к очистке терминала.

***

26.05.2016

Tor следующего поколения получит генератор равномерно распределенных случайных чисел

Эксперты организации Tor Project разработали новый способ генерации случайных чисел, с помощью которого удастся усилить безопасность пользователей ПО Tor, пишет InternetUA.

Генераторы случайных чисел являются ключевыми компонентами любого защищенного приложения и играют главную роль в создании ключей шифрования. Последовательности генерируемых символов должны быть случайными и непредсказуемыми. Если злоумышленник может предугадать числа, используемые при создании ключа шифрования, то он также способен определить диапазон возможных ключей и скомпрометировать весь процесс шифрования.

Разработчики Tor в течение нескольких месяцев работают над созданием генератора равномерно распределенных случайных чисел и уже добились больших успехов. Как сообщается в блоге организации, специалисты Tor Project собрались в Монреале (Канада) и целую неделю не покладая рук трудились над разработкой onion-сервисов следующего поколения.

«Мы начали разрабатывать систему генерации равномерно распределенных случайных чисел для сети Tor. Генератор равномерно распределенных случайных чисел представляет собой систему из нескольких компьютеров, совместно генерирующих одно случайное число, используя способ, который никто (даже сами компьютеры) не может предугадать заранее. [..] Разработчики закончили реализацию протокола несколько месяцев назад и с тех пор проводят аудит и тестирования кода», – сообщается в блоге организации.

Участники проекта уже тестировали свой генератор случайных чисел с помощью модели сети Tor, состоящей из расположенных по всему миру 11 узлов. Каждый разработчик настраивал узел Tor и активировал функцию генерирования равномерно распределенных случайных чисел. В течение недели узлы генерировали случайные числа, что позволило исследователем исправить уязвимости.

***

26.05.2016

5 ежедневных ошибок, которые делают вас уязвимыми в Интернете

Вы можете этого не осознавать, но многие простые вещи, которые вы ежедневно делаете в Интернете, могут ставить под угрозу вас и ваш компьютер. Вот несколько элементарных ошибок, которые делают вас уязвимыми, пишет IGate.

Использование публичного Wi-Fi

Так или иначе, все мы пользуемся общественным Wi-Fi. Но безопаснее от этого он не становится. Использование публичных Wi-Fi-точек, особенно в многолюдных местах, вроде кафе или аэропортов, может открыть Вас и Ваш компьютер для множества атак.

Общественный Wi-Fi чреват проблемами безопасности. Сети с простыми названиями, вроде Free Wi-Fi, могут быть созданы или подделаны для перехвата подключения. Безопасность общественных Wi-Fi-точек вообще довольно низкая, ведь даже если это легальная точка, ее все равно намного проще взломать, чем частный Wi-Fi.

Иными словами, когда вы думаете, что подключаетесь к Free WiFi вашего отеля, то на самом деле можете подключаться к поддельной сети, установленной для перехвата логина, пароля и других ваших данных при подключении. Потому, в случае, если вам все же приходится пользоваться общественным Wi-Fi, используйте VPN (виртуальную частную сеть). Это зашифрует ваши данные и обеспечит их безопасную передачу даже через публичную точку доступа.

Заполнение онлайн-форм

Помимо осторожного использования общественных точек доступа, необходимо не менее осторожно следить за тем, кому вы предоставляете свои

личные данные. Ведь никакая техническая защита не поможет вам сохранить информацию, если Вы раздаете ее собственноручно.

Следует понимать, что многие сайты собирают информацию о вашей онлайн-деятельности. Прежде чем сообщать ресурсу свой е-мейл, физический адрес или номер телефона, узнайте, что сайт планирует со всем этим делать. Как правило, эта информация оговорена соглашением о конфиденциальности.

Очень осторожно используйте функцию, позволяющую авторизоваться на ресурсе с помощью аккаунта в социальных сетях. Авторизоваться всюду при помощи всего одной кнопки – это, конечно, удобно. Но также можно по неосторожности предоставить сайту слишком много прав доступа к своей странице.

Использование одинаковых паролей

Довольно трудно запоминать сложные пароли, но оно того стоит. Ни в коем случае нельзя использовать один и тот же пароль на таких сервисах, как электронная почта и банкинг.

Помните, что никто не застрахован от утечек данных. Даже если ваш пароль сложен, его могут украсть, похитив базу данных сайта. Если этот пароль вы использовали на нескольких ресурсах, все ваши аккаунты будут скомпрометированы. Наличие уникальных паролей гарантирует, что злоумышленники, похитившие один из них, не получат остальных.

Придумать множество уникальных паролей довольно сложно, потому Вы можете пользоваться специальными программами-генераторами. Также Вы можете воспользоваться нашим советом и придумать сложный мастер-пароль, а затем модифицировать его для разных ресурсов.

Размещение фото в социальных сетях

О том, что процесс размещения фото в соцсетях может быть небезопасным, не задумывается практически никто. Люди в огромном количестве делятся фотографиями своих питомцев, своих покупок, даже своей еды. При этом они не проверяют, включена ли функция геотегирования, рассказывающая всем желающим, где была сделана та или иная фотография.

Конечно, не беда, если фотография салата, сделанная в местном кафе, попадет в соцсеть. Гораздо хуже, если фото сделано у вас дома. Разместив его в соцсети, Вы выдадите всему миру точные координаты своего жилища.

Решить проблему просто – раз и навсегда отключите шпионскую функцию геотеггинга. Если захотите сообщить миру, где было сделано то или иное фото, напишите об этом вручную.

Слепое принятие соглашения о конфиденциальности

Принятие политики конфиденциальности – важное условие пользования ресурсом, предоставляющим много услуг. Конечно, такие соглашения длинные. Но ознакомление с ними – необходимое зло. Пользователь должен (!) прочесть каждый пункт политики конфиденциальности, прежде чем принимать ее. Это позволит ему точно понимать, как именно компания намерена распоряжаться его личными данными.

Соглашаясь с этой политикой вслепую, пользователь не знает своих прав, а потому никак не защищен от возможных злоупотреблений.

***

1.06.2016

Эксперты доказали, что приложение Facebook постоянно прослушивает разговоры пользователей смартфонов

Американский профессор нашла доказательства того, что мобильное приложение Facebook постоянно прослушивает пользователей смартфонов, пишет InternetUA.

Разработчики самой популярной в мире социальной сети внедрили в официальный клиент возможность постоянного прослушивания пользователей. Эта функция появилась у приложения для мобильных устройств в 2014 г., пишет BFM.

По словам профессора университета Южной Флориды К. Бернс, решившей подробнее изучить новые функции Facebook, приложение использует эти возможности не только в заявленных целях оказания помощи пользователям, но и для прослушивания их разговоров с последующим предложением им определенных услуг.

Для проверки своего предположения К. Бернс специально обсуждала с собеседниками строго определенные темы при выключенном доступе к социальной сети, а затем обнаружила, что на открываемых ею на этом устройстве интернет-сайтах демонстрировались рекламные объявления, связанные с затронутыми в разговорах вопросами.

На запрос журналистов представитель Facebook официально заявил, что компания «не использует аудиовозможности встроенных в телефоны микрофонов для сбора и передачи информации рекламодателям или новостным агентствам в той или иной форме».

При запуске новой функции два года назад руководители Facebook утверждали, что телефоны с установленным приложением вовсе не всегда слушают пользователей и что компания не хранит аудиозаписи.

В официальных документах Facebook, опубликованных на сайте компании, также утверждается, что она не записывает разговоры клиентов, но использует звуковую информацию «для идентификации происходящего вокруг устройства». Используется такая возможность якобы только для того, чтобы определить, что именно пользователь слушает или смотрит, «чтобы облегчить ему возможность размещения соответствующих постов» в социальной сети.

Как пишет британская газета, нежелательную функцию телефонов, на которой установлено данное приложение, можно отключить с помощью программных средств при настройке операционной системы. Эта возможность предусмотрена для смартфонов, работающих как на операционной системе iOS, так и на Android.

***

31.05.2016

Пароли от 65 млн Tumblr-аккаунтов выставили на продажу

Хакеры выставили на продажу базу данных, состоящую из 65 млн учетных записей пользователей блог-платформы Tumblr. Цена предложения составляет 150 долл., сообщает Motherboard, пишет InternetUA.

Пароли и электронные адреса были получены злоумышленниками еще в 2013 г.

Администрация Tumblr ранее заявила, что воспользоваться ими нельзя. Несмотря на то что сведения не были зашифрованы, пароли содержат случайные байты, добавленные перед их хешированием.

Хакер Peace утверждает, что компания использовала SHA1. Также была задействована так называемая соль – строка данных, которая передает хеш-функции вместе с паролем. При таких условиях подобрать оригинальный набор символов взломщикам затруднительно. По этой причине злоумышленники выставили столь низкую цену на всю базу данных.

Исследователь компьютерной безопасности Т. Хант добавил базу данных Tumblr на ресурс Have I been pwned, с помощью которого пользователи могут проверить, были ли взломаны их аккаунты.

***

31.05.2016

Уязвимость WordPress ставит под угрозу множество интернет-сайтов

В Интернете появились данные о том, что все владельцы сайтов, где используется система WordPress, обязаны обновить плагин JetPack. Такая срочность связана с потенциальным вирусом, который может угрожать стабильной работе ресурсов, пишет InternetUA.

Плагин на сегодняшний день является довольно популярным среди пользователей Интернета. С его помощью можно совершено бесплатно оптимизировать разные веб-сайты и обеспечить их безопасность. У плагина уже имеется более одного миллиона установок, что только говорит о его большой популярности среди юзеров.

Сообщается, что вышеупомянутая уязвимость была найдена аналитиками одной из структур безопасности. По их мнению, уязвимость есть во всех эпизодах приложения, которые выходили с 2012 г.

***

31.05.2016

Новый вирус шифровальщик может заразить компьютер ваших друзей

Текущий год продолжает неприятно радовать появлением новых крайне опасных вирусов. Так, в конце мая специалисты по кибербезопасности обнаружили новый троян-шифровальщик Crypren, который имеет необычную функцию – самораспространение, пишет InternetUA.

Троян скопирует себя на все подключенные переносные устройства, в том числе карты памяти и флешки, которые становятся переносчиком Crypren и опасны для других ПК при подключении к ним. Поэтому не стоит передавать друзьям или знакомым устройства хранения информации, которые использовались на зараженном ПК.

Пути заражения

Заражение вирусом происходит через почту, или при загрузке поддельных установочных файлов известных программ, например Flash Player.

Почтовый путь чаще всего использует текстовые документы MS Word , при открытии которых ПК пользователя подвергается заражению вредоносным ПО. Заражение через установочные файлы также происходит при запуске инсталятора с «вшитым» трояном.

В результате, Crypren зашифровывает все найденные на ПК файлы. Возможности трояна стремительно растут. Так, еще два недели назад он шифровал порядка 80 видов файлов. На сегодня – более 120, включая zip, xlsx, jpeg, mpeg и другие. На экран зараженного ПК выводится блокирующая работу картинка с требованиями выкупа.

Злоумышленники требуют за расшифровку данных порядка 500 долл. США, однако в биткоинах (1,2Bt). Если же пользователь подождет несколько дней цена вырастет до 5 биткоинов (2,2 тыс. дол США).

***

31.05.2016

В Украине хакеры начали массовые атаки на Госреестр недвижимости

В Украине хакеры начали массово взламывать компьютеры нотариусов, чтобы получить доступ к Госреестру недвижимости, пишет InternetUA.

Уже «заражена» почти тысяча компьютеров нотариусов, госисполнителей и других уполномоченных лиц, рассказал начальник лаборатории компьютерной криминалистики CyberLab С. Прокопенко (эксперты компании участвуют в расследовании подобных дел).

Первые инциденты, зафиксированные лабораторией, датируются еще ноябрем-декабрем 2014 г. Во всех случаях была использована одинаковая схема, когда с помощью рассылки на электронные адреса нотариусов писем с вредными функциями, злоумышленник получал доступ к Госреестру и вносил изменения от имени нотариуса.

«Зачастую взлом происходит в нерабочее время, например, ночью, когда на рабочем месте никого нет и оперативно выявить изменения сложно. В основном мошенники нацеливаются на владельцев крупных компаний,

предприятий и пр. Но также есть случаи атак и на физлиц, которым принадлежит дорогая недвижимость, в частности, квартиры», – рассказал старший партнер юркомпании «Кравец и Партнеры» Р. Кравец.

В свою очередь в Минюсте утверждают: с их стороны все защищено и никаких взломов они не фиксировали. И обвиняют во всем нечестных на руки нотариусов. «Реестр ни разу не был взломан. Он проходил стресс-тесты независимых компаний, и те подтвердили его защищенность. Периодически заявления о взломе делают недобросовестные регистраторы или нотариусы, которые или самостоятельно внесли в реестр неправдивую информацию и этим нарушили закон, или отдали свой ключ помощникам, что тоже недопустимо. А теперь они пытаются оправдать свои действия техническим сбоем», – считает первый заместитель министра юстиции Н. Севостьянова.

При этом сами нотариусы, хотя и не исключают недобросовестности некоторых своих коллег, утверждают: случаи атак настолько массовые, что без хакеров здесь явно не обошлось. «Речь идет о десятках случаев взломов в месяц, а несанкционированных нотариальных действий – так и вовсе сотни», – рассказали в одном из отделений Нотариальной палаты Украины. При этом на хакерских форумах услуги по «решению вопросов», связанных с нотариусами, предлагают по цене от 300 долл.

***

30.05.2016

18 % популярных сайтов не установили последнее исправление OpenSSL

В начале мая вышло исправление безопасности популярной библиотеки OpenSSL, используемой для шифрования трафика. В версиях 1.0.1t и 1.0.2h был исправлен ряд уязвимостей, в том числе ошибки, связанные с работой буфера и обработкой различных алгоритмов шифрования. Разработчик оценил критичность этого исправления как высокую, пишет InternetUA.

Наличие исправленной версии OpenSSL можно удаленно проверить с помощью эксплоита к уязвимости CVE-2016-2107 (также известна как атака padding-oracle).

Согласно опубликованным результатам исследования самых популярных сайтов по рейтингу Alexa Top 10 000, проведенного компанией High-Tech Bridge, чуть более 18 % сайтов не установили последнюю версию OpenSSL.

Исследование проводилось с использованием инструмента проверки безопасности SSL/TLS, разработанного компанией. Исследователи осуществили проверку не только веб-сайтов, но и почтовых серверов, использующих OpenSSL. По результатам, 6258 хостов (62,58 %) успели установить исправление безопасности, 1829 (18,29 %) систем оказались уязвимы, а на 1913 (19,13 %) серверов эта уязвимость не распространяется.

***

2.06.2016

Facebook добавит в мессенджер надёжное шифрование

По данным The Guardian, в скором времени в Facebook Messenger будет добавлено двухстороннее шифрование переписки. Оно обезопасит пользователей этого приложения от хакерского перехвата сообщений методом «человек посередине». Кроме того, зашифрованную таким способом переписку будет невозможно расшифровать, даже получив удалённый или физический доступ к серверам мессенджера, пишет InternetUA.

Ранее подобное шифрование переписки появилось в Telegram (только в приватных чатах), WhatsApp, Viber и некоторых других, менее популярных мессенджерах.

Издание пишет, что шифрация сообщений в Facebook Messenger будет реализована по-особому – в ней задействован искусственный интеллект. Приложение сможет шифровать даже данные, которые будут передавать боты, и с этим сопряжена наибольшая сложность, ведь общение с виртуальным ассистентом M корректируют сотрудники Facebook, соответственно, они будут иметь доступ к некоторой части незашифрованной переписки.

***

1.06.2016

Правообладатели потребовали от «ВКонтакте» удаления 10 групп с миллионами пользователей

Правообладатели требуют от социальной сети «ВКонтакте» удаления порядка 10 групп, которые специализируются на видеоконтенте. Каждая группа насчитывает более одного миллиона подписчиков, сообщают «Известия» со ссылкой на правообладателей и представителей отраслевой ассоциации. По данным издания, это первое требование по удалению такого количества видеогрупп, пишет InternetUA.

«Правообладатели, имеющие права на видео, фильмы, при участии ассоциации выбрали в соцсети 10 самых популярных групп, специализирующихся на распространении видео», – рассказал глава ассоциации «Интернет-видео» А. Бырдин. По его словам, у каждой группы количество подписчиков более 1 млн человек, а у самой большой – порядка 7 млн.

Гендиректор компании-правообладателя WebKontrol О. Валигурская подтвердила изданию, что они потребовали удалить несколько популярных групп «ВКонтакте» с видео, где постоянно находят контент, нарушающий права авторов.

«Мы неоднократно обращались в сами группы с требованием удалить контент, но жалобы не были удовлетворены, контент продолжал оставаться активным», – пояснила О. Валигурская.

В пресс-службе социальной сети заявили, что удаление сообществ считают чрезмерной мерой.

«В большинстве случаев в блокировке самих сообществ, специализирующихся на видеоконтенте, отказываем… Вместо этого мы удаляем конкретные ролики, которые нарушают права конкретного правообладателя при условии, что этот правообладатель предоставил все необходимые документы. А администраторам подобных сообществ отправляем уведомления о недопустимости размещения нелегального контента», – приводит сообщение пресс-службы.

***

1.06.2016

Трояны для Android приспособились к новому способу получения прав

Разработчики вредоносных приложений постепенно адаптируются к особенностям новой системы управления правами доступа к системным сервисам и персональной информации, которая встроена в Android 6.0 Marshmallow. Её поддержка появилась в двух известных троянах для мобильной платформы Google, пишет InternetUA.

Android давно критикуют за неэффективную систему управления правами. Из-за неё пользователи ещё в магазине узнавали о том, какие права нужны приложению, и должны был одобрить весь список сразу. Вероятно, в Google рассчитывали, что люди будут внимательно изучать требования приложений, но желающих вникать в длинные и непонятные списки оказалось мало. Подавляющее большинство пользователей одобряет любые требования, не глядя.

В Android 6.0 Marshmallow управление правами доступа переделали по образу и подобию iOS. Теперь после установки приложение получает лишь права, относящиеся к нормальному уровню доступа. Когда оно пытается сделать что-то, требующее другого уровня доступа (например, получить геолокационную информацию или забраться в список контактов), система спрашивает у пользователя разрешение и запоминает ответ. Предполагается, что так приложениям будет труднее незаметно от пользователя получить чересчур широкие права доступа.

Для разработчиков, желающих использовать старый подход, оставили лазейку. Если значение атрибута target_sdk меньше 23, все требования, как и в старых версиях системы, придётся одобрять списком во время установки, а не по одному, как в Marshmallow. Впрочем, даже в том случае, если все разрешения выданы в момент установки, новый Android позволяет в любой момент отобрать их. На первых порах пользователей, которые умеют и желают отключать права доступа, почти не было, но теперь их стало больше. Это начинает мешать нормальной работе вредоносных приложений, поэтому их разработчики вынуждены реагировать.

Специалисты компании Symantec обратили внимание, что новые версии вредоносных программ, основанных на Android.Bankosy и Android.Cepsohord, в той или иной степени учитывают особенности Marshmallow. Банковский троян Android.Bankosy стал использовать программный интерфейс checkSelfPermission, чтобы узнать, есть ли у него права, которые нужны для запуска вредоносного кода. Android.Cepsohord не только проверяет наличие прав, но и запрашивает новые разрешения, если их не хватает.

Чтобы избежать проблем с вредоносным софтом для Android, Symantec рекомендует не скачивать приложения из сомнительных мест и внимательно следить за разрешениями, которые они спрашивают. Кроме того, лучше быть готовым к худшему и периодически делать резервные копии всей ценной информации.

***

1.06.2016

Тестирование антивирусов на Windows 10 для предприятий за март – апрель 2016

Показав пользователям личных устройств под управлением системы Windows 10, какие антивирусы надёжные и удобные, а какие нет, AV-TEST не забывает об организациях, где вопрос защищённости является ещё более важным. И здесь единственным лидером также стала компания Bitdefender, антивирус который был признан идеальным по всем направлениям, пишет InternetUA.

Bitdefender набирает по 6 баллов за уровень защиты, минимальное влияние на скорость работы системы и удобство использования. Продукт лаборатории Касперского занимает второе место, не досчитавшись половины балла за скорость, а Symantec столько же не получил за удобство. Далее располагается AVG с общим результатом в 16,5 баллов.

Антивирус от Microsoft занимает второе место с конца, набрав 3 из 6 возможных баллов за уровень защиты и получив 14 баллов из 18 в целом. Единственным другим получившим за защиту только 3 балла антивирусом является занимающий последнее место Seqrite. По этой причине большинство пользователей отдают предпочтение сторонним антивирусом, а Защитник Windows автоматически активируется при их отсутствии.

***

24.05.2016

Что происходит с личными данными после хакерской атаки

Развитие и повсеместное распространение онлайн-сервисов приводит к попаданию в сеть большего количества личных данных пользователей, которые нередко становятся целью для атак хакеров, пишет InternetUA.

Для того, чтобы минимизировать угрозу, специалистам по информационной безопасности приходится изучать природу атак и их последствия под самыми разнообразными углами, информирует news.eizvestia.com.

Исследователи компании Bitglass провели интересный эксперимент, озаглавленный «Где ваши данные?» (Where's Your Data?). Специалисты создали сайт вымышленного банка, снабдили его несуществующих служащих фейковыми личностями, подключили аккаунт Google Drive и добавили ко всему этому информацию о настоящих банковских картах.

Затем аналитики Bitglass сами слили эти сфабрикованные данные в даркнет, под видом результата фишинговой атаки, и принялись ждать.

В первые же 24 часа после «взлома» специалисты зафиксировали три попытки входа в Google Drive и пять попыток логина на фальшивом банковском портале. Однако давно известно, что личные данные после утечки распространяются по сети очень быстро. Спустя 48 часов уже можно было наблюдать сотни просмотров аккаунтов и скачиваний файлов. За месяц компания зафиксировала более 1400 попыток использования фальшивых данных хакерами из 30 разных стран.

Исследователи отдельно отмечают тот факт, что хакеры пробовали использовать известный им пароль жертвы для входа в аккаунты других сервисов, где жертва якобы была зарегистрирована. Это еще раз доказывает, что использовать везде одинаковые пароли не стоит.

Вот другие интересные цифры, которые помог выявить данный эксперимент:

– 68 % трафика, сгенерированного хакерами, проходило через Tor;

– 34,85 % хакеров, не использовавших Tor, имели российские IP-адреса. Еще 15,67 % заходили с территории США, 3,5 % пришли из Китая и 2 % из Японии;

– 94 % хакеров получили доступ к Google Drive аккаунтам жертв, раскрыли информацию о других их аккаунтах и попытались получить доступ к банковскому счету;

– 36 % хакеров сумели получить доступ к личным банковским аккаунтам фальшивых жертв, использовав утекший пароль;

– 12 % хакеров, после удачного входа в аккаунт Google Drive, пытались скачать файлы, содержащие конфиденциальные данные, некоторым даже удалось взломать шифрование этих документов после скачивания.

***

1.06.2016

Исследователи продемонстрировали новый вид атак на NTP сервер

На конференции Hack In The Box исследователи продемонстрировали атаку на NTP сервер через беспроводную сеть. Ю. Чжен и Х. Шань из

компании Qihoo360 выступили с докладом, демонстрирующим успешное изменение времени на первичном NTP сервере, пишет InternetUA.

NTP является очень важным протоколом в сети Интернет, поскольку предназначен для синхронизации времени между компьютерами. Неавторизованное изменение времени на уязвимой системе может использоваться для обхода авторизации, например, с использованием устаревших учетных данных или цифровых сертификатов.

Исследователи продемонстрировали возможность изменения времени на NTP сервере, находящемся на большом расстоянии. Для осуществления атаки использовалась беспроводная сеть и дешевое оборудование.

Для успешной атаки на NTP сервер злоумышленнику необходимо осуществлять незначительные изменения времени – до 1 000 секунд за раз. Это необходимо во избежание аварийного завершения работы сервера.

Разработанное исследователями устройство передает поддельные GPS и JJY сигналы на целевой NTP сервер. Для осуществления атаки на GPS злоумышленник может находиться на расстоянии до 100 м, а при наличии усилителя – до 2 км.

Исследователи утверждают, что подобная атака может быть осуществлена против самых популярных NTP серверов, использующих GPS для синхронизации времени в Европе, Северной Америке и Китае.

***

5.06.2016

Android-троян Marcher атакует клиентов банков по всему миру

Разработчики вредоносного ПО усовершенствовали банковский Android-троян Marcher и добавили в список его жертв клиентов крупнейших банков Великобритании, пишет InternetUA.

По данным IBM X-Force, злоумышленники используют вредонос с конца 2013 г. Marcher рекламировался на русскоязычных хакерских формах и поначалу не предназначался для банков. Инфицировав устройство, поверх настоящей страницы в Google Play троян отображал поддельную с целью выманить у пользователей данные кредитных карт. В 2014 г. Marcher стал использоваться в атаках на клиентов финансовых организаций в Германии. В настоящее время в список его жертв входят банки в Германии, Франции, Польши, Турции, США, Австралии, Испании, Австрии, а с конца прошлого месяца и Великобритании.

Отображаемые Marcher поддельные страницы для каждого банка в точности повторяют настоящие. Как считают в IBM X-Force, скорее всего, их на заказ за отдельную плату разработали сами авторы трояна. Подобные страницы создаются довольно просто, поэтому их могли также разработать операторы Marcher или другие киберпреступники.

Согласно IBM X-Force, в большинстве случаев (88 %) вредонос атакует пользователей банковских программ, но также может похищать данные

кредитных карт, отображая фальшивые страницы бизнес-приложений (2 %), платежных сервисов (2 %), а также приложений авиакомпаний (1 %), торговых площадок (1 %) и пр.

Примечательно, что операторы трояна не дожидаются, пока пользователь сам откроет приложение, а обманным путем заставляют его запустить программу. Для этого они присылают жертве фишинговое смс-сообщение о том, что на ее счет якобы были перечислены деньги. Заинтригованный пользователь открывает приложение, чтобы проверить баланс, и попадает на фальшивую страницу, где вводит данные своей кредитной карты. Завладев информацией, злоумышленники проверяют ее достоверность, отправляя на сервер банка. Если данные подлинные, они перенаправляются на подконтрольный преступникам C&C-сервер.

***

5.06.2016

Банковские трояны научились обходить защиту Android 6.0

Ключевую роль в мобильных банковских троянах играет способность определять, какое приложение в настоящее время запущено на устройстве. Идентифицировав программу, вредонос отображает соответствующую ей фишинговую страницу, выманивая у жертвы данные банковской карты. С выходом Android 5.0 Lollipop и Android 6.0 Marshmallow компания Google отказалась от getRunningTasks() API, позволяющего определять открытые приложения, и банковские трояны наподобие Bankosy оказались бесполезными, пишет InternetUA.

Как сообщают эксперты Symantec, несмотря на предпринимаемые Google меры по усилению безопасности своей ОС, злоумышленники не отстают и продолжают совершенствовать вредоносное ПО. По словам исследователей, новые варианты банковских троянов Bankosy и Cepsohord используют два способа обхода механизмов защиты последних версий Android. Один из них предполагает получение от пользователя специального разрешения, однако второй не требует никаких дополнительных разрешений.

Первый способ позволяет определить запущенную задачу, используя представленный в Android 5.0 интерфейс программирования приложений UsageStatsManager. С помощью этого API вредоносное ПО получает статистические данные об открытых приложениях за последние две секунды и вычисляет самую последнюю активность.

Для использования UsageStatsManager вредонос запрашивает у пользователя доступ на системном уровне «android.permission.PACKAGE_USAGE_STATS». Поскольку разрешение может быть получено только через приложение «Настройки», троян использует социальную инженерию с целью заставить пользователя предоставить доступ. Вредонос запрашивает разрешение, отображая иконку и название браузера Chrome.

Второй способ заключается в использовании опубликованного на GitHub популярного проекта с исходным кодом для определения открытого на устройстве приложения. Сам по себе он не является вредоносным, однако злоумышленники используют его в преступных целях. Проект позволяет читать данные файловой системы «/proc/» для вычисления запущенных процессов и определения открытого приложения. Как сообщают эксперты Symantec, данный способ не будет работать с выходом следующей версии ОС от Google, известной как Android N.

***

5.06.2016

93 % фишинговых писем распространяют вымогательское ПО

Среди злоумышленников стремительно растет популярность вымогательского ПО. С появлением огромного количества разновидностей и версий, антивирусные лаборатории просто не в состоянии своевременно выпускать декрипторы, пишет InternetUA.

Относительно быстрый способ вернуть вложенные инвестиции и отсутствие какого-либо серьезного сопротивления со стороны антивирусной индустрии могут в скором времени сделать вымогательское ПО самым распространяемым вредоносом.

Согласно данным PhishMe, по состоянию на конец марта текущего года, 93 % фишинговых писем распространяли вымогательское ПО. В декабре 2015 г. всего 56 % от общего количества фишинговых писем распространяли вымогателей.

Обычная сумма выкупа для расшифровки данных: от 400 до 800 долл., иногда 1000 долл. Эта сумма не является огромной для малого и среднего бизнеса, и довольно часто проще заплатить выкуп, чтобы вернуть себе всю информацию, чем потерять ее. Такого мнения придерживается Б. Гриффин, аналитик компании PhishMe.

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.