СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(3.10–16.10)

2016 № 12

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(3.10–16.10)
№ 12

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
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

3.10.2016

Facebook выпустила упрощенную версию фирменного мессенджера для развивающихся стран

Социальная сеть Facebook анонсировала упрощенную Android-версию приложения Facebook Messenger, предназначенную для пользователей из развивающихся стран. Сообщение о выходе приложения под названием Messenger Lite опубликовал на своей странице топ-менеджер Facebook Д. Маркус (InternetUA).

Как отмечает Phone Arena, программа отличается сниженным потреблением трафика, а также более скромными требованиями к техническим характеристикам Android-смартфонов.

Сообщается, что Messenger Lite в ближайшее время станет доступен пользователям из Кении, Малайзии, Шри-Ланки, Туниса и Венесуэлы. В дальнейшем этот список будет расширен, однако какие именно страны могут его пополнить, в компании не уточнили.

Стоит отметить, что это уже второе приложение Facebook, получившее специальную облегченную версию. Ранее социальная сеть представила упрощенный вариант своего основного мобильного приложения для платформы Android.

***

3.10.2016

Facebook тестирует самоуничтожающиеся «истории»

Социальная сеть Facebook приступила к тестированию новой возможности Messenger Day в своем фирменном мессенджере. Функция позволяет отправлять другим пользователям самоуничтожающиеся сообщения, подобно «историям» в Instagram и Snapchat (IGate).

Как сообщает TechCrunch, тестирование возможности началось в Польше. Компания специально выбрала эту страну для испытаний, так как Snapchat здесь мало популярен. В США, к примеру, активное продвижение уже существующего на рынке сервиса могло бы вызвать раздражение пользователей.

«Мы уверены, что люди используют Messenger для того, чтобы ежедневно делиться своими яркими моментами с друзьями и близкими. Мы начали небольшое тестирование в Польше нового способа, позволяющего пользователям делиться фотографиями и видео», – прокомментировали в Facebook.

***

5.10.2016

Базиленко Анна

End-to-end шифрування повідомлень тепер доступне для всіх користувачів Facebook Messenger

Facebook Messenger запустив можливість end-to-end шифрування для всіх користувачів додатку. Про це повідомляє Wired з посиланням на представника компанії (Watcher).

End-to-end шифрування дає змогу засекречувати повідомлення таким чином, що ніхто, окрім співрозмовників чату, не зможе прочитати їх – ні Facebook, ні правоохоронні органи. І хоча у Facebook запевняють, що повідомлення у месенджері й так захищені, нова функція забезпечить наскрізне шифрування одного пристрою від іншого.

Скористатись функцією шифрування зможуть ті користувачі додатку, які оновили Messenger до останньої версії. Шифрування повідомлень у Facebook Messenger вмикається вручну для кожного листування. End-to-end шифрування дає можливість обирати час, коли повідомлення зникнуть – від п'яти секунд до одного дня.

Для того, щоб активувати шифрування потрібно відкрити Secret Conversation на вкладці «Me». Далі – активувати функцію, перетягнувши перемикач. Месенджер також дає змогу вимикати функцію шифрування, після чого користувач не зможе отримувати та відправляти зашифровані повідомлення.

Також функцію можна активувати з вкладки «Home», якщо створити новий чат, натиснувши на відповідну піктограмку, та обрати «Secret». Далі – додати до чату співрозмовника та ввести повідомлення, обравши час, коли повідомлення зникне.

Messenger використовує систему шифрування Signal. Як пише Wired, ця система має хорошу репутацію в співтоваристві інформаційної безпеки. Вона була розроблена громадською організацією Open Whisper Systems та була впроваджена на власному месенджері Signal.

***

3.10.2016

Facebook построит дата-центр в Дании

PixabayFacebook планирует построить третий центр обработки данных за пределами США. Как сообщает Reuters, новый дата-центр разместится в Дании, в городе Оденсе, в котором родился писатель Ганс Христиан Андерсен (Зеркало недели. Украина).

Новый центр обработки данным поможет Facebook хранить и обрабатывать фото и видео, количество которых все время растет. Общая площадь центра составит 184 тыс. кв. км, он обеспечит 1,2 тыс. рабочих мест.

Как отмечает издание, Facebook открыл похожий центр в Швеции в 2013 г. и на сегодняшний день занимается строительством дата-центра в Ирландии.

Ранее сообщалось о том, что Facebook планирует создать социальную виртуальную реальность. Суть проекта, запущенного Facebook, состоит в интеграции виртуальной реальности в интернет-пространство, в том числе в социальные сети. Созданный отдел будет заниматься изучением того, насколько люди смогут обмениваться данными и взаимодействовать в условиях виртуальной реальности. Специалисты отдела будут работать совместно с Oculus и другими подразделениями Facebook, что позволит обеспечить внедрение новой технологии на всех платформах.

***

4.10.2016

«ВКонтакте» для iPhone получил долгожданную функцию

Пользователи приложения «ВКонтакте» для iPhone получили возможность отправлять голосовые сообщения другим абонентам. Обновленная версия мобильной программы уже доступна в магазине App Store (InternetUA).

Для того чтобы отправить голосовое сообщение, пользователю достаточно нажать кнопку с изображением микрофона, находящуюся рядом со строкой для ввода текста в окне чата.

Отправлять голосовые сообщения можно как в личных, так и в групповых чатах. Отправка сообщения осуществляется после того, как пользователь уберет палец с кнопки с микрофоном.

Разработчики отмечают, что отправить голосовое послание проще, чем набирать длинный текст. Кроме того, в некоторых ситуациях – например, за рулем – печатать ответ на сообщение бывает затруднительно.

***

6.10.2016

Олеся Блащук

Украинцы стали больше доверять онлайн-платформам и меньше – традиционным медиа

За последний год телевидение, радио и печать потеряли до четверти своей аудитории, заинтересованной в новостях. При этом количество потребителей новостного контента онлайн возросло почти на четверть. Лидирует Facebook, в два раза увеличивший количество таких пользователей (AIN.UA).

Украинцы очень заинтересованы в новостном контенте: лишь 1 % принявших участие в исследовании Internews не просматривают новости. Однако за последний год традиционные медиа существенно потеряли в аудитории. Больше всего читателей и слушателей потеряли печатная пресса и радио: 25 и 20 % аудитории соответственно или по 7 п. п. Немного сократилось

за год и количество телезрителей: с 85 до 82 %. Впрочем, телевизор до сих пор остается основным источником новостей для украинцев.

При этом доля потребителей новостей онлайн возросла почти на четверть: с 45 до 55 %. Социальные сети для просмотра новостей используют почти столько же пользователей – 52 %.

Телевидение удерживает, в основном, аудиторию старше 35 лет, в то время как популярность сайтов и соцсетей растет за счет молодежи. Примечательно, что последняя все чаще использует для получения новостей не обычные онлайн-медиа, а новостные агрегаторы (например, ukr.net) и социальные сети – Facebook и Twitter, а также «ВКонтакте» и «Одноклассники».

Facebook при этом за прошедший год нарастил на треть количество пользователей в целом (с 27 до 36 %), и почти наполовину – количество использующих платформу для прочтения новостей (12 до 21 %).

Традиционные медиа теряют не только аудиторию, но и ее доверие. При этом онлайн-медиа, напротив, стали доверять больше: за год украинским медиа стало доверять на 10 % больше пользователей. Немного потеряли в доверии и российские медиа.

***

9.10.2016

Duo заменит Hangouts в качестве предустановленного приложения на Android

Приложение Allo может стать будущим мессенджеров компании Google, однако другое приложение под названием Duo заменит собой Hangouts в качестве предустановленного варианта в будущих Android-смартфонах. Электронное письмо с описанием грядущих изменений недавно поступило партнёрам компании, использующим на своих аппаратах сервисы Google Mobile (InternetUA).

Это не то же самое, что Android Open Source Project, поскольку активация этих сервисов означает лицензионное соглашение с Google относительно установки определённых приложений. Можно сказать, что все устройства с наличием магазина Google Play Store используют сервисы Google Mobile, а остальные устройства ставят сторонние магазины без соглашения Google Mobile Services. Встретить подобные модели в продаже можно нечасто.

Согласно письму, Google убирает Hangouts из списка предустановленных приложений для будущих смартфонов. Изменение вступит в силу 1 декабря. Это может свидетельствовать о том, что Hangouts будет использоваться на корпоративном направлении, а заменой станет приложение Duo. Оно позволяет совершать видеозвонки, так что будет конкурентом Skype и других подобных программ на мобильных платформах Android и iOS.

Возможно, в будущем приложение Allo также войдёт в состав предустанавливаемых, пока же его можно скачать в магазине Play Store.

***

10.10.2016
LinkedIn расширяет функциональность сети

После долгих лет просьб пользователей сети обновить или увеличить функциональность сети, LinkedIn наконец-то отозвалась на мольбы. Теперь LinkedIn стал продуктом, который сконцентрировал внимание на главном – имидже работодателей. В последнем анонсе они презентовали Next Gen Career Pages – обновление, которое содержит три вкладки: «Обзор», «Работа» и «Жизнь», что значительно расширит функционал сети. Вкладка «Работа» будет предназначена для упрощения поиска подходящих кандидатов, в то же время, у кандидатов будет повышаться интерес к работодателю. Во вкладке «Жизнь» работодатели смогут делиться информацией для того, что бы вовлечь работников в свои активности, и ценности. Раньше LinkedIn отставала от Facebook и Twitter по предоставлению аналитических услуг. После обновления станет доступным размещение рекламы и полный спектр услуг по аналитике (Marketing Media Review).

***

11.10.2016
Компания Facebook запустила еще одну соцсеть

Компания Facebook запустила сайт Workplace – платную соцсеть для рабочего общения (Украинские реалии).

Сайт устроен практически так же, как Facebook, при этом для работы на нем пользователям популярной соцсети понадобится отдельный аккаунт. В Workplace, в отличие от Facebook, не будет рекламы, передают «Украинские реалии» со ссылкой на «Хвилю».

В Workplace не предусмотрен сервис для работы с документами, пишет Recode. В первых публикациях о Facebook at Work (рабочее название сети) сообщалось, что в сервисе может быть такая функция.

Стоимость работы в Workplace – 3 долл. за человека в месяц, если в сети меньше тысячи активных пользователей. Компании с коллективом больше тысячи и больше десяти тысяч человек будут платить 2 и 1 долл. в месяц за пользователя соответственно.

Recode отмечает, что низкая цена – одно из главных конкуретных преимуществ Workplace. Для сравнения, стандартная стоимость Slack, одного из самых популярных сервисов для рабочего общения, стоит 6,67 долл. за пользователя в месяц. Кроме того, пишет издание, «все умеют пользоваться Facebook».

По словам основателя Facebook М. Цукерберга, Workplace появился как «версия Facebook» для общения сотрудников компании. Позже сервис было

решено адаптировать для массового использования. В тестировании Workplace приняли участие около тысячи компаний.

***

11.10.2016
«ВКонтакте» позволит пользователям пообщаться с космосом

В 2017 г. социальная сеть «ВКонтакте» запустит на Международную космическую станцию (МКС) капсулу с умным ботом Спотти. Об этом 10 октября на своей странице сообщил директор по маркетингу «ВКонтакте» М. Чернышев (InternetUA).

По его словам, запуск бота приурочен к десятилетию соцсети. Устройство станет связующим звеном между пользователями и экипажем МКС, будет передавать на Землю фотографии и видео происходящего на станции, а также сможет получать контент от юзеров.

«Мы решили пойти дальше – дать пользователям возможность общаться не только на Земле, но и за ее пределами», – отметил М. Чернышев. Он также подчеркнул, что первая версия космобота уже была запущена в виде простого искусственного интеллекта, отвечающего на вопросы о космосе.

***

11.10.2016
Базиленко Анна
Facebook запустив окремий додаток Events

Для пристроїв на iOS Facebook запустив окремий додаток Events («Події»). За функціоналом додаток нагадує відповідний розділ соцмережі. Версію додатку для Android обіцяють випустити вже «найближчим часом» (Watcher).

За допомогою Events можна переглядати рекомендовані заходи, обирати події з урахуванням місцезнаходження та захоплень. Користувачі додатку можуть шукати цікаві події за допомогою інтерактивної карти. У стрічці додатку будуть відображатися тільки події. Тут не буде реклами, оновлень статусу чи відео. Таким чином, можна буде шукати потрібну інформацію, не відволікаючись на інші публікації.

Користувачі також зможуть синхронізувати свій розклад, додавши до Events свій календар з мобільного телефону. Як наслідок користувачі зможуть переглядати всі заходи в одному місці.

Крім того, новий додаток синхронізовано з Facebook. Усі дії користувачів будуть відображатися в обох сервісах.

***

16.10.2016
Google и Facebook построят подводную магистраль на 120 Тбит/с

Компании Google, Facebook, TE SubCom и PLDC (Pacific Light Data Communication) заявили об объединении усилий в рамках проекта строительства крупнейшей подводной кабельной системы. Как отмечается в официальном пресс-релизе, результатом сотрудничества станет транстихоокеанская подводная кабельная система длиной 12,8 тыс. км (InternetUA).

Новая система станет первым высокоскоростным кабельным телекоммуникационным соединением между Гонконгом и Лос-Анджелесом. Коммерческий запуск магистрали запланирован на лето 2018 г. Во время монтажа будет использована технология C+L компании TE SubCom, которая позволит удвоить пропускную способность оптоволоконных соединений по сравнению с традиционными система типа C-band. Разработчики уверены, что это будет самый быстрый транстихоокеанский маршрут с минимальными задержками.

По предварительным оценкам, система Pacific Light Cable Network будет способна передавать данные на скорости до 120 Тбит/с. Это почти в два раза больше, чем предложили Nokia Bell Labs и Alcatel-Lucent Submarine Networks в своей последней разработке.

Отметим, для Google это далеко не первый проект подводной магистрали. Она уже инвестировала в такие системы, как Unity, SJC, FASTER, MONET и Tannat.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

3.10.2016

#FreeSushchenko: хэштег в поддержку украинского журналиста вышел в топ Twitter

Хэштег #FreeSushchenko, направленный в поддержку задержанного в Москве журналиста Р. Сущенко, вышел в топ украинского сегмента Twitter (From-UA Новости Украины).

Твиттер-шторм был запущен по инициативе информационного агентства «Укринформ», корреспондентом которого и является задержанный Р. Сущенко, пишет «Обозреватель».

По состоянию на 16:15 хэштег #FreeSushchenko поддержали как минимум 1,3 тыс. пользователей, в том числе посол Украины при ООН В. Ельченко, посол Украины в Польше А. Дещица, посол Украины в Аргентине Ю. Дудин и др.

***

3.10.2016

План капитуляции Путина: российский журналист взорвал сеть

Российский журналист А. Тверской вызвал бурную реакцию в социальной сети своим планом по масштабным изменениям внутри России, который в частности, включает выведение войск из Донбасса и деоккупацию Крыма (From-UA Новости Украины).

Об этом он написал на своей странице в Facebook.

А. Тверской отмечает, что России необходимо уйти с Донбасса, Крыма и Сирии, начать выполнять требования Конституции и международной конвенции о правах человека, провести люстрацию, похоронить В. Ленина, газифицировать страну, продать часть вооружения и вложить деньги в гуманитарную сферу и медицину, отделить церковь от госвласти, амнистировать политзаключенных и прекратить практику показушных праздников.

***

7.10.2016

Херсонская областная служба занятости внедряет новые методы коммуникации

Видеовакансия – новая уникальная услуга на рынке труда, это самый современный и эффективный инструмент для подбора талантливых и перспективных специалистов (Херсон онлайн).

Речь идет о самопрезентации работодателей (размещение видеовакансий на собственном канале YouTube Херсонской областной службы занятости).

«Нынешнее время требует современных методов в работе службы занятости.

Использование видеовакансий позволит оптимизировать и ускорить процесс подбора вакансий, сделает его более неформальным, мобильным, современным», – отмечает Е. Ерашов, директор Херсонской областной службы занятости.

С помощью видеовакансий работодатель имеет шанс выделиться среди конкурентов, рассказать о преимуществах работы именно своего предприятия.

В свою очередь соискатели работы могут внешне оценить потенциального работодателя, наглядно увидеть как выглядит рабочее место, ведь лучше один раз увидеть.

Областная служба занятости предлагает предоставлять видеоинформацию в любой центр занятости для ее дальнейшего размещения на собственном канале YouTube Херсонской областной службы занятости. Услуга бесплатна.

***

6.10.2016

SMM с человеческим лицом: в сети восхитились аккаунтом Верховной Рады в Twitter

Официальный аккаунт Верховной Рады в соцсети Twitter привлек внимание общественности из-за специфической манеры его ведения (Обозреватель).

В частности, журналист Р. Голубовский на своей странице в Facebook разместил несколько скриншотов самых необычных, как для страницы госоргана, твитов.

«SMM с человеческим лицом. Это официальный Twitter Верховной Рады Украины, и он прикольный», – отметил он.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

4.10.2016

Павел Красномовец

Facebook запустил конкурента OLX – сервис Marketplace

Более четверти всей аудитории Facebook, 450 млн человек в месяц, пользуются группами по купле и продажи в социальной сети. Для них компания М. Цукерберга запустила в основном приложении отдельную вкладку Marketplace. Она позволяет быстро просматривать отсортированную ленту вещей, выставленных на продажу неподалеку от пользователя, или самому размещать объявления (AIN.UA).

Marketplace начал работу в США, Великобритании, Австралии и Новой Зеландии на мобильных устройствах, но будет запущен глобально и получит веб-версию, если докажет свою популярность. Вкладка с новым сервисом в iOS-версии Facebook займет центральное место, заменив мессенджер.

У Marketplace есть три основные функции: Browse To Buy, Sell Your Stuff и Search Your Surrounings. Первая – это лента вещей, выставленных на продажу. Благодаря тегам, которые продавцы добавляют в описание вещей, машинным алгоритмам анализа текста, данным о страницах, которые нравятся пользователям, и вещам, которые они просматривают в Marketplace, лента ранжируется по релевантности. Sell Your Stuff или «продавайте ваши вещи» позволяет сфотографировать вещь, добавить описание, цену и опубликовать объявление. Search Your Surroundings позволяет помимо просмотра товаров по категориям вводить в поиск конкретную вещь и фильтровать выдачу по местоположению, цене или увидеть объявления на карте.

«Мы показываем вам наиболее релевантные вещи, даже если вы не знаете, что хотите», – рассказала TechCrunch продуктовый менеджер

Marketplace Б. Пэн. Алгоритмическая лента вместе с фото в качестве главного описания товара может привести к тому, что люди будут листать ее вместо Instagram, провоцируя спонтанные покупки.

Среди преимуществ Marketplace – использование реальных Facebook-профилей продавцами и покупателями, что вызывает больше доверия у сторон. При этом, в сервисе нет системы рейтингования, которая помогла бы отсеять недобросовестных продавцов. Facebook не будет отвечать за какие-либо проблемы, возникающие в процессе заключения сделки и не интегрирует возможность оплаты за товар прямо в Marketplace – пользователям придется решить этот вопрос самостоятельно. «Мы видим нашу роль только в том, чтобы помочь продавцам найти покупателей», – говорит Б. Пэн.

В Украине до запуска сервиса Facebook еще далеко, но крупные площадки для онлайн-торговли уже закрываются. Недавно прекратила свою работу Aukro.ua, а все торговцы были переведены на ecommerce-проекты группы компаний EVO.

***

5.10.2016

Пользователи торговой площадки Facebook стали продавать оружие и наркотики

Торговую площадку Facebook Marketplace пополнили предложения о продаже наркотических средств и огнестрельного оружия. На это обратило внимание издание Quartz (InternetUA).

Помимо наркотиков и различных винтовок и пистолетов Markeplace содержит также объявления о продаже змей, ежей и других диких зверей. При этом правила площадки запрещают торговать наркотиками, оружием, табаком, алкоголем и животными.

«Мы работаем над решением проблемы и будем внимательно следить за системой, чтобы гарантировать выявление и устранение нарушений, прежде чем большое количество людей получит доступ к Marketplace», – заявила директор по продуктам Facebook М. Кю.

***

6.10.2016

Как онлайн-видео меняет рекламную индустрию

В 2015 г. впервые за последние 10 лет медийная онлайн-реклама на американском рынке обошла поисковую рекламу по объемам. Ранее поиск уверенно занимал лидирующую позицию, и, казалось, ничто не может помешать ему продолжать свой рост вместе с увеличением количества интернет-пользователей и расширением функционала. Однако, изменения в поведении пользователей онлайн-сервисов, драйвером которых стало распространение мобайла, изменили и рекламные тренды. Одним из таких

факторов, значительно повлиявших на увеличение объемов медийной рекламы, стал бурный рост онлайн-видео (МедиаБизнес).

Видеопросмотр перетекает в онлайн

Изначально тенденция перетекания пользователей платного ТВ в онлайн-видеосервисы началась в США в 2013 г., но особенно ярко проявилась в 2016 г. Только за II квартал почти миллион американских пользователей отказались от ТВ-подписки, заменив ее интернет-сервисами. Например, одна из крупнейших вещательных сетей ESPN с 2011 г. утратила более 11 млн подписчиков, причем 2,2 млн из них только за последние полгода.

То есть очевиден тренд: зрители все чаще отдают предпочтение онлайну как более гибкой среде в выборе программ и фильмов для просмотра.

Причиной этих изменений стал переход к мульти-девайсной манере потребления контента. В течение дня пользователи стали намного чаще заходить в Интернет через мобильные устройства в дополнение к привычным десктопным. При этом значительную часть своего онлайн-времени они проводят в социальных сетях. И естественно, что появление в них видеосервисов спровоцировало бурный рост просмотров онлайн-видео. В результате, среднее время, проводимое в мобильном видео в день, увеличилось с 2013 г. в два с половиной раза.

Вторая тенденция – это использование дополнительных устройств параллельно с просмотром ТВ. По данным Google Consumer Barometer, более половины пользователей в США уже используют смартфоны, планшеты и ноутбуки во время просмотра ТВ, в том числе и для параллельного просмотра видеоконтента. То есть внимание телезрителей все больше перетекает в онлайн.

Рекламодатели идут онлайн вслед за аудиторией

Вместе с ростом аудитории, которая смотрит видео в онлайне, увеличиваются и рекламные бюджеты на этот канал. Особенно быстро в последние два-три года росли расходы на мобильное видео – плюс 50–100 % в год, в то время как десктопное видео росло намного скромнее – на 20–25 % ежегодно. Фактически, онлайн-видеореклама в США прибавляет из года в год до 2 млрд долл.

Вместе с этим доля ТВ-рекламы в общем рекламном пироге продолжает уменьшаться. По прогнозам ZenithOptimedia, уже в следующем году digital-реклама в США обойдет по объемам телевизионную, во многом за счет тренда роста видеорекламы в онлайне.

Крупные рекламодатели, традиционно размещающие рекламу на ТВ, сейчас активно трансформируют свои стратегии под онлайн для получения эффективного охвата. Интернет-платформы идут в этом им навстречу, обеспечивая инструментами, которые могут измерять эффективность онлайн-видеокампаний в понятных для брендов метриках. Так, Facebook совместно с исследовательской компанией Nielsen в прошлом году запустил систему планирования совместных размещений ТВ+Facebook Video на основании TRP, а также инструмент для оптимизации рекламных кампаний в Facebook и Instagram по показателям Brand Awareness. А Google разработал и внедрил

решение Brand Lift для измерения эффективности размещений в YouTube. Оно позволяет оценивать уровень осведомленности потребителей о бренде, запоминаемость рекламы, предпочтительность бренда и намерение купить.

Недавно Google заявил о планах расширить действие Brand Lift и на ТВ-кампании. Таким образом, рекламные размещения в онлайне и ТВ будут сравниваться по одной базе, что дает возможность более точно оценивать эффект от размещений в каждом из каналов и делать оптимизацию во время рекламной кампании.

Высокие темпы роста рекламных бюджетов на онлайн-видео прогнозируются и на следующие три года – видео будет расти быстрее других digital-каналов. Это отражает тенденцию роста потребления видеоконтента: к 2018 г. видео будет составлять 75 % всего мирового интернет-трафика.

Онлайн-видео в Украине

Украина традиционно отстает от мировых тенденций, поэтому изменения, происходившие на западных рынках за последние годы, еще только предстоят нам в ближайшее время. Одним из драйверов роста послужит распространение быстрого 3G-интернета. Оно уже начало оказывать влияние на потребление видеоконтента через мобильные устройства, существенно увеличив количество обращений пользователей к видеоресурсам.

За последний год просмотр видео онлайн в Украине рос очень быстро. По данным Factum Group, YouTube в августе 2016 г. по доле активных пользователей вышел на второе место среди всех интернет-ресурсов, хотя еще год назад занимал лишь пятое место. По данным Google, украинский сервис YouTube по показателям роста занимает одно из лидирующих мест в Европе.

Не отстают от лидера и другие видеоплатформы, существенно прибавившие в доле и количестве пользователей за последний год. При этом увеличивается частота посещения видеоресурсов и время, которое проводят пользователи за просмотром. В украинском YouTube это время возросло на 70 % за год.

Эти тенденции не остались незамеченными для рекламодателей. С начала года рекламные агентства все чаще предлагают модели размещения ТВ+Онлайн. Именно такой формат позволяет сейчас построить максимальный охват и частоту контакта, особенно по молодым группам пользователей. Для отраслей, имеющих ограничения в ТВ-рекламе, это позволяет качественно достигать аудиторию, а для рекламодателей с ограниченным бюджетом – контактировать только с целевой аудиторией.

Как результат, бюджеты на онлайн-видео очень быстро растут, занимая всё большую долю в медийном пироге интернет-рекламы. В ближайшие время они повторят те тренды, которые наблюдались на западных рынках за последнее два года.

Единственным препятствием на пути роста онлайн-видеорекламы остается ограниченность видеоинвентаря на рынке. Несмотря на быстрый прирост онлайн-видеосмотрения в Украине, спрос на видеоразмещения растет гораздо быстрее предложения, что подталкивает цены на видеорекламу вверх.

Результатом послужит переход в ближайшее время основных продавцов рекламы на аукционную модель продаж.

***

10.10.2016

Apple воздержится от приобретения Twitter

Судя по сообщениям последних недель, основная битва за приобретение сервисов микроблогов Twitter должна будет развернуться между тремя потенциальными покупателями – Apple, Google и Disney. Однако, как передает издание Recode, ни одна из упомянутых корпораций в действительности не заинтересована в покупке компании, судорожно ищущей нового хозяина (InternetUA).

Несмотря на появлявшиеся ранее сведения, источники Reuters утверждают, что процесс переговоров может и не закончиться подписанием сделки. По словам этих же источников, Twitter хочет свернуть эти переговоры к моменту оглашения квартальных результатов, запланированному на 27 октября.

Крупнейшая социальная сеть является лакомым кусочком для корпораций с тугими кошельками в первую очередь потому, что приобретение этой компании предоставит им доступ к миллионам новых пользователей и их данным, которые можно будет с выгодой использовать. К примеру, Google мог бы расширить свой рекламный бизнес, Apple – укрепить социальную составляющую своих онлайн-сервисов, а Disney получить новый инструмент для продвижения своего контента.

Для Twitter же возможная продажа может значить одно: рекламодатели переместят свое внимание на другие популярные социальные сервисы, такие как Facebook, Instagram и Snapchat. Тем временем на фоне сообщений о возможной утрате интереса со стороны потенциальных покупателей акции Twitter на бирже заметно упали в цене.

***

10.10.2016

Исследование: как бренды раздражают пользователей в социальных сетях

По словам потребителей, слишком частое размещение постов больше всего раздражает их в действиях брендов в социальных медиа, отмечает проведенное в июле 2016 г. исследование Sprout Social среди 1,022 американских юзеров. Как отметили респонденты, бренды раздражают их частыми постами/промо (57,5 %), использованием сленга/жаргона (38,4 %), отсутствием индивидуальности (34,7 %), неудачными попытками быть смешными (32,3 %) и игнорированием их сообщений (24,7 %).

Потребители следуют за брендами, так как заинтересованы их продуктами/услугами (73,4 %), предложениями/акциями (58,8%) и так как находят компании занимательными (51,3%). Среди главных причин отказа

следовать за брендами опрошенные назвали частые посты/промо (73,4%) и нерелевантный расшариваемый контент (41,1%) (Marketing Media Review).

***

12.10.2016
Скільки заробляють блогери в Instagram

За рекламну публікацію блогери можуть отримувати від 26 до 78 тис. дол. (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це повідомляє The Independent.

Британка З. Сагг має більше дев'яти мільйонів підписників, що забезпечує їй щомісячний дохід у розмірі 65 тис дол. А всі її статки становлять близько 3 млн дол.

Соціальні медіа стали потужним знаряддям фешн-індустрії, оскільки забезпечують комунікацію з величезною аудиторією.

***

11.10.2016
Facebook экспериментирует с рекламой в группах

Рекламные объявления в группах имеют такой же вид, как и в новостной ленте социальной сети, и таргетируются по тематикам групп так же, как и в стандартном варианте, отмечает cossa.ru. «Мы начали тестировать доставку рекламы пользователям групп. После оценки полученных результатов мы решим, как действовать дальше», – объявила пресс-служба Facebook. Все новшества направлены на обеспечение стойкого роста доходов от рекламы и увеличение объемов запускаемых кампаний. В числе прочих Facebook также тестирует «живое видео» в формате мид-роллов и спонсорские объявления для бизнеса в своём мессенджере. А в начале месяца Facebook запустил в США, Великобритании, Австралии и Новой Зеландии раздел Marketplace для организации покупки и продажи местных товаров – расширение функционала продающих групп (Marketing Media Review).

***

13.10.2016
Google купила медиастартап Famebit

Интернет-компания Google, входящая в состав холдинга американского Alphabet, анонсировала приобретение медиастартапа Famebit, который специализируется на взаимодействии рекламодателей с YouTube-блогерами (InternetUA).

Стоимость сделки не раскрывается. По условиям соглашения, Famebit останется независимой компанией, но будет работать в интересах Google.

Платформа FameBit позволяет блогерам устанавливать контакты с брендами для создания контента, спонсируемого рекламодателями. Сейчас блогерам приходится самостоятельно заниматься поиском спонсоров или подключаться к медиасетям, что отнимает время и деньги.

«Мы уверены, что технологии и опыт Famebit предоставят создателям контента в YouTube больше возможностей для сотрудничества с брендами и поможет увеличить их доход», – отмечает вице-президент по управлению продуктами Google А. Бардин (Ariel Bardin).

В Google также надеются, что благодаря Famebit рынок брендированного контента и доходы его участников возрастут. За свое существование Famebit привлекла около 1,5 млн долл. инвестиций.

***

12.10.2016

Twitter запустила в Нью-Йорке загадочную рекламную кампанию

Twitter запустила в Нью-Йорке новую рекламную кампанию, разместив разноцветные изображения со своим логотипом на стенах некоторых станций метро. Картинки с большими восклицательными и вопросительными знаками ничего понять не дают – они даже не объясняют, что такое Twitter и для чего его можно использовать. Однако в короткой публикации в своём блоге компания заявила, что это расширение цифровой кампании под названием «What’s happening?», которая была запущена в июле и, в отличие от нынешней рекламной кампании, объясняла назначение Twitter (InternetUA).

Поэтому вполне можно предположить, что это всего лишь начало чего-то большего. Директор по маркетингу Twitter Л. Берланд (Leslie Berland) написала в блоге, что скоро начнёт появляться больше рекламы, «отражающей и подчёркивающей самые большие истории, разворачивающиеся в Twitter». Вполне вероятно, это такой намёк на грядущие выборы президента США и недавние дебаты, которые транслировались в сервисе микроблогов. Возможно, скоро Twitter начнёт рисовать на стенах Нью-Йорка твиты кандидатов в президенты. Представитель компании отказался давать какие-либо комментарии касательно этого.

Во всём этом есть одна забавная деталь: среди небольшого числа мест, где Twitter решила разместить свою рекламу, присутствует станция метро Уолл-стрит, на которой в силу её местонахождения за день бывает огромное множество работников финансового сектора. Возможно, так компания напоминает о том, что даже если её никто не приобретёт, она всё равно никуда не уйдёт.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

5.10.2016
Наркота, або Чому ми так любимо соціальні мережі

Юрій Мартинович
репортер, оператор, письменник
Чи часто ви думаєте над тим, чому соціальні мережі були, є і будуть популярними? (Західна інформаційна корпорація).

Коли ви це читаєте, саме тут, в Інтернеті, то можу побитися об заклад, що ви десь таки зареєстровані: Facebook, «ВКонтакте», Instagram, Twitter, Skype, «Одноклассники» і т. д., а як ні, то не забувайте про електронну пошту – це теж свого роду соціальна мережа. Отже, коли я довго сиджу в цих онлайн-мережах, то починаю думати, що знаю відповідь на запитання, яке виніс у заголовку. Це проста та зрозуміла відповідь: соціальні мережі збільшують рівень серотоніну, допаміну та окситоцину у нашій голові. Допоки це так, допоки вони роблять нас щасливішими, людині складно кинути ці легкі й приємні наркотики. Нам подобається безпека, можливість спостерігати, знати й спілкуватися у будь-який емоційний чи розумовий спосіб, який ми самі вибираємо. Нам подобається збирати лайки, подобається це відчуття гри, яке пробуджує у нас те первісне щастя – бути потрібним і не самотнім. Мільярди наркоманів по всьому світі вірять у цей наркотик, бо він психо-фізично діє. Тому Інтернет коштує мільярди мільярдів і так добре розвивається. Та цікаво інше, мені здається складно не погодитися із тим, що людина ще не придумала такого наркотика, від якого б не страждала у підсумку (Інтернет – залежність), хіба ні?

***

5.10.2016
София Булгакова
Жители Франции чаще проводят время за смартфоном, чем за телевизором

Жители Франции стали чаще проводить время со своими телефонами и различными гаджетами, чем с телевизором. Такие выводы сделали сотрудники аналитического центра Flurry Analytics после проведенного исследования (HiTech-News.ru).

Организация является филиалом компании Yahoo!, в её обязанности входит проведение различных исследований, обработки и анализ полученных данных. По результатам 2015 г., французы провели больше времени в «компании» своего смартфона, а не телевизора.

Экспертам пришлось изучить данные от более 14 тыс. мобильных приложений, которые устанавливали на свои гаджеты жители Франции. Оказалось, что телефоны в развлекательных целых стали использовать на 17 % чаще, и на 31 % больше выполнять с их помощью работу. На 217 % в 2015 г. возросла популярность различных спортивных приложений. Это связано, в первую очередь, с футбольным Чемпионатом Европы и Олимпийскими играми.

Аналитики подчёркивают, что люди с каждым днём становятся всё зависимее от мобильных программ. Количество пользователей, которые запускают приложения чаще 60 раз в день, возросло на 60 %. Для получения этой информации специалисты проанализировали данные с 830 тыс. мобильных программ, установленных во всех странах мира.

***

5.10.2016

Павел Красномовец

Почему просмотр глупых видео с котиками полезен для людей – исследования

Просмотр видео с котиками в Facebook выглядит пустой тратой времени, но многое из того, что пользователи делают в соцсетях, хорошо влияет на их настроение. Об этом свидетельствует множество исследований, пишет Wall Street Journal. Время, проведенное онлайн, может способствовать развитию социальной жизни пользователей, бороться с одиночеством, улучшать настроение, отношения и память (AIN.UA).

Нейрофизиологи уверены, что люди получают впрыск нейромедиатора дофамина, когда активируется система вознаграждений мозга. Это может происходить, когда пользователи получают лайк или комментарий под своим постом. Так, исследование ученых университета Карнеги-Меллона и Facebook показало, что когда люди получают 60 дополнительных персонализированных комментариев в месяц сверх нормы от людей, которые им не безразличны, то их самочувствие улучшается. «Когда вы взаимодействуете с кем-то, то подаете сигнал, что вам не все равно. Это вас подпитывает», – говорит М. Берки, исследователь Facebook.

Исследование ученых из университетов Корнелла и Пекина показало, что если люди постят личные события в соцмедиа, то они лучше их помнят. Так, через неделю эксперимента участники помнили 55 % событий, которые они запостили онлайн, против 42 %, которыми они не поделились. Через две недели эти цифры составили 44 и 31 % соответственно.

Ученые из университета Калифорнии, Сан-Франциско, Торонто и Клермонта в своем исследовании показали, что пользователи, которые ставят

на аватар фото со своими «половинками», более удовлетворены своими отношениями, чем те, кто так не делает. А в те дни, когда пользователи удовлетворены своими отношениями, они с большей вероятностью разместят пост об отношениях в соцсетях.

Доктор Дж. Мирик, ассистент профессора в медиашколе университета Индианы, изучала видео с котиками. В своем исследовании она пришла к выводу, что люди, которые смотрят видео с котиками, больше времени проводят онлайн. Помимо этого, они были больше готовы к социальным взаимодействиям: 75 % сказали, что лайкают по крайней мере последнее видео с котами; 54 % сказали, что они поделились этим видео; 23 % его прокомментировали. Участники исследования также сказали, что чувствовали себя более счастливыми, уверенными, полными энергии и менее тревожными и раздраженными после просмотра видео.

***

4.10.2016
Ольга Карпенко
Как я несколько недель делал все, что предлагал мне Facebook

Facebook старается подталкивать пользователей к тому, чтобы те рассказывали о себе, лайкали фото, праздновали годовщину дружбы. Но не всегда эти призывы к действию смотрятся уместно и служат своей цели: вовлекать аудиторию. Журналист BuzzFeed Ч. Уорзел решил проверить, насколько хороши эти алгоритмы Facebook, и несколько недель делал все, что сеть подсказывала ему сделать. Результаты получились устрашающими (AIN.UA).

В Facebook очень легко опростоволоситься. Ваша небрежная ремарка о политике втихую настроит против вас политически сознательного родственника и заранее разрушит семейный обед на День благодарения. Здесь найдутся фотографии счастливых деньков, запечатлевшие решение, о котором вы позже пожалеете. Старые знакомые вашей бывшей, из-за которых вы начинаете вынужденно «дружить».

Подобные небольшие проблемки встречаются в сети повсеместно и являются побочным результатом неутомимых требований Facebook скармливать ему все новые данные, а в конце каждого скролла – заводить новых друзей, поддерживать связи с теми, кто вам нравится и кого вы любите. Именно это привело к тому, что на прошлой неделе я пригласил 240 человек на вечеринку в честь дня рождения парня, с которым я виделся всего дважды.

Эта вечеринка родилась из опыта, нацеленного на экспериментальную проверку концепции таинственных алгоритмов работы Facebook – сложных самообучаемых программ, которые зазывают нас читать, постить, делиться, заводить друзей, тех подмосток, на которых возводятся наши Facebook-личности.

Представим, что постоянные посылы от алгоритмов Facebook, которые приглашают нас делиться контентом и общаться с друзьями – это чистейшее выражение того, как сеть хочет, чтобы ее использовали. Тогда, если пользователь следует каждому указанию сети – это теоретически создаст платоновский идеал общения в соцмедиа – как его представляют в этой компании.

Так что несколько недель подряд я делал в Facebook все, о чем меня просили его алгоритмы. Ни один френд-реквест, ни один перепост не попадал для меня в категорию «это уж слишком».

Facebook для каждого из своих 1,7 млрд пользователей создает цифровую личность. Компания требует от пользователей регистрироваться под настоящими именами, и эти данные используются как цифровое удостоверение в мириадах сервисов и приложений. Из-за своих масштабов Facebook – это место, где вы с большой вероятностью повстречаетесь со всеми своими родственниками, ближними и дальними. Сеть часто используют для проверки кандидатов как работодатели, так и приемные коммисии вузов. И поэтому на Facebook мы размещаем стилизованную, несколько идеализированную версию себя.

Эволюция Facebook – от вузовского фотостока до вездесущей социальной платформы – проходила во время тектонического сдвига в отношении к публикации личной информации. Меняющиеся социальные нормы привели к тому, что в Кремниевой долине называют context collapse (особенность презентации себя в социальных сетях перед множественными аудиториями и группами в противовес обычному общению в небольших группах в офлайне. Если при обычном взаимодействии человек может считывать социальный контекст и подстраиваться под него, то в сети невозможно вычленить какой-то один контекст. – Ред).

В апреле подобный коллапс обвинили в 21%-ном падении количества оригинальных репостов на Facebook. Именно в тот момент я стал замечать внезапный прилив призывов от Facebook отпраздновать странные праздники или же написать о какой-то онлайн-трансляции. Представитель Facebook рассказывал мне, что компания начала тестировать эти виды вовлекающих сообщений еще 18 месяцев назад, но постепенно усиливала их присутствие в сети. Facebook приглашал меня поучаствовать. Чем я и занялся.

Первые дни эксперимента протекали вяло, Facebook довольно мало от меня требовал, поскольку обычно я использую сеть эпизодически, не давая ее алгоритмам шанса вовлечь меня во что-то. Но в какой-то момент я провозгласил свою лояльность бейсбольному клубу Cleveland Indians в виде брошенного мимоходом лайка.

Как-то вечером, вначале эксперимента, я открыл Facebook и на самом верху ленты обнаружил текущий счет игры этой команды, с дружеским предложением от Facebook рассказать друзьям о том, что я смотрю игру. Так что 16 августа я быстро написал комментарий «Прикольно» и зашвырнул

информацию о том, что превратилось в проигрыш чикагским White Sox, в ленты примерно 650 людей, которые доверяли мне как другу.

Друзья восприняли это, скажем так, прохладно. Реакции посыпались преимущественно не в Facebook, а в виде расстроенных эсэмесок. «Пожалуйста, прекрати, что ты там вытворяешь с “Индианс”, ОК?», – говорилось в одной из них.

Так продолжалось несколько дней. Facebook с ответственностью увлеченного спортом дедушки ежедневно предоставлял мне счет игры, веря, что мне это настолько интересно, чтобы я делился этим с друзьями. Мне было все равно. Но я превратился в иронический аналог спортивного канала и постил об этом. Все это время Facebook вдохновлял меня продолжать: «Вам и еще 1 218 967 пользователям нравятся Cleveland Indians», уговаривал он меня, как будто пытаясь убедить в том, что где-то в голубых далях все же сыщутся читатели для моих говнопостов.

Учуяв кровь свежей жертвы, Facebook начал подбивать меня высказываться на всевозможные странные темы. Таким образом, я отметил 177 лет фотографии, поблагодарил олимпийских спортсменов за их труд, порадовался 25-й годовщине коммерческого Интернета.

Я отпраздновал дружбу на Facebook с коллегой по работе, затем размышлял о 100 годах «невероятных пейзажей из наших национальных парков». Казалось, каждое утро Facebook отыскивал для меня что-то новенькое в качестве повода попраздновать. Как и с бейсбольной командой, я начал репост с колкости в стиле «Обожаю фотографировать со своего смартфона», но после очередной возмущенной SMS решил воспользоваться возможностью и пообщаться со своими друзьями на Facebook. Я старался истово служить алгоритмам сети.

На 25-летие Интернета я серьезно написал о том, как утешительно осознавать: я старше, чем явление, столь могущественное, как сеть. Несколько друзей даже подпели мне в лад и не последовало никаких пассивно-агрессивных SMS. Так что я продолжал.

Через пару дней я прокомментировал очередной счет игры «Индианс», признавшись, что я редко смотрю игры до плей-оффов и вряд ли могу прикидываться серьезным фанатом бейсбола. Мои друзья, как ни удивительно, повелись на приманку. Кто-то поддержал меня, кто-то – начал рассуждать о самоидентификации. Сразу несколько друзей уверили меня в том, что я все еще могу называться фанатом бейсбола. И только один из них писал об этом с иронией.

Так что, из приглашения Facebook у меня получилось даже нечто вроде настоящего обсуждения с несколькими людьми. В том числе – с хорошими друзьями, с которыми мы какое-то время не общались.

Но вообще говоря, вовлекающие статусные сообщения Facebook всегда выглядят очень аляповато, видно, что это – искусственное вовлечение. Они смотрятся как «дудлы» Google с местом для подписи. Что неудивительно, Facebook – это все же рекламная машина, работающая на широких потоках

пользовательских данных. Во II квартале 2016 г. компания заработала 6 млрд долл. на рекламе.

Есть смысл в том, что маркетинговый бизнес Facebook понемногу влияет на ее старания вовлекать аудиторию (что, в свою очередь, может отпугнуть пользователей от публикации личной информации).

Если рассматривать это с точки зрения вовлекающих сообщений, идеальный пользователь Facebook не просто часто взаимодействует с контентом, ставит лайки, но публично, ежесекундно и с огромным энтузиазмом общается со своими любимыми брендами – от основных спортивных команд до изготовителей открыток.

Спустя пару недель после старта эксперимента я понял, что мое определение вовлекающих действий Facebook – слишком узкое. Я понимал, что всюду, начиная с ленты, меня окружают изощренные алгоритмические намеки.

Я кликнул по запросам на добавления в друзья и там меня ожидал кошмар. Кнопки «Принять запрос» с шестилетней историей игнорирования. Я принял их все. Всего за пару минут во «Входящих» появилась целая группа милых турков, благодарящих меня за запоздалую реакцию. PR-специалист сразу бросилась в меня питчем приложения. Пользователь без аватарки просто написал «Кто это?». Чувство было взаимным.

Затем пришел черед «Предлагаемых друзей». Меня шокировал этот список – перечень людей, которых Facebook подобрал для меня довольно точно. В каком-то извращенном диккенсовом понимании Facebook представил мне духов прошлого, настоящего и будущего. Тут был список людей, которых я знал и хотел бы забыть. Были и знакомые, которых я не готов был наблюдать через постоянное Facebook-окно. Были и те, с кем бы я желал познакомиться, но недостаточно знал их, чтобы просить о дружбе.

Были и прочие: бывшая девушка, с которой встречался мой бывший сосед по общежитию, коллега по работе, с которым я виделся всего единожды, пару псевдознаменитостей, которых я, как казалось, где-то видел. Запрос, запрос, запрос. После каждого Facebook требовал у меня написать приветственное сообщение.

В большинстве случаев я печатал что-то схематично-дружелюбное, это бы могло убедить моих новоприобретенных друзей в том, что это сообщение сгенерировано роботом. Никто не ответил. Как-то вечером, после особенно глубокого заплыва за друзьями я почти физически скукожился от неловкости, выслав запрос президенту BuzzFeed – милому мужчине, которого я видел только походя. Моя девушка взглянула на экран, потом перевела на меня взгляд: «Ты сейчас разрушаешь собственную жизнь».

Я стал королем «желаний на день рождения». Я вливался в десятки предложенных Facebook-групп: от каких-то сообществ наблюдателей за птицами, которые высылали мне уведомления всякий раз, как кто-то постил прекрасное фото цапли, до групп гаражных распродаж, я вступил в три группы естественных родов, парочку дурацких групп с вирусными видео, и в несколько прикольных групп клубов по игре Magic: The Gathering.

Никто из них не отверг меня. Даже группа республиканцев-выпускников Бруклинского колледжа 2008 г. выпуска. Я никогда не учился там, я даже выпустился не в этом году. Facebook приглашал меня лайкать все больше страниц в какой-то гротескно-бессмысленной прогрессии: сначала страницы журналистов, затем страницы ТВ-ведущих-блондинок, затем страницы большегрудых моделей и малоодетых женщин-бодибилдеров. Видимо, его алгоритмы интерпретировали мои ураганные реакции как действия человека, которому все мало.

Итак, вначале сентября Facebook предложил, чтобы я организовал для Патрика вечеринку. До 23 июня этого же года я не догадывался о существовании какого бы то ни было Патрика. Предложение от Facebook по этому поводу объявилось примерно на трети длины моей ленты, вместе с картинкой мультяшного тортика и дружественным, хотя и пассивно-агрессивным CTA: «Если вы встречаетесь 21 сентября, почему бы не пригласить друзей, организовав ивент?». Это смотрелось как обычное ванильное предложение, если не учитывать тот факт, что до 23 июня этого года я не знал о самом существовании Патрика, а с тех пор встречал его дважды.

Хотя я хорошо отношусь к нему. Мы прекрасно общаемся, у нас много общих интересов, мы одинаково шутим, поэтому я подружился с ним на Facebook после того, как мы впервые встретились. Но я многого не знаю о Патрике, и не смогу это выучить даже из его Facebook-профиля. Все эти мелкие таинственные личные особенности, общие переживания и секреты, которые скапливаются за время дружбы. И вот, несмотря на крайне поверхностное знакомство, Facebook решил, что я достаточно готов, чтобы организовывать Патрику вечеринку – празднование с его друзьями и моими. Конечно же, откуда здесь взяться неловкости.

Как ни странно, Facebook даже был в чем-то прав. Патрик и я живем в разных городах, и поскольку я на его вечеринке быть не смогу, я создал ивент, открыто говоря, что создать его мне предложил алгоритм Facebook. Я пригласил около 250 людей, которых знал сам, и оставил список открытым, чтобы друзья Патрика также смогли добавлять себя и других. Я настроил и страничку, куда люди могли бы скидываться деньгами по PayPal, чтобы Патрик мог закупить алкоголь на пьянку. После чего, мертвея от страха, стал ждать реакции.

Мое приглашение люди воспринимали ошарашенно и недоуменно. Другие общие друзья обменивались шутками. Мне стали сыпаться SMS с вопросами, настоящая ли это вечеринка. Вся эта штука была смехотворной с самого начала, но народ развлекался. Мы набрали целых 55 долл. Очень надеюсь, что вечеринка все же состоится.

Интересно, заметило ли всевидящее око Facebook потенциальную дружбу между нами еще до предложения организовать вечеринку. Я следил за Патриком на Facebook после знакомства, проверял, где он учился. Патрик расшарил мою статью с комплиментом, а я поставил лайк. Нас обоих затегали на фото с вечеринки, где мы встретились.

Иными словами, мы скормили алгоритму Facebook достаточно тонких намеков, указующих на связь. Так что Facebook совершил именно то, чего можно было бы ожидать от свахи, работающей только с сырыми данными и обрывками дорогого проприетарного кода. Он отбросил всяческую воспитанность и пропустил то, что казалось ему зарождающейся дружбой, через свой ускоритель элементарных частиц. И это даже, можно сказать, сработало.

Алгоритмы Facebook вечно жаждут данных. Им хватает пары намеков. Они не ждут трех дней, чтобы скинуть SMS после первого свидания, они – это тот парень, который, скучая по вашему голосу, позовет вас в видеочат, сидя в туалете, даже если свидание не закончилось.

И в этом заключается проблема: Facebook склонен неверно понимать, чего хотят его пользователи, при этом пытается вываливать в общий доступ как можно больше их данных. В 2010 г. Facebook поменял настройки приватности так, что обновления статуса по дефолту стали публичными. Facebook пытался запрещать псевдонимы, но затем отменил этот бан из-за жалоб трансгендеров и жертв домашнего насилия.

Мой опыт – делать все, о чем меня просил Facebook, указал на подобные же проблемы. Я замусорил ленты друзей банальщиной. Я посылал наверняка неадекватные запросы на дружбу. Я истово делился всем подряд. Когда Facebook предложил создать слайд-шоу из недавних фото, я запостил видео, состоящее из чеков отчета о расходов под какую-то дурацкую музычку.

Алгоритм Facebook, может, и верно угадал мою склонность подружиться с Патриком, но чаще, чем стоило, он оказывался грубым, тупым инструментом, предполагающим, что все мои мимолетные увлечения – это страсти на всю жизнь.

Я уже перестал реагировать на призывы сети, но ужасные последствия моего эксперимента все еще всплывают в ленте. Мое непритязательное одобрение всех запросов в друзья вдохновило еще больше милых пользователей из Турции стучаться ко мне. Моя лента представляет собой хаос из уведомлений от различных стремных групп, а всякий раз, как Патрик лайкает фото, оно вцепляется в топ моей ленты, как будто это минимум объявление о помолвке.

Но было и нечто успокаивающее в том, чтобы смотреть на работу алгоритма, открыв рот. Несмотря на свои миллиарды пользователей, тонны денег, армии гениальных инженеров, компания все еще ни на миллиметр не приблизилась к пониманию человека. Facebook знал обо мне больше, чем мне хотелось бы, воздадим ему должное, но на самом деле довольно плохо понимал, кто же я такой. Я почти десять лет рассказывал сети, кто я, но в конце она слышала только то, что ей хотелось услышать.

***

12.10.2016

Больше половины украинцев не могут представить свою жизнь без мобильного

51 % украинских потребителей говорят, что они чувствуют тревогу, когда их мобильные устройства не под рукой, следует из глобального исследования Nielsen Mobile shopping, banking and payment о потребительских привычках пользоваться мобильным устройством для покупок и банковских операций (ITnews).

Больше половины потребителей в Украине (54 %) не могут представить свою жизнь без мобильного устройства, а 72 % потребителей говорят, что мобильное устройство делает их жизнь лучше.

В современном цифровом мире, где новости, покупки онлайн, банковские услуги и развлечения доступны 24/7 с помощью всевозможных мобильных устройств, страх выпасть из информационного поля – объяснимый феномен. Почти половина украинских потребителей (43 %) согласна с тем, что личное общение заменяется электронным, однако не считает это проблемой, поскольку 27 % респондентов предпочитают написать сообщение, а не поговорить. На вопрос «Что именно Вы делали с помощью мобильного устройства за последние шесть месяцев?», 80 % украинских потребителей ответили – «пользовались соцсетями».

Параллельно с тем, как мобильное устройство изменило наш стиль общения, оно делает революцию в мире розничной торговли и банковских услуг. По оценкам Института Спроса (Demand Institute) в Нью-Йорке, которым управляет Nielsen совместно с Членами Совета Конференции (Conference Board), в течение следующих 10 лет объем безналичных операций достигнет 10 млрд долл. США в дополнительных потребительских расходах.

«Мобильная коммерция имеет огромное значение для всей розничной экосистемы, – говорит Т. Бессмертная, Генеральный директор Nielsen в Украине и Беларуси. – Мобильные устройства не только привлекают новых потребителей, они также позволяют применить индивидуальный подход к ним. Это значит, что предложения о товарах и услугах могут формироваться с учетом модели поведения потребителя, его потребностей и предпочтений. И хотя в Украине мобильная коммерция только развивается, ритейл активно интегрирует новые решения. Потребители все еще не доверяют операциям онлайн, особенно платежным. Бизнесу важно понять, как потребитель делает покупки, и предложить удобное и безопасное решение».

Маніпулятивні технології

4.10.2016
Тролесфера

Надія Романенко, Ярина Михайлишин, Павло Солодько, Орест Зог

«Тексти» вирахували мережу з близько 2 тис. користувачів Facebook, яка тісно пов'язана з групами бойовика ДНР С. Мазури. Останній довго видавав себе за патріота України. Це мережа з публічних груп і користувачів, які, прикриваючись патріотичними слоганами, поширювали заклики до перевороту та протестів (Дніпроград).

Кожен із нас чув про інформаційну війну. У соціальних медіа її гарматне м'ясо – тролі. У 1921–1926 рр. ГПУ (Государственное политическое управление) створило фальшиву підпільну організацію білогвардійців «Монархическое объединение Центральной России» (МОЦР). Туди стікалися противники більшовиків. Цю успішну операцію назвали «Трест». Крім того, що вся контра була під ковпаком, завдяки МОЦР вдалося відговорити білу еміграцію від терактів у радянській Росії. Подвійні агенти, хитрі обманні ходи, інформаціний супровід у білоемігрантській пресі з оприлюдненням безлічі версій щодо МОЦР – ось складові успіху.

Створити організацію, до якої увійдуть твої вороги, – чудовий спосіб війни. Він використовується і зараз. За даними українських спецслужб, близько 300 фахівців у Москві займаються вербуванням і кураторством агентів в Україні. Ідеться не лише про гроші й шантаж, а й про нашіптування на вухо потрібним людям.

Але ця стаття про інше – про Інтернет. Тут працювати ще простіше, адже ви не бачите, хто саме наповнює той чи інший акаунт. І знаючи, що хоче почути цільова аудиторія, можна втертися до неї в довіру та проштовхувати вигідні меседжі.

Ми вирахували та візуалізували мережу акаунтів у Facebook, які пов'язані з акаутом С. Мазури. Хто забув – це віртуальний агент впливу, якого викрив «Укрінформ». Він удавав із себе простого українського патріота, який розчарувався у владі, політичних іграх, тому планує творити долю країни на майданах: Майдані 3... За акаунтом С. Мазури тягнувся російський слід – по той бік монітора сидів колишній бойовик російської гібридної армії на Донбасі С. Жук.

Не тільки С. Мазура, а й вся пов'язана з ним соціальна мережа активно закликає до силового повалення влади в Україні. Безумовно, частина цих акаунтів – живі люди зі справжніми переконаннями, жодним чином не пов'язані з Росією. Ми будували мережу на основі зв'язків між акаунтами у Facebook. Якщо ви знайшли себе у нашій візуалізації, це лише привід замислитися: хто ваші друзі у Facebook і наскільки заражені тролями спільноти, в яких ви пишете.

На початку варто визначитися з термінологією. Кого ми маємо на увазі під «тролями»? У нашому розуміння «тролі» – це акаунти живих людей або роботів, яких використовують для політичної пропаганди.

Як створюються тролі?

Як правило, наш троль – це на 80 % програма і на 20 % – людина. Троль-програма робить автоматичні запити про дружбу. З кожним новим френдом троль «товстішає». Особливо його вага в соцмережі збільшується, якщо вдалося подружитися з популярним блогером.

Програма-троль може навіть постити якусь нісенітницю чи обмінюватися лайками з такими ж програмами. Ці дії також збільшують їхню вагу. Але в годину Х, коли потрібно розігнати якусь тему, акаунти тролів починає наповнювати жива людина.

Також живі люди, часто під псевдонімом, модерують групи, де велика концентрація тролів. Цих модераторів ми теж для зручності називаємо тролями. Як і акаунти живих людей, які є впливовими фігурами в нашій мережі і які активно постять чи коментять.

Як це працює? Хтось один із тролів робить пост. Величезна кількість інших починає лайкати, коментити та репостити його. Алгоритм Facebook сприймає це як інтерес живих людей до цього поста. І він починає з'являтися у стрічках НЕ тролів, які колись френднули троля.

Якщо пост вдалий, його починають репостити звичайні люди, а потім підхоплюють журналісти. До слова, за аналогічною схемою розганяються ролики на YouTube.

«Елементом радянського (а тепер російського) інструментарію були так звані "активні заходи" – пряме втручання в політику іншої країни за допомогою прихованих засобів. Активні заходи можуть містити таке:

– вплив на політику інших урядів;

– підрив довіри до лідерів і державних установ у країні;

– розвал її відносин з іншими націями;

– дискредитація та послаблення урядових і неурядових опонентів», – пишуть у своєму аналізі російської пропаганди редактор The Economist Е. Лукас і дослідник П. Померанцев.

Якщо у вас забагато друзів, які поширюють контент тролів, то у вас складеться враження, що «єдиний» спосіб вибратися з безнадії та зради – насильство. Акаунти тролів зовсім не тонко натякають зробити з нинішнім президентом й оточенням те ж саме, що і з попереднім.

Ми зараз живемо у постфактуальному світі, коли значення має емоційне налаштування, а не факти. Тролі працюють з емоціями та конспірологією. Мішень – патріотично налаштовані українці, тобто ті, хто найбільше переймається станом справ у країні.

«Парадоксально, але люди, які не довіряють "традиційним" медіа, є більш схильними споживати дезінформацію, як це показало дослідження Північно-східного університету. Те, що починається як здоровий скептицизм, закінчується пошуком диких конспірологічних теорій», – пише П. Померанцев.

Про подібну до української тактику російських тролів у США писав Е. Чен для The New York Times. Американський троль-патріот – це твіти з національним прапором і нездоровим патріотизмом, приправлений добірними грубими образами на адресу Б. Обами. Те саме що і з очільниками України.

Мережа тролів

Зараз ви побачите як розплутували клубок зради, відслідковуючи мережу тролів-пропагандистів у Facebook. Нагадаємо, що насправді мережа може бути значно більшою. Також існує безліч інших мереж російських тролів, кожна з яких налаштована на свої «цільові аудиторії» у різних країнах світу.

Журналісти почали дослідження з візиту на профілі С. Мазури (М. Гайдука) у Facebook та «ВКонтакте», до сторінок, які, за даними «Укрінформу», він вів. Це «Патріоти України» та «Українська Революція». Згодом були знайшдені інші групи, які у своїй назві мали «Майдан 3» або аналоги. Також узяли в роботу групи, які рекомендував Facebook за цією тематикою. Виявилося, що запеленговані користувачі френдили один одного і неозброєним оком стало видно, що в соціальних медіа існує своєрідна мережа умовного Майдану 3.

Потім було додано адмінів цих груп. У результаті склали список з 29 груп, з них три закриті, тому мережа не враховує дані про активність на їхніх сторінках, лише членство та адміністраторів.

Із загальної кількості друзів адмінів і всіх членів групи відбирали лише тих, хто був членом п’яти і більше груп, хто мав понад п’ять адмінів у друзях, хто написав більше 5 % постів/коментів в одній групі або ж понад 15 у всіх 26 відкритих групах загалом. Потім додали тих, хто зафрендив понад п’ять людей з попереднього списку. Саме ці користувачі в результаті потрапили до мережі. Повторюємо: невелика частина з них – можливо, звичайні люди.

Отож перед вами модель «галактики тролів». Фіолетові – це групи, «інфіковані» тролями, тобто у цій групі багато тролів і вони її адмініструють. Блакитні – це тролі-користувачі.

Розмір кола користувача залежить від кількості адміністрованих груп, написаних постів і коментів, кількості друзів у мережі та членства у групах. Розмір кола групи визначали за кількістю зафіксованих у ній тролів і кількість лінків на неї в мережі. Колір ліній означає тип зв’язків: блакитні – френди, фіолетові – членство в групі і ступінь його активності.

Товщина зв’язку з групою відображає сумарно членство (1), коментування (×2), пости (×3) та адміністрування (×10). Наприклад, якщо троль написав у групі чотири коменти, три пости та є її членом, то сила його зв’язку з нею буде 4×2+3×3+1=18, отже візуально лінія буде товщою, ніж просто зв’язок членства в групі (1).

Клікніть на блакитне коло – і побачите зв’язки персонажа. Клікнувши на фіолетове коло, ви побачите, які користувачі пов’язані з групою. Можна скористатись пошуком і знайти М. Гайдука. При кліку з’являється інформація про вузол: статистика, лінк на сторінку у Facebook і список його зв’язків.

Якщо у мережу потрапила реальна людина, яка не є платним тролем, то точка, яка її позначає, буде невеликою та віддаленою від центра Мережі.

Існують й особливі випадки. Група «Волю в’язням режиму!» переважно складаєтья з реальних людей, вони точно не тролі і НЕ платні пропагандисти. У групі постять фотографії своїх акцій на підтримку активістів «Правого сектору»

й учасників АТО, які зараз мають проблеми з правоохоронцями. Ми не знали про її існування, і знайшли її, досліджуючи зв'язки Мазури–Жука–Гайдука.

Ще одна нетипова група – «Украинский фронт». Це чиста «вата», місиво кремлівських тролів і тих, хто їм вірить. Але нам її порекомендував Facebook, оскільки в ній багато наших друзів-тролів патріотів. І у «ватній» групі, і в радикально-патріотичній є спільні члени, зокрема О. Витязь. Він прихильник Г. Балашова та його партії 5.10.

Акаунти, які потрапили до мережі, визначалися програмою. Частина акаунтів належить звичайним людям, які не є пропагандистами. Вони потрапили до цієї мережі через те, що серед їх друзів багато тролів.

Від Мазури до Гайдука

Розсекречення Мазури–Жука набуло розголосу ще в січні 2016 р., напередодні так званого Майдану 3. Після провалу віртуального агента і Майдану 3, який він пропагував, сторінку С. Мазури видалили.

Зникло ім'я, але справа жива. Зараз про С. Мазуру майже забули. Але відомий волонтер Р. Донік у своєму Facebook написав, що тепер Жук–Мазура діє під псевдонімом «Микола Гайдук».

На відміну від «Укрінформу», нам не довелося зламувати акаунти С. Мазури чи М. Гайдука, але ми точно знаємо, що М. Гайдук став адміном сторінок і груп С. Мазури, виник він дуже раптово та продовжив те саме, що й С. Мазура.

Отже, свідчення Р. Доніка, раптова поява після видалення С. Мазури, «успадкування» його груп і сторінок підтверджують, що по той бік екрану все ще С. Жук. Цікаво те, що Мазура–Гайдук–Жук не найвагоміший персонаж серед «тролів-патріотів».

Мережа Мазури

Активісти слідкували за групами третього майдану у Facebook уже півроку. І це доволі нудне заняття, адже мало що змінюється, окрім профілів користувачів, які наповнюють контент. Кожна група зберігає свою публікаційну активність і має постійних дописувачів. Вони мають і мережу сторінок у «ВКонтакте», проте дещо слабшу, але зараз лише про Facebook.

Рейтинг «зараженості» ви побачите нижче. Наголошуємо, що більшість членів груп, які адмініструються сподвижниками С. Мазури, є звичайними користувачами. Ці групи служать приманками, такими собі онлайн-«трестами».

Як відбирали групи? Якщо адмін, наприклад, «Майдану 3» адмініструє або активно постить в іншій групі, – вона наша.

Список груп складали суб'єктивно, проте ми маємо підстави сумніватися, що це самоорганізовані об'єднання патріотів, бо всі вирахувані групи мають спільні ознаки:

– специфічний контент, який створюють у середньому три людини;
– понад міру заполітизований зміст;
– мало авторських постів, здебільшого лінки;
– низька активність користувачів (мало коментів, лайків);
– подібний контент в усіх групах: репости з одних і тих самих сайтів.

У результаті склали список із 29 груп, з них три закриті, тому мережа не враховує дані про активність на їхніх сторінках, лише членство та адміністраторів. Таким чином було зібрано всю інформацію про кожну групу. Потім почали вираховувати ключових персонажів, і всі вони виявилися пов'язаними один з одним – у віртуальному просторі, зрозуміло.

Хто і як наповнює групи?

Беремо п'ятьох людей, які найбільше постять. Увага! Вони не забувають про конспірацію і часто змінюють свої імена, але id – вічне. Це частина веб-адреси: https://www.facebook.com/profile.php?id=100011309687992. Читаємо їхню творчість.

ТОП-5 тролів, які найбільше постять

Ім'я	Адмін. груп	Коментарів	Член. груп	Постів за два місяці
Татьяна Манина (Tatyana Manina)	0	1	14	637
Anatoliy Trofymenko	0	9	17	440
Микола Яровий	1	0	1	425
Микола Гайдук	1	16	11	338
Ваня Романов	0	1	9	294

Але ті, хто постить, мало коментує. Виявляється, є юзери, що спеціалізуються на коментах. Ми вибрали ТОП-5 найактивніших коментаторів.

ТОП-5 тролів, які найбільше коментують

Ім'я	Адмін. груп	Коментарів	Період
Valera Lapin	1	720	7/01/2016–11/03/2016
Зеновій Шепітько	0	361	01–24/03/2016, +3 коменти 28–29/08/2015
Петро Чайка	1	314	22/02/2016–23/03/2016
Иван Гайдамак	0	220	09/03/2016–21/03/2016
Дмитро Зволінський	0	189	16/06/2015–11/10/2015 – 100 коментів, 89 коментів від 19/01/2016 по 23/03/2016

Живі люди

Дуже цікавим є персонаж Д. Люкшева, адміна «Майдану 3» та «Національного Відродження». Він реальна людина, адмініструє сторінку «Майдан 3.0», також є головою громадської організації «Національне Відродження». На її сайті останнє оновлення датоване серпнем 2015 р. Інформації майже немає, лише декілька новин, переважно із закликами скидати П. Порошенка.

Дмитро вивішує багато особистих фото і дуже вболіває за ідеали Майдану. Серед проектів «Національного Відродження» є арт-терапія для ветеранів АТО, декларується, що вона організована спільно з Солом'янською райадміністрацією.

Але набагато більше уваги він приділяє проекту своєї ГО «Майдан 3», увесь час закликаючи на «безстроковий Майдан». Останнє таке звернення – червень 2016 р.

У Facebook також присутній власник та аміністратор групи «Майдан 3» у «ВКонтакті» – М. Єременко. Незважаючи на виявлений «Укрінформом» зв'язок із С. Жуком, 18 липня М. Єременко виграв перевибори до Коцюбинської селищної ради, балотувавшись від партії «Сила людей». Його активність у мережі тролів Facebook невисока, хоча М. Гайдук є у друзях.

Несподівані знахідки

Чим більше контент, який поститься у групі, чим більше шерять і лайкають користувачі Facebook, тим вищий рейтинг у цьому графіку.

ТОП-3 постів із найбільшим «залученням»

В аналізі соціальних мереж використовують показник рівня залучення (engagement). Це сума коментарів, репостів і лайків публікації. За цим показником вираховується, наскільки успішним є пост. Ми визначили три пости тролів з найбільшим рівнем залучення:

Я – відповідальний президент

Відео, на якому відома журналістка Соня Кошкіна звертається до П. Порошенка із запитанням і реплікою. Він губиться з відповіддю і закінчує фразою: «я – відповідальний президент». Понад 1200 шерів, 339 лайків і 69

коментарів. У коментарях – принизливі репліки, порівняння з фашизмом і звинувачення в бездіяльності.

Країна, що з'їхала з глузду

300 лайків і 1100 шерів, коментарів мало. Суть посту проста і в дусі тролів: як такі прекрасні, гарні ми – українці можуть терпіти жахливу владу, яка чверть сторіччя грабує та гвалтує країну. Пам'ятаєте, що таке «активні заходи» у термінології Москви? Один із них: «Підрив довіри до лідерів і державних установ у країні».

Тепер зацитуємо частину посту (орфографія і стиль збережені): «УСЯ НАША ВЛАДА – БАНДИТИ, ЯКІ ВКРАЛИ ВЛАДУ В НАРОДУ І ЗНИЩУЮТЬ ЙОГО ЧЕРЕЗ ДИКУ ЖАДОБУ НАЖИВИ. Та 42 млн розумних, працьовитих, сильних, вольових людей терплять нелюдські знущання, платять гадинам по диким тарифах, працюють на паразитів за копійки, яких ні на що не вистачає, помирають на дивній війні, яка створена бандитами для знищення найактивніших… УЖЕ ЧАС, ЯК КАЗАВ ТАРАС, ВИГОСТРИТЬ СОКИРУ ТА СПАЛИТИ ВСЮ НЕЧІСТЬ!!!»

Він мені не президент

Фото від однієї з головних тролих – О. Фергюсон. Суть фото в тому, що президент багатіє, народ бідніє, тому давайте щось із ним робити. Більше 780 шерів, лише п'ять коментарів і 159 лайків.

Основні типажі, вони ж ідеальні типи

Типовий учасник Галактики Тролів зазвичай підпадає під один із чотирьох основних типажів.

Портрети, описані нижче, змальовують чималу частину мережі. Це те, що К. Юнг називав архетипами. Знайомі кожному на рівні підсвідомості, закріплені в національній пам'яті універсальні образи. Дієвий засіб маніпуляції.

Перший: РЕВОЛЮЦІОНЕР-РАДИКАЛ, пропагандист насильства. Машингвери-штурмгевери, Українська Україна, внутрішня окупація, національна революція, … чиновників на ліхтарі, за корупцію – розстріл, прийдем – порядок наведем! Чорно-червона гама, культ війни і смерті, ікони Саші Білого і Лісника. Знищимо державу, поубиваємо всіх поганих – і заживемо.

Аватарки – з військовим акцентом. Образ Добровольця або Бійця АТО, або Повстанця. Сучасний козак, тобто з гвинтівкою або елементами кіберпанку, проте неодмінно грізний і з оселедцем. Якщо на аватарці обличчя, то обов'язково закрите хустиною (Повстанець) чи тактичними окулярами (Воїн). Люблять ставити на аватарку козаків і повстанців художника А. Єрмоленка. На сторінці знайдете фотографії зброї, колажі з палаючими будівлями органів влади, заклики до боротьби.

Керівників України зображають негативно. Нюанс: П. Порошенка і В. Путіна ставлять в один ряд. Звичайно, цей типаж не оминає увагою резонансні події, але Президент України – їхня постійна мішень. Ці войовничі тролі часто симпатизують ультраправим політичним рухам і вдають культ С. Бандери.

Частина таких профілів радше є реальними людьми, це стає зрозуміло при візиті на сторінку: волонтерство, багато фото, мало політичних дописів. Але тролі люблять маскуватися під цей типаж.

Другий тип: ПОЛІТИЧНИЙ КОМЕНТАТОР, більше зосереджений не на закликах до революції, а на поточних політичних подіях. Загальний настрій постів: на фото, які вони постять, часто образливі зображення політиків і посадовців, на обкладинці – цитати про зраду та боротьбу. Можна часто зустріти рядки із творів українських літераторів або цитати борців за незалежність різних часів. Часом ВИГАДАНІ.

Зміст сторінки приблизно такий самий, як і в Козака, тільки частина політичного бруду більша. Окремі персонажі, наприклад, П. Чайка, зосереджуються на піарі винятково конкретної політичної сили, найчастіше БЮТ і Ляшка.

Третій тип: ПОКАЗОВІ УКРАЇНЦІ. Особливо популярними є замріяні дівчата у віночках (із жовто-блакитними стрічками або тернових), сукнях-прапорах, вишиванках, на фоні пшениці тощо. Оля Україночка, наприклад. У цього образу є елемент страждання, щось, що нагадує героїнь Шевченка та знедолену Україну. Фотографія, звичайно, тільки одна і занадто професійно відзнята. На змісті контенту це не дуже відображається: усе ті ж посилання з сумнівних сайтів, дискредитація влади, приклади несправедливості та залізні докази того, що «всё пропало».

Четвертий тип, не надто поширений – ХИЖІ ЗВІРІ: вовки, тигри. Не котики! До цього типу належать декілька користувачів, які мають багато зв'язків у мережі. Вони часто адмініструють групи, у них багато друзів, але вони мало постять.

Зовнішні посилання. Куди ведуть лінки?

Наше дослідження не було б повним, якби ми не вивчили, які лінки найчастіше постять тролі. Ні, вони не ведуть на Russia Today. За допомогою FB Netvizz ми дізналися, що більшість постів у групах – ЗОВНІШНІ ПОСИЛАННЯ (сайти, інші групи/сторінки у ФБ). Тролі рідко пишуть самі.

Серед зовнішніх сайтів є і популярні ресурси: 112, Цензор.нет тощо, навіть на наші тексти посилались сім разів. Але невиправдано багато сумнівних, нікому не відомих сайтів.

ТОП-10 сайтів, новини з яких найчастіше розганяють тролі

Сайт	Кількість посилань	Опис
varota.com.ua	2236	Впадає в очі не зловісний контент, а низька якість сайту
amn.com.ua	1384	Контент, на перший погляд, проукраїнський, найбільш позитивно зображують військових, Н. Савченко (дослідження відбувалося тоді, коли вона сиділа). Применшують авторитет більш «мирних» політиків
zvamynews.blogspot.com	1252	«Час новин». Публікують близько п'яти новин на день. На початку червня десь третина контенту була присвячена Н. Савченко
uaexpert.blogspot.com	955	Цей «експертний сайт» не публікує жодних думок експертів, окрім «пророцтво, коли ми повернемо Крим». Багато матеріалів про Росію

Сайт	Кількість посилань	Опис
kozak.co.ua	863	Сайт для справжніх козаків (у степу, з голим торсом, шаблею та вовками), використовує символіку «Правого сектору»
v7ved.ru	794	Типовий сайт новин із дуже нав'язливою пропозицією залайкати його
bbcccnn.com.ua	712	Не читайте Бі-бі-сі, не читайте Сі-ен-ен, їхні матеріали двохмісячної давності разом з контентом попередніх гівносайтів є на bbcccnn.com.ua
followneWs.info	653	Агрегує новини з різних сайтів: від усім відомих «Кореспондента» та «Ліги» до популярної в троляндії «Диванної сотні» та схожих однакових гівносайтів
retrans.in.ua	651	Адреса нагадує відомий агрегатор – сайт, що збирає різні новини
joinfo.ua	600	Адреса нагадує відомий агрегатор – сайт, що збирає різні новини

Троль і пересічний юзер: як відрізнити?

Усе, що ми бачимо, – це профілі у Facebook, ми не могли кожного перевірити особисто. Мережу збирали за суто кількісними критеріями. Є типові ознаки тролів, які принагідно нагадаємо.

Вони мають друзів, їх багато – тисяча, дві, п'ять. Хоча трапляються і так звані несоціальні тролі, у яких по 30–60 друзів.

Типові ознаки несправжніх акаунтів: відсутні особисті фото та хоча б мінімальна інформація про людину, на сторінці мало власних записів, переважно репости про «зрадників», «ворогів» або ж білий шум на кшталт відео про швидкісне зав'язування краватки та миттєвий спосіб схуднути, все це без особистих коментарів і вражень. На початку статті ми писали, що часто тролі – це на 80 % програма, і вона здатна постити такий неосмислений контент.

Більшість користувачів з отриманої мережі мають ці ознаки: ненаповнені сторінки, мало або, навпаки, занадто багато друзів (таких самих, як вони, або популярних користувачів: зустріли в «троледрузях» Ю. Луценко, А. Авакова та інших політиків). У фотографіях та альбомах відсутні реальні фотографії з життя, проте є демотиватори, інколи відмітки на фото з іншим, реальним, користувачем.

У стрічці троля переважають репости, емоційні дописи про зраду, лінки на фото дівчат чи беззмістовні статті. І нічого про реальне життя: важливі події, селфі, фото з подорожей та гулянок відсутні.

Якщо реальна людина потрапила до мережі, на це є підстави.

У неї був активний френд-троль, що додав її у відповідні групи. Тут радимо слідкувати за списком друзів і груп. Звичка всіх френдити – погана, подумайте про ризики, коли додаєте в друзі незнайомців.

І третя причина: людина могла просто повірити у творчість тролів. У цьому випадку варто нагадати, що кібер-світ дає безмежне поле для маніпуляцій, і якщо ти особисто не знаєш людину, то ніколи не можеш бути впевнений у реальності її профіля.

Як прогнозував декілька років тому керівник Google Е. Шмідт у своїй книзі «Новий цифровий світ», створення фальшивих акаунтів у соцмережах

стане одним з найприбутковіших бізнесів майбутнього. Це майбутнє вже настало. Усі, хто має потребу та ресурси, можуть насичувати соцмережі ботами і тролями та з їхньою допомогою пробувати маніпулювати іншими.

Якщо реальна людина потрапила до мережі, на це є підстави.

Де Кремль, а де Майдан, що ви таке кажете?

Складно переконати людину змінити погляди на 180 градусів. «Класична» російська пропаганда не діє на більшу частину українців, адже сильно йде врозріз з їхнім баченням ситуації. Вона радше розрахована на проросійськи налаштовану аудиторію.

Мета інформаційної війни – посіяти безлад і зневіру, позбавити чітких орієнтирів. Зброя в цій війні – дискредитація влади та державних інститутів, адже навіщо «воювати за олігархів».

«Посіяти недовіру між верхами і низами» – один із методів перемоги над ворожою державою. Його описували ще давньокитайські стратеги.

Українські патріоти та добровольці, тобто їхні електронні муляжі, – чудовий засіб для поширення «зради» і закликів до нової революції. І неважливо, що «революціонери» у Facebook пишуть бридоту і про Росію, і Путіна & Co. Невже В. Путіна хвилює, хто, як і наскільки його любить? Певно, що ні, коли це стосується справи.

Контент груп і профілів Facebook у виявленій нами мережі сповнений зневаги та ненависті до української влади та політиків. Тут акцентується увага на несправедливості й проводяться паралелі між В. Путіним та Порошенком–Яценюком–Гройсманом. У цьому контексті прізвище прем'єра чи президента України не має значення. Хто б ним не став, тотальне «мочилово» буде тривати, а аргументація залишиться незмінною.

Як же бути?

І це найважливіше. По-перше – доносити до широкого загалу інформацію про тролів, так само, як про необхідність писати складні паролі і нікому їх не показувати.

Але, крім пропаганди, тролі виконують іншу важливу місію: змушують замовкнути. Не висловлюй свою думку – тебе ж затролять!

Уже тому варто не пасувати перед засмиканим робітником фабрики тролів. Варіант є: скаржимось на їхні акаунти, причому масово. Вони будуть відповідати (як раніше це робили), але хіба реальній людині складно розблокувати акаунт і довести, що фото з музею чи інше не є порнографією або пропагандою фашизму? Для троля розблокувати сторінку – складніше.

Ми у цьому дослідженні й інші ЗМІ у своїх розслідуваннях навели достатньо доказів того, наскільки потужна фабрика тролів. Якість їхнього контенту сумнівна, але це компенсується кількістю. Нічого нового, стара КГБшна школа. На тролів не шкодують коштів. Щоб їх виростити, працюють високооплачувані програмісти та найкращі з московських інтелектуалів.

Українська ж відповідь мізерна. Анонсовані Мінстецем інформаційні війська мають лише 34 тис. лайків у Facebook, а Google на відповідний запит видає жменьку статей про неефективність «військ МінСтеця».

Деяка робота щодо впливу на ворога через соцмережі ведеться військовими, але її масштаби теж не порівнювані з російськими.

Ми не можемо перемогти тролів тролінням, адже російські бюджети на пропаганду все ще космічні. Рецепт простий:

1. Не френдити тролів і не шерити їхні пости та лінки.

2. Якщо ви бачите обурливий та занадто емоційний допис про «зраду», то перед тим, як поширити його, порахуйте до десяти, а потім подумайте: «Чому тут так багато емоцій і слів написаних ВЕЛИКИМИ ЛІТЕРАМИ?»; «Ця інформація зміцнить обороноздатність чи посіє паніку?»; «Як саме можна зробити те, що пропонує занадто емоційний автор?».

3. Відразу баньте акаунти, які поширюють підкреслено агресивну ненависть, навіть до ворога. Скоріше за все вони імітують своє обурення, аби відключити ваш мозок, використати ваші емоції та втертися у вашу довіру.

Псевдопатріотичні тролі набагато небезпечніші, ніж вульгарні проповідники «русского міра». В Україні надзвичайно низький рівень довіри до владних інститутів і силових структур (за винятком Армії), і цим користується ворог.

Але щоб покращити якість управління, важливо шукати причини тих чи інших проблем, змінювати кожну конкретну ситуацію, обґрунтовано критикувати, але не дискредитувати їх ще більше. Немає довіри владі – немає базового порядку. Хаос.

Методологія

Відправним пунктом для збору даних про мережу стали групи «Майдану 3», на які вийшли за даними «Укрінформу». Вони мали «Майдан 3» у назві, у них активно брали участь адміни/активісти груп Мазури–Гайдука, нарешті, їх пропонував Facebook як подібні (і вони мали зміст у дусі «Майдану 3»). Ми вирішили дослідити мережу С. Мазури кількісно: почати з груп, які виділили при ручному пошуку, та отримати список їхніх членів, адмінів, друзів адмінів, пости та коменти у Facebook, джерела новин. Тим паче, що ми маємо справу з особами, які френдять тисячами.

Вручну зібрати дані просто неможливо. Facebook має велику перевагу для користувача і водночас недолік для дослідника: занадто строгі налаштування приватності. Те, що ми можемо бачити щось на сторінці користувача, ще не значить, що це можна завантажити за допомогою API.

Тому збір даних автоматизували модулем «Selenium» для Python. Це інструмент для симуляції, який може керувати роботою браузера. Тобто, є скрипт з інструкціями (зайти на сторінку, залогінитись, перейти до списку друзів/списку членів групи, прогортати його до кінця, дані завантажуються в процесі гортання – технологія AJAX, витягти з коду сторінки імена та фейсбук-id користувачів списку, записати їх у файл, перейти до наступного користувача або групи). Це те ж саме, що збирати дані вручну, заходячи на сторінки тролів, єдина відмінність – купу однотипних кліків і прокруток у звичайному браузері робив Selenium.

Отже, спочатку викачали список адміністраторів і членів груп. Facebook не показує повний список членів групи (наприклад, надає лише 5 тис. з 10), але створений нами бот (знайомтесь, О. Гаврицький: любить футбол, революцію й ультраправі ідеї) додав у друзі кількох важливих тролів, а сам Facebook надає друзів і друзів друзів на початку списку учасників групи. І це підвищує надійність даних.

Надалі завантажили списки друзів адміністраторів груп. Теж варто зважати на обмеження: якщо користувач не відкрив список друзів – його дружні зв'язки не зафіксовані. Потім відібрали лише тих користувачів, які є членами більш ніж п'яти груп або друзями більш ніж п'яти адміністраторів груп. Через додаток у Facebook Netvizz отримали всі пости та коментарі у відкритих групах, через які сформували:

– Список активних дописувачів і коментаторів: тих, хто написав більше 3 % коментарів або постів в окремій групі або написали понад 15 постів чи коментарів загалом у всіх підозрілих групах.

– Перелік сайтів, на які часто посилаються у групах (більше п'яти посилань).

Оскільки Netvizz початково надає анонімні дані, додатково з записів завантажили імена авторів постів і коментарів. Отримавши «список підозрілих тролів» (адміни, активні члени, коментатори та дописувачі), завантажили їх друзів у Facebook. Потім прибрали зі списку тих, хто не мав більше п'яти друзів-тролів. Таким чином сформували перелік усіх ядер і зв'язків мережі.

Відбір груп, завантаження друзів адмінів і членів відкритих груп відбувався у березні 2016 р. Завантаження даних членів та адміністраторів (а отже і їхніх друзів) закритих груп («Майдан 3», «Національне відродження» й «Організаційний комітет третього майдану») відбувалось у червні 2016 р. Дані про контент відкритих груп отримано у листопаді 2015 – наприкінці березня 2016 р. Період залежить від кількості постів у групах, так як завантажували або останні 1000 постів, або більше постів за 1–26 березня (у деяких групах 1000 постів пишуть за кілька місяців, у деяких – за кілька днів).

***

6.10.2016

Львовянина будут судить за пропаганду сепаратизма в Интернете

Жителя Львова будут судить за призывы в Интернете к изменению конституционного строя Украины и захвату государственной власти, сообщает пресс-служба прокуратуры Львовской области (InternetUA).

«Прокуратурой Львовской области направлено в суд обвинительный акт в отношении жителя Львова, подозреваемого в совершении уголовных правонарушений против основ национальной безопасности Украины», – говорится в сообщении.

По данным прокуратуры, уже доказано, что мужчина у себя дома через соцсеть «ВКонтакте» с мая 2014 г. по март 2015 г. проводил незаконную агитационную работу среди пользователей Интернета.

В частности, по информации прокуратуры, он распространял на своей странице посты с призывами к насильственному изменению или свержению конституционного строя и захвату государственной власти, а также к изменениям границ территории или государственной границы Украины.

Мужчине грозит наказание в виде лишения свободы на срок до пяти лет.

***

10.10.2016

Людям для сварки достатьо бота у Twitter, – експеримент

Активістка та художниця Н. Рід провела цікавий експеримент, яким довела, що для того, щоб змусити людей сперечатися, достатньо дурного робота в Twitter (Espreso.tv).

Про це пише Washington Post.

Як експеримент Нора створила двох ботів, які останні три місяці твітили розлогі, в основному ліберальні твердження на кшталт «фемінізм – це добре» або «я думаю, що Д. Трамп жахливий».

Тим, хто починав з ними сперечатися, боти відповідали однією з 18 заготовлених реплік. Це фрази на кшталт «ого», «ти не правий», «загугли це». Незважаючи на те, що такі відповіді не дуже мудрі та провокаційні, безліч людей сперечалось у відповідь.

Що дивного в двох ботах Н. Рід – це те, що вони показують, наскільки відчайдушно деякі люди намагаються вплутуватися в онлайн-суперечки. Бот не використовує хештеги і у нього всього 82 фоловера, а значить, більшість хейтерів, які з ним сперечаються, – це люди, які постійно друкують в пошуковому рядку Twitter спірні теми.

Варто відзначити, що такі онлайн-сварки, навіть коли вони щирі, не змінюють точки зору співрозмовників.

***

12.10.2016

Базиленко Анна

СБУ затримала адміна сепаратистської спільноти, яка провокувала протестні настрої у Дніпрі

Служба безпеки України затримала мешканця Дніпра, який за вказівками російських спецслужб вів антиукраїнську пропаганду в одній з інтернет-спільнот (Watcher).

Як стало відомо, 47-річний адміністратор розповсюджував підготовлені спецслужбами РФ сепаратистські матеріали, спрямовані на загострення суспільно-політичної обстановки в області, провокування масових акцій

протесту, пропагував входження Дніпропетровської області до складу Російської Федерації.

Пропагандист «русского міра» інформував своїх «кураторів» про настрої серед населення та готовність до протестних акцій, пов'язаних із підвищенням тарифів на комунальні послуги. Також вивчав можливість організації проплачених російською стороною мітингів.

Під час проведення обшуку співробітники спецслужби вилучили у зловмисника телекомунікаційне обладнання з доказами протиправної діяльності. Відкрито кримінальне провадження за ч. 2 ст. 110 (посягання на територіальну цілісність і недоторканість України) Кримінального кодексу України. Тривають слідчі дії.

Зарубіжні спецслужби і технології «соціального контролю»

3.10.2016

Росіян запропонували виявляти за IP і штрафувати за скачування піратських фільмів

Влада РФ обговорює можливість введення в Росії системи штрафів для користувачів нелегального контенту (LB.ua).

Про це Rambler News Service повідомило джерело, знайоме з міжвідомчими консультаціями в цій темі.

За його словами, чиновники орієнтуються на досвід країн Європи, де громадяни, які завантажили піратську музику або фільми, сплачують персоніфікований штраф. «Це як платна парковка. Визначають IP-адресу, за якою встановлюють домашню або юридичну адресу, надсилають штраф», – зазначило джерело і додало, що технічна сторона питання повинна бути опрацьована.

Подібну практику сьогодні використовують у Німеччині. Особу, що скачала нелегальний контент, встановлюють за її IP-адресою, після чого можуть оштрафувати на суму до 1000 євро.

***

3.10.2016

У Росії блогера оштрафували майже на 8 тис. дол. за статтю про Сирію

Пресненський суд Москви засудив блогера А. Носика до штрафу в розмірі 500 тис. рублів (7,9 тис. дол.) у справі про екстремізм (LB.ua).

Приводом для порушення кримінальної справи став його пост «Стерти Сирію з лиця Землі» у «Живому журналі», де А. Носик порівнював Сирію з нацистською Німеччиною, повідомляє «Дождь».

«Я з першого дня говорив, що буде штраф», – сказав А. Носик після оголошення вироку.

Раніше прокуратура вимагала засудити блогера до двох років позбавлення волі.

В обвинувальному висновку йдеться, що своєю публікацією блогер «мав умисел розпалювати ненависть і ворожнечу до групи сирійців за національною та територіальною ознакою».

Носик 1 жовтня 2015 р. опублікував у своєму ЖЖ пост під назвою «Стерти Сирію з лиця Землі». У ньому блогер схвально відгукувався про початок російської операції в Сирії, а країну порівнював із нацистською Німеччиною. Під час судового засідання адвокат А. Носика С. Бадамшін стверджував, що його підзахисний лише висловлював свою особисту думку.

Сам блогер заперечував свою провину і стверджував, що Конституція захищає право говорити те, про що він думає. «Ніхто не зобов'язаний мене читати, ніхто не зобов'язаний слухати мене на "Ехо Москви", ніхто з моїх читачів і слухачів не зобов'язаний зі мною погоджуватися», – писав він.

***

5.10.2016

Вас читают: Компания Yahoo сканировала письма для разведки

Yahoo разработала приложение для чтения и анализа входящих сообщений в интересах американской разведки («КОММЕНТАРИИ:»).

Об этом сообщило агентство Reuters, со ссылкой на несколько независимых источников.

Из-за несогласия с решением руководства Yahoo сотрудничать с разведкой, компанию покинул директор по информационной безопасности А. Стэмос, который сейчас занимает аналогичную должность в Facebook.

В комментарии агентству представители Yahoo не подтвердили, но и не отрицали информацию о сотрудничестве с разведкой. «Yahoo – это компания, соблюдающая законы Соединенных Штатов Америки», – заявили представители компании.

Это первый случай, когда американская интернет-компания согласилась передавать поступающие данные. Неизвестно, поступали ли предложения о сотрудничестве другим крупным почтовым интернет-сервисам.

Добавим, бывший сотрудник американских спецслужб Э. Сноуден через Twitter призвал пользователей Yahoo как можно скорее закрыть свои аккаунты, передают «Комментарии».

«Пользуетесь Yahoo? Они тайно сканировали все, что вы когда-либо писали, далеко за рамками закона. Закройте свой аккаунт сегодня же», – прокомментировал Э. Сноуден.

***

5.10.2016

Google и Facebook заявили о непричастности к слежке за пользователями

В компаниях Google, Facebook и Microsoft заявили, что никогда не проводили секретную слежку за пользователями своих почтовых сервисов. Представитель Yahoo, в свою очередь, сообщил, что компания является «законопослушной». Об этом пишет портал Ars Technica (InternetUA).

После информации о том, что компания Yahoo в 2015 г. секретно создала программу для спецслужб США, которая позволяет читать электронные письма пользователей, журналист портала направил нескольким IT-компаниям, в частности Google, Facebook, Microsoft и Yahoo, вопрос о том, помогали ли они спецслужбам читать сообщения их пользователей.

Представители Google, Facebook, Microsoft сообщили, что компании никогда не шли на подобную сделку с американской разведкой. Однако в Yahoo заявили, что компания является законопослушной и подчиняется требованиям законов Соединенных Штатов Америки.

В ответ на историю с Yahoo экс-сотрудник Агентства национальной безопасности США Э. Сноуден написал в Twitter, что те компании, которые не отрицают свою помощь разведке США в чтении переписок пользователей, автоматически можно считать виновными в этом.

***

5.10.2016

В Кремле ликование: Россия якобы обвалила разведсистему США с помощью Microsoft, Facebook и Google

Whatdoesitmean.com, имеющий обыкновение ссылаться на инсайдерские источники информации в РФ, публикует 5 октября данный материал под заголовком: «Russia Collapses Entire US Intelligence System Using Microsoft, Facebook And Google» (From-UA Новости Украины).

Ниже newsstreet.ru приводит перевод статьи.

Очень интересный (и написанный в ликующих интонациях) доклад Федеральной службы охраны, циркулирующий сегодня в Кремле, утверждает, что вся Дирекция внутреннего надзора Соединенных Штатов Америки (DSD) была доведена до почти полного краха разведкой Федерации с использованием американских технологических гигантов Microsoft, Facebook и Google (заключивших «соглашение о шпионаже») для достижения «цифрового цунами», которое показало, что мульти-миллиардный Utah Data Center/дата-центр в Юте (UDC), созданный американским Агентством национальной безопасности (АНБ) всего три года назад, устарел.

Федеральная служба охраны – спецслужба, осуществляющая функции по государственной охране руководства страны и обеспечению их защищенной связью (включая все министерства Федерации), объясняет этот доклад, в то время как миссия Дирекции внутреннего надзора США состоит в том, чтобы

«собирать, обрабатывать и хранить данные граждан США на благо нации», а Центр обработки данных в Юте / Utah Data Center (кодовое название – Bumblehive) описывается как «массивное хранилище данных», предназначенное для работы с огромным увеличением потока цифровых данных, которое обусловлено ростом глобальной сети.

В 2013 г., говорится в этом докладе, Федеральная служба охраны стала «тревожиться», когда секретные документы АНБ были выпущены одним из его сотрудников, Э. Сноуденом, показывая, как крупнейшие технологические гиганты Америки работали в частном порядке с американскими спецслужбами, чтобы шпионить не только за американским народом, но, на самом деле, за всем миром.

После выпуска документов NSA / АНБ Э. Сноуденом, продолжает этот доклад, Федеральная служба охраны приказала всем министерствам Федерации начать использовать пишущие машинки для коммуникации, однако возволила дальнейшее использование Microsoft (Outlook), электронной почты Google и Facebook для «выбранных целей».

И вот президент В. Путин издал указ о полном запрете использования Microsoft (Outlook), электронной почты Google и Facebook.

В 2013 г. Федерация не имела существующего аналога для немедленной замены Microsoft–Google–Facebook коммуникаторов. Аналитики в области компьютерной разведки Федерации раскрыли, что Microsoft дала неограниченный доступ АНБ/NSA к своим зашифрованным сообщениям, Google уже создал тайный союз с АНБ, а Facebook стал идеальным инструментом массового наблюдения как для АНБ, так и для ФБР. И вот, в этой ситуации, Федерация нашла возможность «нанести ответный удар» по американцам.

В 2015 г. было обнаружено, что новая операционная система от Microsoft, Windows 10, не позволяет отключить её автоматическую систему слежки – что позволяет АНБ иметь непосредственный доступ ко всем персональным данным, в том числе содержанию (например, содержание электронных писем, иных личных сообщений или файлов в личных папках) на любом компьютере, на котором была установлена эта операционная система.

Для того, чтобы наилучшим образом проводить слежку со стороны Microsoft–Google–Facebook не только в отношении Федерации, но и всего мира, говорит этот отчет доклад, как сообщил Э. Сноуден, американские аналитики разведки предусмотрели массивное количество «ключевых слов», чтобы пометить то, что они считали подозрительными сообщениями и/или компьютерными файлами.

Как только они узнали это «ключевые слова» АНБ, объясняет этот доклад, аналитики разведки Федерации начали «наводнять» АНБ десятками миллионов электронных писем, файлов и других подобных компьютерных документов на ежедневной основе не только с официальных компьютеров российских министерства с использованием Microsoft–Google–Facebook, но также и со всех других правительств в мире.

Федерация «завалила» АНБ сообщениями с ключевыми словами и их производными, причём не только от правительств, но и из личных и корпоративных компьютеров простых граждан в этих странах, в том числе из Соединенные Штатов Америки, где, по оценкам этого доклада, за последние три года АНБ пришлось пометить почти каждое из писем и/или компьютерных файлов своих граждан как подозрительные в плане «террористических связей», что добавило миллионы файлов в правительственный террористический список.

При том, что АНБ не имеет возможности физически прочитать сотни миллионов (если не миллиардов) документов, которыми Федерация наводнила его сервера, они стали совершенно беспомощными в плане определения, кто настоящий террорист, а кто нет, что не остановило эти американских «шпионов-идиотов» от добавления в их террористический список даже младенцев, как они это сделали с 7-месячным «Бэби Доу» (Baby Doe) в прошлом году.

Относительно того, как именно эксперты разведки Федерации смогли использовать Microsoft–Google–Facebook, чтобы сокрушить АНБ с, буквально, цунами цифровой информации, это остается в строго засекреченной части этого отчета, но интересно отметить новости от 2013 г. относительно Border Gateway Protocol (BGP) hijacking events, позволяющих хакерам подменить IP-адрес другого лица, чтобы перенаправлять трафик таким образом, что принимающая сторона не будет иметь ни малейшего представления, откуда он на самом деле пришел.

В этом докладе делается вывод, что, по оценкам экспертов разведки Федерации, центр обработки данных в Юте, принадлежащий Дирекции внутреннего надзора США, в настоящее время хранит на своих серверах от 4 до 6 млрд Гбайт по сути бесполезной информации и, кроме того, этот поток не прекращается, т. к. сервера ежедневно наводняются огромным количеством документов, а американцы не в состоянии остановить этот поток, либо осмыслить его.

***

6.10.2016

Кримчанина оштрафували за пісню в соцмережі

23-річний хлопець розмістив на своїй сторінці «ВКонтакте» аудіозапис групи «Коловрат», за що був оштрафований на 1000 рублів (Інформаційна агенція «Вголос»).

Про це повідомляє прес-служба прокуратури Криму.

Рок-група «Коловрат» вважається радикальною і в РФ заборонена.

Було порушено справу про адміністративне правопорушення.

***

06.10.2016

ФБР заарештувало «Сноудена номер два»

Федеральне бюро розслідувань (ФБР) США заарештувало співробітника фірми-підрядника Агентства національної безпеки 51-річного Гарольда Томаса Мартіна за підозрою в крадіжці секретної інформації (LB.ua).

За даними The New York Times, він викрав код для злому комп'ютерних систем урядів інших країн, таких як Росія, Китай та Іран, що вважаються зовнішньополітичними опонентами Америки.

ФБР поки не знає, чи встиг Мартін комусь передати вкрадений код.

Арешт відбувся ще в серпні, однак інформацію про те, що трапилося, Мін'юст США розкрив тільки зараз.

Гарольд Томас Мартін працював у тій самій компанії (Booz Allen Hamilton), що й Е. Сноуден. Утім поки що немає ніяких даних про те, що вони знали один одного або хоча б могли зустрічатися.

***

11.10.2016

WikiLeaks опублікував другу частину листування голови штабу Г. Клінтон

Сайт WikiLeaks 10 жовтня опублікував другу частину листування голови передвиборного штабу Г. Клінтон Дж. Подести (LB.ua).

Про це повідомляють на сторінці ресурсу в Twitter.

Опубліковано 2086 листів, датованих 2015 р.

У листах працівники передвиборного штабу Г. Клінтон обговорюють, як відповідати на запитання преси та давати коментарі щодо дражливих тем, одна з яких – публікація книги «Гроші Клінтонів», у якій Фонд Клінтонів звинувачують у сумнівних операціях, зазначає CNN.

В одному з листів колишній радник Б. Клінтона Д. Бенд назвав доньку Гілларі та Білла Клінтон «розпещеною дитиною».

Радник Д. Трампа Д. Міллер опублікував посилання на нові дані WikiLeaks із фразою: «Ну ось і почалося». У штабі Г. Клінтон у відповідь на це розкритикували Д. Трампа за «радість від публікації, організованої В. Путіним».

«Час (публікації файлів) показує, що навіть В. Путін знає, що у Д. Трампа були погані вихідні та погані дебати», – заявив представник Г. Клінтон Г. Каплін.

Це друга частина анонсованих раніше WikiLeaks документів. Першу частину було опубліковано 8 жовтня, вона стосувалася питань ядерної енергетики та пожертвувань до Фонду Клінтон від гірничодобувної та ядерної галузей.

У липні WikiLeaks опублікував майже 20 тис. листів і понад 8 тис. документів Національного комітету Демократичної партії США.

У результаті свій пост покинула голова комітету: з листів стало відомо, що організація всупереч правилам підтримувала під час передвиборної кампанії Г. Клінтон і перешкоджала її суперникові по партії Б. Сандерсу.

Пізніше The New York Times повідомляла, що метадата (інформація про дані) вкрадених зі серверів Демократичної партії США документів і опублікованих на сайті WikiLeaks показала, що їх «пропускали» через безліч комп'ютерів, у тому числі і з російськомовними налаштуваннями.

У п'ятницю, 7 жовтня, США офіційно звинуватили Росію в проведенні широкомасштабної кампанії з втручання у вибори президента США, включаючи злом комп'ютерів Національного комітету Демократичної партії США та інших політиків.

***

11.10.2016

У Туреччині заблокували Google Drive через зятя Ердогана

Турецька влада перекрила доступ до хмарних сервісів, серед яких Google Drive, Dropbox, OneDrive і GitHub (Espreso.tv).

Про це передає thenextweb.com.

Уряд, як вважають, зробив це, намагаючись запобігти витоку електронних листів міністра енергетики і природних ресурсів країни Б. Албайрака, зятя Ердогана.

Витік 17GB, який, як вважають, охоплює 57,623 електронних листів починаючи з квітня 2000 р. до кінця вересня цього року, стався через діяльність хакерської групи Redhack. Рішення влади про блокування хмарних сервісів і про розслідування діяльності групи вказує на справжність витоку.

За даними джерел, які отримали доступ до бази даних, електронна переписка містить відомості про те, як Ердоган використовував свою посаду і владу для впливу на засоби масової інформації та вказівок щодо публікації тієї чи іншої інформації в провладних газетах.

На ранок вівторка 11 жовтня робота сервісів уже відновлена.

***

12.10.2016

Олександр Ліщінський

Роскомнадзор терроризирует интернет-издания и украинских хостинг-провайдеров

Роскомнадзор – преобразившаяся из Россвязьохранкультуры федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, а так же исполнению директив ФСБ по борьбе со свободой слова в Интернете и блокированию неугодных Кремлю сайтов, как в России, так и в Украине. Главной задачей этой федеральной службы является установление информационного контроля в русскоязычной среде глобальной

сети Интернет и отгораживание рунета от всего остального цивилизованного мира путем закрытия доступа к неугодной для власти информации (Четверта Влада).

Примечательно, что в отличии от остальных подобных служб в ведении Минкомсвязи России, Роскомнадзор с момента создания в 2012 г. продолжает показательно имитировать работу и доказывать свою незаменимость в системе государственной программы зомбирования населения, в частности, путем глобальных чисток альтернативных мнений в Сети. Ни для кого уже не секрет, что журналистика в России деградировала до уровня Гебельсовской пропаганды и сталинских СМИ конца 1930-х годов. Нынешняя ФСБ, через тот же Роскомнадзор, активно отсекает от российского информпространства зарубежные издания, пользуясь федеральным законом № 398-ФЗ от 28 декабря 2013 г., который вводит новый порядок незамедлительной блокировки информации во внесудебном порядке. Он позволяет генпрокурору и его заместителям блокировать сайты и домены, содержащие «призывы к массовым беспорядкам, осуществлению экстремистской деятельности, разжиганию межнациональной или межконфессиональной розни, участию в террористической деятельности». В первую очередь, под прицелом недовольства РФ оказались украинские СМИ, ведь именно из них сегодня можно узнать об альтернативном положении дел, как в России, так и на территориях псевдореспублик Востока Украины. Собственно, как и в недавнем прошлом, зубной скрежет российских властей вызывали любые упоминания героев чеченского сопротивления России или героической обороны Республики Ичкерия от российских оккупантов. Ситуации с развитием войны в Ичкерии и конфликтом на Донбассе схожи, как собственно и тотальная фильтрация инакомыслия в РФ, поэтому методику подобного информационного блокирования мы отчетливо можем прослеживать на уже существующих прецедентах, неизменно следующих вместе со всеми военными компаниями России.

Подобные механизмы влияния на население и общественное мнение отрабатывались и совершенствовались десятилетиями для того, чтобы скрывать правду, выдавая желаемое российской властью за действительное, либо же просто ограждая людей от информации. В РФ люди не знают, кого больше бояться – бандитов или полицейских, поэтому у каждого в автомобиле есть бита, видеорегистраторы со всех сторон и по две камеры в каждой руке для вежливых разговоров с сотрудниками ГИБДД, а у пешеходов – ножи и травматические пистолеты (капитализм и вседозволенность, всюду дешёвые проститутки и наркотики). Даже закон о запрете курения в общественных местах никто не соблюдает и полиция на нарушителей не обращает внимания. Зато в рунете – чище, чем где бы то ни было, и строго соблюдается закон, ведь за малейшие нарушения сразу закрывают доступ к сайту на уровне магистральных интернет-провайдеров.

За одно только упоминание о «Яроше» или «Правом секторе» в 2014 г. Роскомнадзор внес в реестр запрещенной информации сайты российских

оппозиционных интернет-изданий «Грани.ру», «Каспаров.ру» и «ЕЖ.ру» и сотни других изданий, публикации которых, по мнению чиновников, содержат призывы к противоправной деятельности и участию в массовых мероприятиях, а по сути просто идущих вразрез с единоверной позицией власти. На этой же волне Роскомнадзор по требованию генеральной прокуратуры внес в единый реестр запрещенной информации блог российского политического и общественного деятеля А. Навального на основании закона 398-ФЗ, позволяющего прокуратуре без решения суда ограничивать доступ к сайтам.

С этой же целью 13 февраля 2015 г. Роскомнадзор отдельным списком назначил «Правый сектор», УНА – УНСО, «Украинскую повстанческую армию» (УПА), «Тризуб им. Степана Бандеры», «Братство» экстремистскими организациями, деятельность которых на территории РФ запрещена решением Верховного Суда и, соответственно, любое упоминание о них в сети нарушает закон об информации, закон о СМИ и закон о противодействии экстремизму.

Тем не менее, работа по борьбе со свободой слова со стороны Роскомнадзора в отношении иностранных сайтов выглядит немного иначе. Если в России Роскомнадзору для закрытия ресурсов достаточно найти просто абсурдные мелкие нарушения на сайтах и объявить их грубыми нарушениями цензурных правил, то прекратить вещание за рубежом довольно проблематично, особенно в условиях открытого военного конфликта с собой же и неприкрытой критике РФ со стороны европейских СМИ. Для этого следует совершенно не замечать нарушений цензурных правил собственными недоСМИ, а так же социальной сети от ФСБ под названием «Вконтакте» и с циничной уверенностью забрасывать редакции украинских изданий гневными петициями о снятии отдельных публикаций под угрозой «бана» издания в «рунете».

Для некоторых изданий рейтинги, посещаемость сайта за счет иностранного читателя и количество просмотров имеют большое финансовое значение, видимо по этому Роскомнадзор еще не заблокировал весь украинский трафик на территории РФ. Все это деньги, но с некоторых пор мы видим, что Кремль с этим не считается, хотя и не дружит с «куполом» если включает Википедию в Единый реестр запрещенных сайтов и грозится отключить Twitter и Facebook.

В 2014 г. по инициативе прокуратуры Роскомнадзором был объявлен запрет отечественного сайта «Аргумент» на территории России. К слову, уголовное дело «о преступлении экстремистского характера» в отношении редакции еще ведется. А попытки прикрыть «Аргумент» предпринимались кремлем не только в России, но и в Украине. Что характерно: в Украине повлиять на сайт и его команду пытались только представители так называемой «пятой колонны» России в нашей стране – например, депутаты ВР от Партии регионов, бизнесмены и «решалы» из окружения В. Медведчука и В. Януковича.

Роскомнадзор в августе этого года заблокировала доступ к сайту Украинского кризисного медиа-центра (УКМЦ) на территории РФ. Основанием

для блокирования стал пресс-релиз по итогам брифинга лидеров крымских татар М. Джемилева, Р. Чубарова и Л. Ислямова об общественной блокаде Крыма, который был опубликован еще 8 сентября 2015 г.

Причем, прокуратура РФ, называя лидеров крымскотатарского народа экстремистами, совершенно забыла, что РФ аннексировала родину коренного народа Крыма. Фактически, претензии генпрокуратуры РФ и Роскомнадзора – это очередной пример наступления на свободу слова, которая осуществляется под тем же прикрытием «борьбы с экстремизмом».

Видимо, экстремисты в Украине – каждый второй, так как за последние несколько лет Роскомнадзором было заблокировано вещание нескольких тысяч только украинских сайтов. За размещение материалов якобы экстремистского содержания был ограничен доступ к сайту издания «РБК-Украина», который в следствии еще и был «забанен» операторами «Akado», «МТС» и «Билайн» по требованию Генпрокуратуры. За комментарий к статье двухгодичной давности, в связи с тем, что данная информация содержит сведения, распространения которых в РФ запрещено, попал под «санкции» Роскомнадзора городской портал Чернигова Gorod.cn.ua. С такой же циничной аргументацией российская аудитория лишилась доступа к сайту украинского волонтерского центра «Миротворец», сайту общественников «Крым SOS», что удивительно, сайт Института национальной памяти Украины тоже был заблокирован за экстремизм, как и многие другие интернет-ресурсы, на свободу слова которых решили наступить кремлевские исполнительные службы.

Ввиду тысячных отказов в различнейших вариациях об удовлетворении требований Роскомнадзора по удалению неугодных России публикаций, в особенности со стороны собственников украинских интернет-ресурсов, Роскомнадзор сформировал «черный список» сайтов и хостинг-провайдеров, которые не реагируют на требования ведомства блокировать якобы противоправный контент. В перечень, являющийся неофициальным, вошли сугубо провайдеры и сайты, зарегистрированные за пределами РФ.

В Роскомнадзоре подчеркнули, что основная цель создания «черного списка» сайтов и провайдеров – информирование владельцев добросовестных ресурсов о нежелательных площадках для регистрации. Роскомнадзор может добиться блокировки IP-адреса, на котором зарегистрирован вредоносный сайт, при этом будет закрыт доступ и ко всем находящимся на том же IP-адресе сайтам, даже если к ним у Роскомнадзора претензий нет.

На деле это получается так – поскольку мало кто идет на поводу у Роскомнадзора и письма в адрес непосредственно собственников сайтов остаются без ответа, ну или же на них следует грубый формат отказа убирать неудобный Кремлю контент, федеральная служба начала терроризировать хостинг-провайдеров в Украине.

Как не странно, шантаж оказывается довольно действенным. В сентябре в адрес информационного издания «Херсонские вести» Visti.ks.ua пришло письмо от ТОВ «Хостинг Украина», которое предоставляет услуги хостинга этому ресурсу, с указаниями требований генпрокуратуры РФ и решением

Заводского районного суда г. Грозного Чеченской Республики о том, что контент херсонского издания несет угрозу информационной безопасности России. В связи с этим сложился некий конфуз – украинский ТОВ «Хостинг Украина» затребовал у украинского издания исполнить решение Чеченского суда не угрожать безопасности России. В случае неисполнения ТОВ «Хостинг Украина» уведомил о разрыве договора по предоставлению хостинг услуг в одностороннем порядке, невзирая на осуществленную «Херсонскими вестями» абонплату.

Все дело в том, что Роскомнадзор осуществляет давление на украинского хостера, угрожая заблокировать функционирование совершенно всех хостов ТОВ «Хостинг Украина» на территории РФ.

И дело здесь даже не в содержании контента интернет-ресурсов, а в цензуре, которую всячески пытается наложить Роскомнадзор на информационные издания в Украине.

Конечно же, это не выход для «Хостинг Украина» – плясать под дудку ФСБшных федеральных служб, ограждая не только российскую аудиторию от информации, способной травмировать их неокрепшие умы, но и украинского читателя, – а чем это не содействие в ведении гибридной войны РФ и не несет ли подобное пособничество угрозу информационной безопасности Украины?

К тому же кому как не специалистам в области интернет-услуг не знать о том, что любые запреты Роскомнадзора возможно обходить как с использованием серверов, находящихся за пределами страны, и не подпадающих под действия системы блокирования, так и через смену прокси-серверов. Например, для браузеров Firefox или Chrome можно установить расширения (плагины), позволяющие обходить запреты Роскомнадзора. Браузер Opera без дополнительных расширений имеет режим «Турбо», при включении которого используется внешний прокси-сервер и обеспечивается сжатие трафика, что также позволяет обходить блокировки действительно заинтересованному читателю.

Спецслужбы РФ уже давно сформировали нужную Кремлю информационную политику, результаты которой принято называть «зомбоящиком», а информационные войска кремлевских троллей качественно поднаторели, участвуя во всех без исключения военных кампаниях РФ. Российские СМИ используют самый маломальский информационный повод в Украине для своих троллей, а при их отсутствии приходится выдумывать распятых мальчиков на Донбассе и что Боинг-777 сбили не их российского «Бука». Поэтому воспринимать всерьез деятельность Роскомнадзора как попытку создания информационной блокады для россиян не приходится, скорее это целенаправленное деструктивное влияние на информационную политику сопредельного государства.

Уступки российским «цензорам» не должны приветствоваться украинскими как частными, так и государственными структурами. И это не только потому, что отец Интернета В. Серф назвал сторонников введения контроля над Сетью динозаврами с крошечным мозгом, а потому, что

продолжать позволять Кремлю обкатывать механизмы по внедрению полной цензуры еще и в Украине недопустимо.

***

11.10.2016

Кіберполіція відстежує IP-адреси всіх, хто критикує владу, – Аваков

А. Аваков, міністр внутрішніх справ України, хотів сказати не зовсім це, проте заявив, що «кіберполіція України стежить за тими з вас, хто критикує владу» (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це пише maidan-ua.livejournal.com.

З юридичної точки зору «аваківці» можуть не тільки визначити вашу IP-адресу, але й отримати повний архів вашого приватного листування в Інтернеті. Якщо Ви в коментарях хоч раз закликали до повалення режиму П. Порошенка, то це – кримінальне правопорушення. Стаття № 109 «Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади», ч. 2 «Публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій».

Кримінальна справа порушується чисто формально для того, щоб надіслати запит адміністрації будь-якої з соціальних мереж з вимогою надати всю інформацію про вас: архів листування та історію IP-входів у ваш аккаунт. «Аваковці» не підуть на масові арешти, адже такі дії ще більше налаштують населення України проти режиму. Мета спочатку інша – не заарештовувати протестувальників, а знати про їхні плани все до останньої деталі.

Тому будьте особливо пильні і не пишіть прямим текстом у приват своїм друзям те, що не варто читати поліцейським. Для конфіденційних розмов використовуйте анонімайзери.

***

12.10.2016

Российские независимые журналисты сообщили о массовом взломе электронной почты

В России совершена атака на электронные почтовые ящики независимых журналистов и экспертов, представителей некоммерческих организаций (НКО), оппозиционных политиков, которую сервисы Google и «Яндекс» опознали как вмешательство спецслужб правительства, сообщает Medialeaks (Телекритика).

По словам специалист по информационной безопасности, консультанта по безопасности Transparency International-Russia А. Шляпужникова и российского активиста, руководителя некоммерческой организации «Образ будущего» О. Козловского, известно об атаке более сотни ящиков.

В частности, О. Козловский сообщил о 16 попытках взлома почтовых ящиков, в том числе своего. Также пытались взломать ящики бывшего шеф-

редактора телеканала «Дождь» И. Клишина, журналиста Д. Костроминой и др. О попытке взлома со стороны спецслужб (так говорилось в предупреждении от Gmail) сообщил и российский журналист Р. Попков.

А. Шляпужников рассказал, что за пять дней до атаки предупредил о ней независимые медиа, НКО, активистов и экспертов, которым помогает на общественных началах. О готовящейся атаке ему сообщили источники. «Хорошо, что все мои подопечные имели фору в пять дней, чтобы подготовиться, и у злоумышленников – только одно попадание, которое мы оперативно пресекли», – сказал он.

Вместе с тем, уточнил А. Шляпужников, неизвестно, сколько случаев взлома не было выявлено. «Более масштабной и системной атаки я не припомню за восемь лет работы», – подчеркнул он.

***

16.10.2016

Черногория заблокировала мессенджеры перед окончанием голосования в парламент

В Черногории, где проходят выборы в парламент, были заблокированы популярные программы для обмена мгновенными сообщениями Viber, WhatsApp и другие подобные серверы вечером в воскресенье, 16 октября (InternetUA).

Сообщается, что распоряжение о блокировке мессенджеров поступило от Агентства в области электронных коммуникаций и почтовых услуг. Причиной блокировки послужило использование подобных платформ в целях «нежелательной коммуникации с пользователями».

По утверждению одного из участников выборов оппозиционной коалиции Демократический фронт (ДФ), данный акт был санкционирован властями Черногории и правящей Демократической партией социалистов, которые опасаются проиграть выборы оппозиции, для того, чтобы затруднить коммуникацию оппозиционно настроенных граждан.

Отключение мессенджеров вызвало бурную реакцию граждан страны. Экс-спикер черногорского парламента Р. Кривокапич обратился с жалобой на нарушение свободы слова и общения в посольство США и в миссию наблюдателей ОБСЕ.

Проблема захисту даних. DDOS та вірусні атаки

4.10.2016

Хакери «положили» Єдиний державний реєстр

На Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців і громадських формувань здійснили комп'ютерну DDoS-атаку (Західна інформаційна корпорація).

Про це повідомив заступник міністра юстиції С. Петухов у Facebook, передає Espreso.tv.

«Реєстр тимчасово частково недоступний, деякі із сервісів не працюють, або працюють із затримкою. Недоступні зовнішні сервіси, як наприклад отримання довідок з нашого сайту, але нотаріуси та реєстратори працюють з системою, хоч і з затримками. Повідомимо, коли він повністю відновить роботу», – написав заступник міністра юстиції.

Він додав, що з цього приводу готують заяву у правоохоронні органи.

У свою чергу, у ДП «Національні інформаційні системи» заявили про успішні спроби блокування атак.

У держпідприємстві уточнили, що Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців і громадських формувань «працює в звичному режимі, однак, поки триває атака, можливі певні складнощі з доступом до реєстру».

***

3.10.2016

Масштабный взлом Yahoo вызывает большое количество вопросов

Глобальный взлом оборудования компании Yahoo вынудил высших менеджеров этого ресурса подозревать в совершённой акции спецслужбы неизвестной страны. Злоумышленникам удалось завладеть важной информацией: именами пользователей, e-mail адресами, телефонными номерами, точных датах рождения, имеющихся резервных электронных адресах, а также проверочных вопросах для восстановления пароля (InternetUA).

По мнению специалистов Business Insider, резонансный взлом компьютерной базы данных интернет-ресурса Yahoo! смог привести к краже данных с 1–3 млрд аккаунтов в Сети. Как удалось выяснить, суммарное реальное число похищенных профессиональными хакерами учётных записей пользователей может составлять не 500 млн, как было официально заявлено специалистами, а до 3 млрд.

Представители Business Insider, делая ссылку на экс-менеджеров среднего звена компании, сумевшего сохранить контакты внутри неё (включая инженеров, которые работают над расследованием взлома баз данных), заявляют о том, что архитектура систем Yahoo! скомпонована таким образом, что при заявленном характере нарушений системы безопасности под удар должен был попасть куда больший объём пользовательских данных.

***

3.10.2016

Аналитики обнаружили в Google Play более 400 вредоносных приложений

Аналитики компании TrendLabs насчитали в магазине приложений Google Play более 400 вредоносных программ. При этом специалисты искали специфические вредоносные программы, например, DressCode, которая не только скрывает опасный код, но и маскирует его (Зеркало недели. Украина).

Этот код активирует скачивание вируса из сети уже после установки приложения на смартфон. Так злоумышленники получают доступ ко всей информации, которая хранится на устройстве. Кроме того, аналитики уделили особое внимание моду Grand Theft Auto V для игры Minecraft: Pocket Edition, который был скачан более 500 тыс. раз. После скачивания и установки мод подключался к серверу злоумышленников. Благодаря этому мошенники могли удаленно подключаться к смартфону и превращать его в точку доступа для удалённых атак на беспроводные сети и устройства.

Стоит отметить, что специалисты Google подтвердили расследование этого эпизода и скорейшее удаление подобных объектов из Google Play. Всего же, по мнению экспертов TrendLabs, в Google Play может содержаться более трех тысяч вирусных приложений. Хакеры нашли способ обходить радар-антивирус, встроенный в магазин, и, несмотря на все усилия Google, продолжают загружать вредоносные программы.

***

4.10.2016

Банкиров предупреждают: биометрические пароли в опасности

Председатель специального комитета британского Казначейства, Э. Тири, призвал банковские регулирующие органы обратить внимание на биометрические пароли (InternetUA).

Он считает, что необходимо разработать систему защиты интересов потребителей. Ведь они уже сейчас активно используют биометрические данные (отпечатки, голос, скан лица) для защиты своих учетных записей, в том числе, мобильных кошельков.

Первые письма касательно этой проблемы уже направлены в два финансовых ведомства Англии. Основная причина беспокойства – незащищенность биометрических данных. Преступники могут относительно легко получить к ним доступ.

Учитывая то, что человек не может изменить свои биометрические данные, как пароль, их безопасность должна быть более совершенной.

Банки также должны предусмотреть процедуру компенсации ущерба через суд. Для этого они механизм работы с биометрическими данными должен быть четко прописан.

***

3.10.2016

Хакери зламали базу інвестиційного банку через відмову розглянути їхні бізнес-пропозиції

База даних каліфорнійського інвестиційного банку WestPark Capital була зламана групою хакерів, які називають себе TheDarkOverlord. Шахраї вимагають від банку грошову винагороду, а в протилежному випадку погрожують оприлюднити дані клієнтів (Finance.UA).

Хакери пред'явили доказ злому, опублікувавши деякі вкрадені файли, де розкрили номери соціального забезпечення п'яти клієнтів банку. Опублікована інформація також містила деякі Угоди про нерозголошення, розміщення акцій, презентації та засекречені контакти.

Видання Hackread повідомляє, що атака хакерів була відповіддю на відмову розглянути вигідні бізнес-пропозиції з боку генерального директора банку Р. Раппапорта. Група готова вести переговори, якщо Р. Раппапорт хоче захистити свій бізнес, цитує хакерів видання.

Якщо банк не захоче вести переговори з хакерами, то йому доведеться заплатити 1 млн дол.., щоб припинити публікацію конфіденційної інформації, згідно з повідомленням.

Група TheDarkOverlord також відома своїм продажем за 770 биткоїнів бази даних про 700 тис. пацієнтів, що належить системі охорони здоров'я та страхування США.

***

3.10.2016

Обнаружен ботнет с трафиком 1,5 Тбит/с из 145 тыс. камер

Мы уже неоднократно отмечали риски информационной безопасности, которые несут в себе устройства Интернета вещей. Например, в конце прошлого года эксперты компании Incapsula выявили целую зараженную сеть, состоящую не из традиционных компьютеров, а из камер видеонаблюдения. Более 900 CCTV-камер было готово к атакам. И это лишь малая часть инцидентов с участием IoT-устройств, зафиксированных в последние годы (InternetUA).

На прошлой неделе новостное издание в сфере информационной безопасности KrebsOnSecurity пострадало от мощной распределённой DDoS-атаки. По оценкам экспертов, это была атака с рекордным потоком 620 Гбит/с, а используемый злоумышленниками ботнет включал в себя домашние роутеры, камеры видеонаблюдения и другие IoT-устройства. Сайт смог возобновить работу только через 24 часа.

Спустя несколько дней жертвой похожей атаки стал французский веб-ресурс. В этом случае атака была ещё более мощной – трафик составил свыше 1,1 Тбит/с. Далее последовала ещё серия атак. Исследователи обнаружили

огромную ботнет-сеть, объединяющую более 145 тыс. камер, которая могла достичь 1,5 Тбит/с.

До событий последней недели самой мощной считалась DDoS-атака, прошедшая в июне с потоком 363 Гбит/с. По словам экспертов, ботнеты с пропускной способностью порядка 1 Тбит/с станут привычным явлением через один-два года. Специалисты раньше уже предупреждали, что IoT-устройства несут в себе высокую опасность и к настройке их защиты производителям стоит отнестись ответственно. Многие такие устройства по умолчанию имеют слабые настройки защиты и легко поддаются взлому. А владельцы этих устройствах могут вообще не подозревать, что они стали частью очередного ботнета.

***

3.10.2016

PayPal заблокировала аккаунты российской компании из-за атаки на серверы США

Представители платежной системы PayPal заблокировали личные и корпоративные аккаунты сотрудников компании King Servers. Второго сентября эксперты ThreatConnect, которая занимается кибербезопасностью, заявили, что атака на национальный комитет Демократической партии США проводилась с серверов российской организации (InternetUA).

Как сообщили в ThreatConnect, шесть из восьми серверов, с которых проводилась июльская атака, принадлежат King Servers. Владельцем компании является В. Фоменко, 26-летний житель Бийска. Он подтвердил, принадлежность серверов, но отметил, что не причастен к взлому и готов к сотрудничеству с американскими спецслужбами.

При этом ни российские, ни зарубежные органы к В. Фоменко не обращались. Он сообщил «Коммерсанту», что сейчас юристы компании ищут способ самостоятельно связаться с ФБР.

***

3.10.2016

Взломавшие базу WADA хакеры опубликовали шестую часть документов

Хакерская группа Fancy Bears обнародовала шестую часть сведений из взломанной базы данных Всемирного антидопингового агентства (WADA). Список с фамилиями спортсменов появился на сайте группы в понедельник, 3 октября (InternetUA).

Хакеры опубликовали данные 20 атлетов из 14 стран. Среди прочих упоминаются олимпийские чемпионы Рио-де-Жанейро – австралийская пловчиха Э. Сибом и британский триатлонист А. Браунли. Все спортсмены,

фигурирующие в списке, получили от WADA разрешение на применение запрещенных веществ в терапевтических целях.

***

3.10.2016
Web-приложения – «ахиллесова пята» кибербезопасности

Когда речь заходит о кибербезопасности, многие пользователи в основном думают о взломах электронной почты, атакующем мобильные платформы вредоносном ПО или утечках данных. Тем не менее, все вышеперечисленное может стать последствием использования уязвимых web-приложений или недостаточно защищенных сайтов, предупреждает эксперт И. Колошенко в своей статье на страницах Forbes. По его словам, скомпрометированные web-сайты являются отправной точкой для начала различных типов атак – от простого взлома учетной записи электронной почты до сложных кибератак (InternetUA).

На сегодняшний день, многие предприятия среднего и малого бизнеса тратят средства на продвижение своих web-сайтов и привлечения посетителей. Проблема заключается в том, что компании чаще обращаются к так называемым хакерам Black Hat, чем пользуются услугами легитимных маркетинговых агентств. По словам эксперта, компании платят за компрометацию сайтов конкурентов и перенаправление посетителей на свои ресурсы.

При желании в Темной паутине можно найти хакерские группировки, специализирующиеся на хищении интернет-трафика. Их услуги значительно дешевле по сравнению со стоимостью законных методов, к тому же они могут скрывать свою деятельность. К примеру, хакеры могут отследить оплачиваемый трафик на ресурс компании и перенаправить его на сайт конкурента.

По данным И. Колошенко, к 2021 г. мировой ущерб от деятельности киберпреступников составит 6 трлн долл. В 2016 г. общий ущерб от вымогательского ПО составил 1 млрд долл.

***

4.10.2016
В библиотеке OpenJPEG обнаружена критическая уязвимость

Исследователи команды Cisco Talos обнаружили критическую уязвимость в кодеке JPEG 2000, реализованном в библиотеке OpenJPEG. Проэксплуатировав проблему, атакующий может выполнить произвольный код на скомпрометированной системе (InternetUA).

Уязвимость CVE-2016-8332 вызвана выходом за границы буфера при разборе записей mcc. Ошибка позволяет выполнить произвольный код при

обработке специально сформированного изображения в формате JPEG 2000 в приложениях, использующих функции OpenJPEG для их обработки.

Уязвимость содержится в версии OpenJpeg openjp2 2.1.1 и затрагивает популярные библиотеки (включая Poppler, MuPDF и Pdfium) для чтения PDF-файлов, использующие OpenJPEG для декодирования встроенных в PDF-файлы изображений. Проблема исправлена в версии OpenJPEG 2.1.2.

***

5.10.2016

Во взломе аккаунта М. Цукерберга заподозрили саудовского школьника-хакера

Американский портал BuzzFeed раскрыл личность хакера, причастного ко взлому Facebook-аккаунта главы социальной сети М. Цукерберга. По информации издания, им стал ученик старшей школы А. Макки, проживающий в г. Джидда в Саудовской Аравии и принадлежащий к хакерской группе OurMine (InternetUA).

Жертвами этой группы в разных соцсетях также стали руководители Google, Uber, Spotify, Pokemon Go, а также актеры Ч. Татум и У. Уоллас.

В августе почта юного хакера 0ahmadmakki0@gmail.com засветилась во время взлома аккаунта У. Уоллас. По адресу электронной почты журналисты вышли на его аккаунт в Instagram. На одной из опубликованных им фотографий за 2013 г. видно, что раньше в описании его профиля стояла ссылка на Our-Mine.net.

В Instagram А. Макки содержится ссылка на его страницу в Facebook, судя по которой подросток всерьез увлекается футболом.

Работники BuzzFeed также обнаружили канал на YouTube, на котором молодой хакер отчитывался о взломе аккаунта президента Sony.

На вопросы издания предполагаемый взломщик не ответил. В OurMine опровергли его причастность к группе.

«Многие думали, что он один из нас, но он – просто фанат. Из-за него все считали, что мы из Саудовской Аравии, но это не так», – пояснили в OurMine.

***

5.10.2016

Хакери зламали сторінку прес-центру шатбу АТО у Facebook

У День незалежності України були зламані сторінки Міноборони та Нацгвардії в Twitter (LB.ua).

Хакери зламали сторінку прес-центру штабу АТО у Facebook.

«Ви були зламані! Прес-центр АТО, пишіть правду, а не брешіть як завжди ви це робите!», – вони написали на сторінці прес-центру.

Зловмисники змінили головне фото та обкладинку облікового запису.

«Ніхто не втече від відповідальності. Брехливі пропагандисти отримають таке ж покарання, як і ті, хто вбиває мирних людей!!! Розплата близька. Задумайтеся!», – написали вони.

Хакери якогось порталу «Спрут» опублікували на сторінці прес-центру штабу АТО матеріали, які «викривають» розслідування катастрофи рейсу MH17 над Донбасом.

***

5.10.2016

Dell EMC устранила шесть уязвимостей в платформе VMAX

Dell EMC исправила шесть уязвимостей в интерфейсе платформы для управления корпоративными данными VMAX, в том числе ряд проблем, позволяющих удаленно выполнить произвольную команду с правами суперпользователя и полностью скомпрометировать систему. Ошибки затрагивают ПО Unisphere для VMAX и приложение vApp Manager (версии 8.0.x – 8.2.x) (InternetUA).

Одна из критических уязвимостей содержится в библиотеке GraniteDS, реализованной в ПО Unisphere для VMAX, предназначенном для управления и мониторинга систем хранения данных. Проблема позволяет неаутентифицированному атакующему извлечь произвольные текстовые файлы с правами суперпользователя.

Компания также устранила две критические уязвимости в приложении vApp Manager для Unisphere, проэксплуатировав которые неавторизованный злоумышленник при помощи специально сформированного AMF-сообщения может выполнить произвольную команду и полностью скомпрометировать систему. Одна из них затрагивает класс GetSymmCmdCommand, вторая – RemoteServiceHandler. В результате успешной эксплуатации последней злоумышленник может выполнить произвольную команду с правами суперпользователя, добавить новую учетную запись администратора и получить полный контроль над системой.

Помимо вышеуказанных, в vApp Manager исправлены три уязвимости, классифицированные как опасные, так как их эксплуатация требует авторизации. Тем не менее, все три проблемы позволяют пользователю с низким уровнем привилегий повысить права на системе и выполнить произвольную команду.

***

6.10.2016

Полиция предупреждает всех пользователей Facebook

В целях предупреждения и пресечения преступлений, совершенных через Интернет, полиция многих стран считает целесообразным предупредить

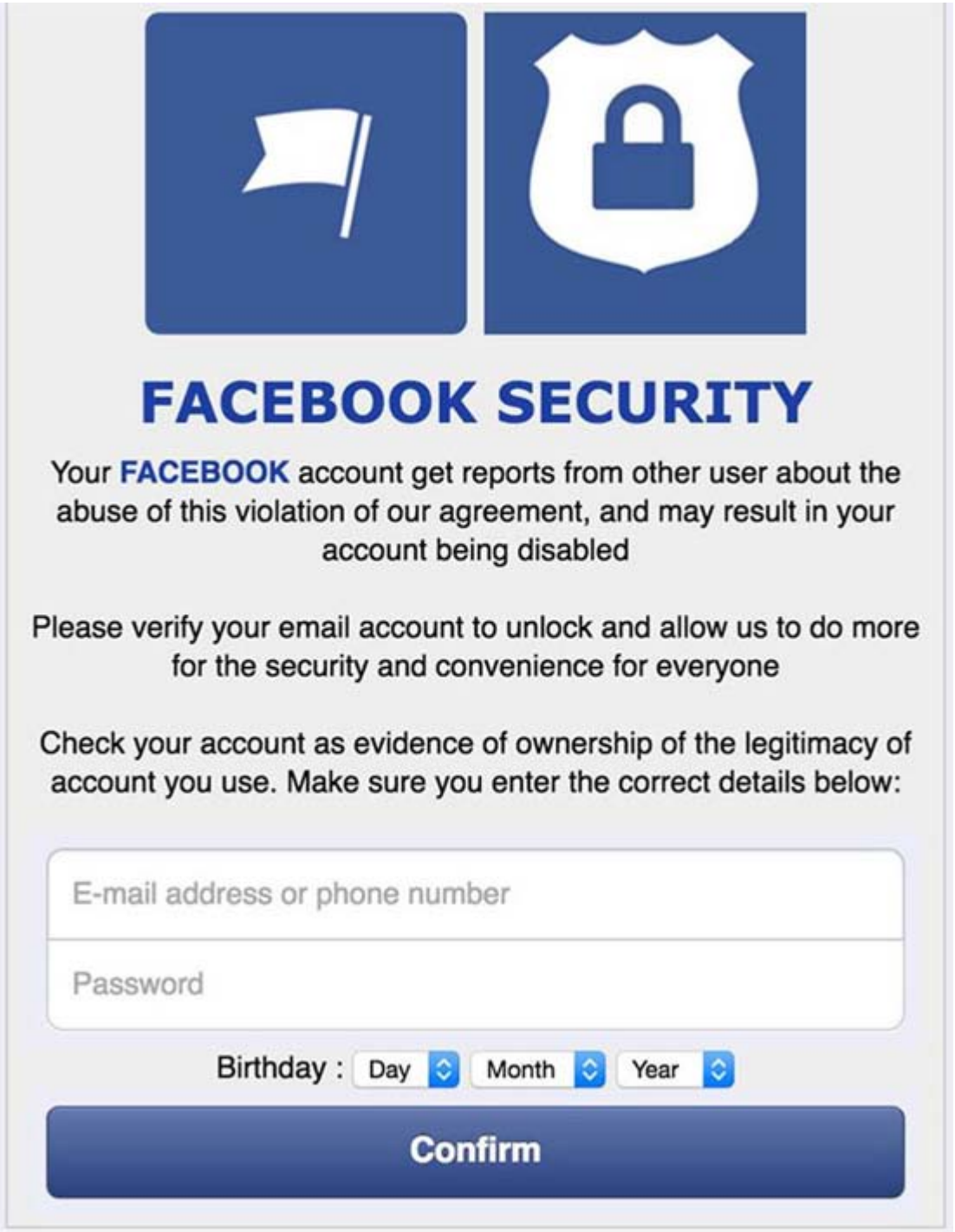
пользователей Интернета об очередном мошенничестве, которое молниеносно распространяется по сети (InternetUA).

Объясним, как защититься от новой аферы, которая крадет личные данные аккаунтов милллионов пользователей Facebook.

Афера проводится таким образом. Вы получаете уведомление от имени Facebook, которое на самом деле не является реальным. Вам его прислали по почте или вы получили личное сообщение, в котором содержится ссылка на страницу, где вас просят ввести имя пользователя и пароль.

Если вы заполнили эти данные – считайте, что ловушка захлопнулась. Будьте очень осторожны, потому что афера основывается на вашем доверии. Вы предоставляете такую информацию, как имя пользователя и пароль в окне, которое выглядит очень похоже на Facebook.

Но на самом деле это способ выманить у вас личные данные. Пошлите это уведомление на Facebook, чтобы в кратчайшие сроки предупредить об афере пользователей. Вот как выглядит сообщение, которое уже получили миллионы пользователей:



Если вы такое сообщение – ни в коем случае не доверяйте этому и не оставляйте свои данные. В противном случае ваш аккаунт будет залит порнографией. Отмеченные в посте друзья, с которыми вы захотите связаться, тоже могут получить этот вирус. Таким образом вероятность кражи личных данных увеличивается в геометрической прогресии.

Этот метод используют хакеры, полагающиеся на добрую волю пользователей. Но теперь, когда вы все знаете, будьте осторожны. А если есть сомнения, обратитесь за советом к тем, кто может помочь.

***

5.10.2016

Микрофон Skype позволяет отслеживать набираемый текст

Ученые из Падуанского и Калифорнийского университетов научились распознавать набираемый текст через микрофон. Атака получила название Skype & Type. Она позволяет злоумышленникам использовать микрофон Skype для отслеживания набираемого текста в других приложениях (InternetUA).

Авторы технологии утверждают, что она способна самообучаться и характеризуется высокой точностью. Разработанный алгоритм способен угадать случайное нажатие с точность 91,7 %, если уже знаком со стилем набора текста жертвы и используемой клавиатурой. Однако если эти параметры неизвестны, точность снижается до 41,89 %.

Отмечается также, что технология работает даже при нестабильном Интернете и способна распознавать даже приглушенные звуки.

***

5.10.2016

Мошенники в Сети оформляют платные подписки в App Store

Антивирусная компания ESET сообщила о распространении новой фишинговой атаки, где мошенники собирают данные банковских карт, рассылая письма от имени App Store (InternetUA).

Потенциальная жертва получает рассылку от лица App Store (на самом деле, мошенники используют почтовый ящик, зарегистрированный на норвежском домене). В письме говорится, что пользователь подписан на сервис YouTube Music Key. Теперь же, как утверждают мошенники, триальный период окончен, и ежемесячная плата за использование сервиса составит 9,55–29,55 евро – в зависимости от подключенных опций.

Мошенники рассчитывают, что адресат попытается немедленно отменить подписку, чтобы избежать обещанного «списания средств». Предполагается, что жертва кликнет на соответствующую ссылку (App Store Payment Cancellation Form) в письме.

При переходе по ссылке пользователь будет перенаправлен на американский домен. На нем размещена поддельная страница «отмены подписки», дизайн которой имитирует оригинальную страницу App Store. Там пользователю предлагается ввести данные карты, чтобы предотвратить списание средств.

Комментируя сообщения о фишинговой атаке, в Apple отметили, что App Store никогда не запрашивает личную информацию и конфиденциальные данные учетной записи (например, пароли или номера кредитных карт) по электронной почте. Электронные сообщения, содержащие вложения или ссылки на сторонние веб-сайты, рассылаются не компанией, хотя может казаться, что их отправителем является iTunes. Ни при каких обстоятельствах не следует вводить данные учетной записи Apple на любых сторонних веб-сайтах.

***

5.10.2016

Уязвимости в Samsung Knox позволяют получить контроль над устройством

Исследователи израильской компании Viral Security Group обнаружили три уязвимости в решении Samsung Knox, призванном «усилить безопасность» операционной системы Android. Специалисты опробовали разработанный ими эксплоит на смартфонах Samsung Galaxy S6 и Samsung Galaxy Note 5 и смогли получить полный контроль над устройствами (InternetUA).

По словам сотрудников Viral Security Group, атака, получившая название KNOXout, работает на гаджетах, подверженных уязвимости CVE-2015-1805, затрагивающей все Android-устройства на базе версии ядра Linux до 3.18. Ошибка позволяет злоумышленнику повысить привилегии и выполнить произвольный код в ядре.

В ходе атаки исследователи смогли повысить привилегии на системе, проэксплуатировав уязвимости в модуле Real-time Kernel Protection (RKP), реализованном в Samsung Knox. При помощи CVE-2015-1805 эксперты смогли обойти защитные механизмы RKP и выполнить код, а также отключить дополнительные механизмы защиты ядра и получить права суперпользователя.

Специалисты Viral Security Group проинформировали Samsung о проблеме. Компания уже выпустила обновление безопасности, устраняющее данную уязвимость.

***

5.10.2016

Ученые разработали новый метод деанонимизации пользователей Tor

Команда исследователей из Принстонского университета, Карлштадского университета и Королевского технологического института (Kungliga Tekniska högskolan, KTH) продемонстрировала новую технику деанонимизации пользователей Tor, предполагающую анализ DNS-трафика из выходных узлов Tor. Метод получил название DefecTor (InternetUA).

По словам соавтора исследования Ф. Уинтера (Phillip Winter), использование Tor не гарантирует полную анонимность. Система имеет ряд ограничений, чем могут воспользоваться злоумышленники с возможностью отслеживания входящего и исходящего сетевого трафика.

Как выяснили эксперты, ряд выходных узлов использует общедоступные DNS-серверы Google, через которые проходит порядка 40 % DNS-запросов, исходящих из сети Tor. По словам специалистов, Google также может отслеживать некоторый входящий сетевой трафик Tor, например, через сервис

Google Fiber или сторожевые узлы, которые периодически размещаются в облаке Google.

Ученые разработали инструмент, получивший название DDPTR (DNS Delegation Path Traceroute), определяющий путь делегирования для доменного имени. Затем программа выполняет трассировку маршрута UDP ко всем промежуточным DNS-серверами. Далее результаты сравниваются с данными трассировки TCP к web-серверу, использующему FQDN. При помощи новой техники исследователям удалось проследить маршрут DNS-трафика и идентифицировать значительное количество посетителей непопулярных сайтов.

***

5.10.2016

Соболев: Вчерашнее отключение е-декларирования было связано с хакерской атакой

Народный депутат («Самопосіч») Е. Соболев заявил, что отключение системы электронного декларирования 4 октября связано с хакерской атакой. Об этом он сказал в комментарии «112 Украина» (Информационное Агентство 112.ua).

Он допускает, что эту атаку организовали государственные служащие Украины, которые не хотят показывать свое имущество.

«Я считаю, что проблемы с системой – это “план Б” для клептократов. Если они не смогут переписать закон, они будут пытаться испортить сайт. Вчера, по моим данным, мы имели фактически хакерскую атаку. И большой вопрос, не это не делается государственными институциями. Не какими-то там агентами В. Путина, или какими-то программистами, а реально нашими государственными служащими. Клептократы будут делать все, чтобы информация исчезала, чтобы сайт ложился, а потом будут в суде говорить “Ваша честь, мы все написали, но там такой бардак был”. “План В” – это Конституционный суд», – сказал Е. Соболев.

***

6.10.2016

НБУ создаст Центр реагирования на инциденты кибербезопасности

Национальный банк создаст Центр реагирования на инциденты кибербезопасности в банковской системе и платежном пространстве Украины. Об этом сообщается на сайте регулятора (Минфин).

«Раньше наши усилия были сосредоточены на отдельных операциях, таких как межбанковские расчеты или операции с платежными картами… Сейчас следует рассматривать проблему надлежащей кибербезопасности значительно шире и сконцентрироваться на обеспечении киберзащиты всего финансово-банковского сектора», – рассказал заместитель главы НБУ Я. Смолий.

НБУ обсудил беспечение кибербезопасности с представителями банковского сообщества, представители киберполиции, Службы безопасности, Государственной службы специальной связи и защиты информации Украины.

Информационный портал Центра должен обеспечить быстрое и надежное взаимодействие между украинскими банками, правоохранительными органами и командами реагирования на компьютерные инциденты субъектов обеспечения кибербезопасности Украины.

«Через эту единую платформу будет происходить централизованное информирование всех субъектов о мошеннических инцидентах и координации действий с их противодействием», – планируют в НБУ.

***

6.10.2016

В ДНР взломана база пенсионного фонда. Выплаты приостановлены

В ДНР взломана и заблокирована база данных «Пенсионного фонда ДНР», а также сайт ведомства. В этой связи пенсионные выплаты в «республике» приостановлены. Об этом сообщают интернет-ресурсы НКТ (РПД «Донецкие новости»).

Председатель «ПФ ДНР» Г. Сагайдакова утверждает, что атаку на базу осуществили украинские хакеры.

Г. Сагайдакова отметила, что к процессу восстановления базы данных привлечены специалисты «минсвязи ДНР», «в самое ближайшее время выплаты будут начислены и выданы жителям республики».

«Пенсионный фонд ДНР делает все возможное, чтобы информация о получателях оставалась конфиденциальной, а также все, чтобы повысить уровень защиты информации о наших гражданах», – констатировала Г. Сагайдакова.

Она считает, что взлом базы был направлен на дестабилизацию экономической ситуации в ДНР. Г. Сагайдакова предположила, что информация базы была необходима украинским властям, чтобы не выплачивать пенсии «гражданам республики», которые смогли оформить выплаты на подконтрольной Украине территории.

***

6.10.2016

Мошенничеством по телефону нередко занимаются осужденные, – глава киберполиции

Осужденные, которые отбывают строк в колонии, нередко оказываются телефонными мошенниками (Podrobnosti.mk.ua).

Об этом сообщил глава киберполиции Украины С. Демедюк в интервью «Сегодня.ua», как сообщает 112.ua.

«Самое распространенное мошенничество – человеку по телефону (обычно через SMS) сообщают о крупном выигрыше (часто автомобиле) и потом под разными предлогами тянут с жертвы деньги. Такими аферами нередко занимаются осужденные, отбывающие срок в колониях, иногда одиночки, но чаще группы из двух-четырех человек. Все, что им нужно – это телефон, несколько сим-карт и интернет-сайт, который можно купить за 100 долл.», – сообщил С. Демедюк.

По его словам, мошенничеством чаще занимаются в больших группах, разделяя сферы деятельности. Нередко в таких группах состоят и бывшие сотрудники правоохранительных органов и банков.

«Мошенники действуют специализированными группами: одна ищет “дропов” (люди, которые отдают свою банковскую карту мошенникам) и занимается фирмами и счетами, другая – сайтами, третья общается с жертвами, четвертая конвертирует и получает деньги… Такие группы разоблачить нелегко, ибо там нередко работают бывшие сотрудники правоохранительных органов и банков, которые знают, как заметать следы. Деньги там вращаются большие», – отметил С. Демедюк.

***

10.10.2016

У Британії міністрам заборонили Apple Watch через російських хакерів

Членам кабінету міністрів Великобританії заборонили носити Apple Watch під час урядових засідань, оскільки на них можуть зробити кібератаки російські хакери (Espreso.tv).

Про це повідомляє The Age.

Хакери можуть використовувати смарт-годинник компанії як прослуховуючі пристрої.

Раніше подібна заборона поширювався на деяких членів уряду країни, коли прем’єр-міністром Великобританії був Д. Кемерон. Наприклад, користуватися гаджетом не мав права глава Мін’юсту країни М. Гоув.

***

10.10.2016

Днепрян пытаются обмануть с помощью «банковских» SMS

С помощью SMS о зачислении денег на карту якобы из банка мошенники выманивают товар у частных продавцов на онлайн-площадках (InternetUA).

Об этом «Информатору» рассказал человек, почти ставший жертвой подобного мошенничества.

Схема работы мошенников проста: они ищут на OLX и прочих онлайн-площадках объявления о продаже дорогостоящих вещей (компьютеров, велосипедов и т. п.), созваниваются с продавцом, уточняют детали и просят

номер карты для перевода денег. За товаром отправляют подставное лицо (чаще всего – таксиста, не подозревающего о «разводе») и присылают продавцу SMS о зачислении нужной суммы на его карту. Сообщение приходит с номера, очень похожего на банковский, отличающегося всего на одну цифру, что можно не заметить, и забирают товар.

***

10.10.2016
Поліція закрила торрент-трекер у Миколаєві

Поліція закрила торрент-трекер, сервер якого був у Заводському районі Миколаєва (LB.ua).

Як повідомляють на сайті поліції, у вересні в обласний відділ протидії кіберзлочинів поскаржилася Українська антипіратська асоціація. Вона заявила про порушення авторських прав особою, яка створила й адмініструє торрент-трекер. Компанії-правовласнику продукції було завдано збитків на загальну суму понад мільйон гривень.

Поліція встановила місце розміщення сервера й особу його власника, провела обшук і вилучила сервер торрент-трекера. Як наслідок інтернет-ресурс припинив роботу.

Кримінальне провадження розслідується за ч. 2 ст. 176 КК України «Порушення авторського права і суміжних прав» (карається штрафом від тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк від двох до п’яти років).

***

10.10.2016
Російські хакери ледь не знищили французьку телекомпанію

Французька телекомпанія TV5Monde була на межі знищення в 2015 р. через кібератаку, в організації якої підозрюють російських хакерів (Espreso.tv).

Про це заявив гендиректор компанії І. Біго, повідомляє BBC.

За його словами, від знищення TV5Monde врятував щасливий збіг. Атака сталася 8 квітня – у цей день був запущений новий телеканал компанії, через що технічні фахівці засиділися в офісі допізна і змогли оперативно відреагувати.

За словами І. Биго, один з фахівців компанії зміг з’ясувати на який саме комп’ютер скоєно атаку. Потім його відключили від Інтернету, зумівши таким чином усунути загрозу.

Спочатку за атаку взяла на себе відповідальність «ІД». Однак пізніше розслідування показало, що за атакою може стояти група російських хакерів APT28.

Мотиви хакерів, за словами І. Біго, залишаються невідомими. Метою хакерів не було шпигунство, а саме знищення телекомпанії.

Наслідки для телекомпанії були дуже серйозними. Вона була змушена знову використовувати факси, оскільки електронні поштові скриньки не працювали. На підключення до Інтернету пішли місяці. Компанія в перший рік витратила близько 5,6 млн дол., а в 2016 р. близько 3,4 млн дол. на заходи щодо захисту.

***

11.10.2016
Роман Черный
Почему контент в Интернете становится вирусным

Пожалуй, каждому пользователю Интернета знаком вирусный контент. Даже если термин вам неизвестен, вы, наверняка, встречались с самим явлением.

Это могли быть вирусные видеоролики, за короткое время набирающие миллиарды просмотров, картинки или тексты, стремительно кочующие между пользователями и социальными сетями. Такой контент поражает Интернет, подобно вирусу. Он очень быстро распространяется, но даже когда первая волна проходит, его не забывают полностью (IGate).

Но что же делает тот или иной контент вирусным? Почему, к примеру, случайно заснятый ролик с чихающим детенышем панды может обойти по популярности куда более профессиональные постановочные видео?

Эксперты считают, что для того, чтобы стать вирусным, контент должен удовлетворять хотя бы нескольким из этих требований.

Эмоциональность

Исследование, проведенное Д. Бергером и К. Милкмен из Университета Пенсильвании, показало, что ключевым фактором становления вирусного контента является эмоциональность. Причем не имеет значения, что это за эмоция. Это может быть умиление, удивление, испуг или даже гнев. Главное – эмоция, которую испытывает зритель, должна быть яркой и искренней. В этом случае пользователь обязательно захочет поделиться увиденным с другими.

Практичность

Еще один тип контента, который имеет шанс на вирусную популярность – нечто очень полезное и практичное. Исследование Бергера и Милкмен продемонстрировало, что пользователи очень часто делятся всевозможными полезными советами и инструкциями из чисто альтруистических побуждений. То есть, человек натыкается на некую полезную статью, и делится ею, поскольку считает, что она может пригодиться кому-то из его знакомых. Этим объясняется популярность в Интернете разнообразных рецептов и лайфхаков.

Удобочитаемость

Вирусный контент – это комфортный контент. Вы можете написать сколь угодно полезную инструкцию, но если она не будет удобочитаемой, она не

станет популярной. Исследователи утверждают, что контент может стать вирусным только в том случае, если он создан достаточно простым для восприятия его девятиклассником.

Эмоционально окрашенные слова

Очень часто вирусный контент имеет в заголовке эмоционально окрашенные слова. К примеру, ролик с названием «Авария на перекрестке улиц N и M» вряд ли привлечет широкое внимание. Другое дело – ролик с названием «Чудовищная авария в городе Z». Конечно, подобную игру словами можно считать манипуляцией. Но такова цена успеха вирусного контента. Кроме того, никакая игра словами не сделает контент вирусным, если его название не соответствует содержанию. И это приводит нас к следующему условию...

Правдивость и правдоподобность

Вы, наверняка, натыкались в Интернете на рекламные статьи с шокирующим заголовком, которые, на поверку, оказывались сообщениями о чем-то невероятно банальном. Как вы думаете, станет ли такая статья вирусной? Конечно же нет, и яркий заголовок в этом никак не поможет. Иными словами, название контента должно соответствовать его содержанию.

Содержание также должно вызывать доверие. К примеру, люди склонны делиться статьями, содержащими ссылки на слова каких-либо экспертов.

Визуальная привлекательность

Красиво оформленное сообщение в социальной сети намного эффективнее обычной ссылки. По статистике, добавление фотографии к твиту повышает его шансы на ретвит на 35 %. Посты в Facebook, содержащие картинки, на 87 % популярнее обычных текстовых сообщений или «голых» ссылок.

Удачное время публикации

Конечно, для контента, уже ставшего вирусным, время публикации не имеет никакого значения. Люди будут делиться им днем и ночью. Но вот для того, чтобы контент всё же стал вирусным, желательно подгадать соответствующее время публикации. Исследование, проведенное порталом Buzzsumo, показывает, что наиболее часто вирусным становится контент опубликованный с понедельника по четверг.

В среднем, пик активности в блогах приходится на 11 утра, а вот почтовые рассылки куда эффективнее в период с 19 до 22 часов. Выходные – не лучшее время для публикации нового контента, но отличное время для репоста чего-то, что уже было опубликовано ранее.

***

11.10.2016

Пользователей Facebook атакует новый троян

Исследователи компании Malwarebytes предупредили о новом трояне Eko, атакующем пользователей Facebook. Для распространения вредоноса злоумышленники используют методы социальной инженерии. Жертва получает

в Facebook личное сообщение от пользователя из своего списка контактов. Сообщение содержит фотографию получателя и ссылку, якобы ведущую на видео с участием самого получателя. Фотография сопровождается надписями «Video» и «xic.graphics» (InternetUA).

После нажатия на ссылку никакое видео, естественно, не открывается, однако через некоторое время пользователю приходит уведомление с предложением установить расширение для Chrome. На самом деле под видом расширения на систему устанавливается троян Eko, распространяющий назойливую рекламу. Вредонос также способен похищать учетные данные (в том числе, для авторизации в банковских приложениях) и рассылать фишинговые сообщения пользователям из списка контактов жертвы.

Первыми с угрозой столкнулись жители Франции, однако затем жертвами Eko начали становиться пользователи и в других странах. В случае инфицирования компьютера трояном необходимо деинсталлировать расширение и изменить учетные данные для авторизации в Facebook и других сервисах.

***

10.10.2016

За большинством кибератак стоят дети и мошенники, а не государство

Несмотря на ажиотаж вокруг так называемых «государственных хакеров», осуществляющих кибератаки по заказу правительства, большинство взломов осуществляют дети и обычные мошенники, уверен ИБ-эксперт Т. Хант (Troy Hunt) (InternetUA).

По словам исследователя, большая часть масштабных утечек данных, о которых стало известно в последнее время, произошли еще в 2012 г. Причины взломов крупных компаний разнятся. «LinkedIn был взломан ради денег, а атаки на Sony и Yahoo! (по ее словам) были спонсированы государством», – цитирует Т. Ханта издание The Register.

По мнению эксперта, несмотря на уверения самой компании, атака на Yahoo! не была осуществлена по заказу какого-либо правительства. «Государственные хакеры стали такой же выдуманной причиной, как “извините, мое домашнее задание съела собака”», – заявил Т. Хант. Напомним, ранее аналогичную точку зрения выразил ИБ-эксперт М. Липински (Michael Lipinski).

Как пояснил Т. Хант, хакеры «сливают» в общественный доступ кеш баз данных (как в случае с LinkedIn), когда их больше никто не хочет покупать. Исключение составляет лишь взлом сайта знакомств Ashley Madison – злоумышленники опубликовали данные пользователей сразу после атаки с целью скомпрометировать виновных в супружеской измене.

Что касается других громких инцидентов, то некоторые из них и вовсе были осуществлены подростками. «Компания TalkTalk пострадала от рук 15-

летнего ребенка, использовавшего свободное программное обеспечение, а не от рук высококлассного хакера», – отметил эксперт.

***

12.10.2016

«Доктор Веб» обнаружил первого энкодера на Go и разработал дешифровку

Вирусные аналитики компании «Доктор Веб» обнаружили первого шифровальщика, написанного на языке Go (ITnews).

Этот троянец, присваивающий зашифрованным файлам расширение .enc, получил название Trojan.Encoder.6491. Специалисты «Доктор Веб» разработали технологию расшифровки поврежденных этой вредоносной программой файлов.

Новые версии троянцев-энкодеров появляются ежемесячно. Trojan.Encoder.6491 интересен тем, что он написан на разработанном компанией Google языке программирования Go: до этого вирусным аналитикам не встречались шифровальщики, созданные с использованием этой технологии. При запуске Trojan.Encoder.6491 устанавливает себя в систему под именем Windows_Security.exe. Затем троянец начинает шифровать хранящиеся на дисках файлы с помощью алгоритма AES. В процессе работы вредоносная программа пропускает файлы, в имени которых содержатся следующие строки:

tmp
winnt
Application Data
AppData
Program Files (x86)
Program Files
temp
thumbs.db
Recycle.Bin
System Volume Information
Boot
Windows
.enc
Instructions
Windows_Security.exe

Троянец шифрует файлы 140 различных типов, определяя их по расширению. Trojan.Encoder.6491 кодирует оригинальные имена файлов методом Base64, а затем присваивает зашифрованным файлам расширение .enc. В результате, например, файл с именем Test_file.avi получит имя VGVzdF9maWxlLmF2aQ==.enc.

Примечательно, что Trojan.Encoder.6491 с определенным интервалом проверяет баланс Bitcoin-кошелька, на который жертва должна перевести

средства. Зафиксировав денежный перевод, энкодер автоматически расшифровывает все зашифрованные ранее файлы с использованием встроенной функции.

Специалисты компании «Доктор Веб» разработали специальную методику, позволяющую расшифровывать пострадавшие от этого троянца файлы. Если вы стали жертвой вредоносной программы Trojan.Encoder.6491, воспользуйтесь следующими рекомендациями:

- обратитесь с соответствующим заявлением в полицию;
- ни в коем случае не пытайтесь переустановить операционную систему, «оптимизировать» или «очистить» ее с использованием каких-либо утилит;
- не удаляйте никакие файлы на вашем компьютере;
- не пытайтесь восстановить зашифрованные файлы самостоятельно;
- обратитесь в службу технической поддержки компании «Доктор Веб» (эта услуга бесплатна для пользователей коммерческих лицензий Dr.Web);
- к тикету приложите любой зашифрованный троянцем файл;
- дождитесь ответа специалиста службы технической поддержки; в связи с большим количеством запросов это может занять некоторое время.

***

12.10.2016

В Украине запускают программу быстрого противодействия кибератакам и карточному мошенничеству

В ближайшее время в Киеве будет запущенна программа немедленного противодействия финансовым мошенникам. Её реализацией займется киберполиция Украины, а также специалисты по борьбе с преступлениями, где используются платежные инструменты (IGate).

Благодаря программе данные о киберпреступлениях будут мгновенно передаваться в общую полицейскую базу, после чего будут оперативно задействованы полицейские для перехвата преступников.

Список преступлений, которые попадают под программу выглядит следующим образом:

– попытки установки на банкомат преступного оборудования;

– зафиксированные факты мошенничества, в том числе с банкоматами (по сообщению граждан, специалистов Ассоциации ЕМА или банков);

– попытки обналичивания средств с карт-подделок;

– попытки расплатиться картой-подделкой в ТСП или в Интернете;

– сообщения о действующих группах мошенников и др.

Киев был выбран первым городом для запуска программы неслучайно, ведь именно здесь чаще всего фиксируются подобные преступления.

***

13.10.2016

Злоумышленники используют платформу WTP для внедрения трояна LatentBot

Платформа диагностики Windows (Windows Troubleshooting Platform, WTP) пополнила список легитимных служб Windows, эксплуатируемых киберпреступниками для распространения вредоносного ПО. Исследователи компании Proofpoint зафиксировали спам-кампанию, в ходе которой распространялся вредоносный документ Microsoft Word, использующий файл .DIAGCAB для инфицирования компьютера жертвы бекдором LatentBot (InternetUA).

После открытия документа на экране отображался бессмысленный набор символов и предупреждение о неправильной кодировке. Для решения проблемы пользователю предлагалось дважды кликнуть на уведомление. Двойной клик запускал файл .DIAGCAB, содержащий набор PowerShell скриптов, загружающих и устанавливающих на компьютер жертвы троян LatentBot.

Как отмечают эксперты, функционально вредоносные макросы и используемые злоумышленниками скрипты «диагностики» практически не отличаются, так как оба позволяют атакующим выполнить серию операций на целевом компьютере. Разница заключается в том, что установленные на устройстве антивирусные решения отслеживают вредоносное ПО, которое может быть загружено вредоносными макросами, тогда как скрипты диагностики по большей части остаются незамеченными.

Платформа Windows Troubleshooting Platform представляет собой средство для выполнения специальных модулей (Troubleshooting Packages), которые создаются на языке PowerShell и призваны решать различные проблемы, касающиеся конфигурации операционной системы, ее отдельных компонентов, устройств, сервисов и приложений.

***

13.10.2016

Глава МАГАТЭ обеспокоен растущей угрозой кибератак на ядерные объекты

Генеральный директор Международного агентства по атомной энергии (МАГАТЭ) Ю. Амано обеспокоен серьезной угрозой кибератак на ядерные объекты. Об этом он заявил в интервью информагентству Reuters (InternetUA).

По словам Ю. Амано, два-три года назад одна из атомных электростанций стала объектом нападения хакеров. Руководитель МАГАТЭ также сослался на инцидент, когда человек пытался провести контрабандой

небольшое количество обогащенного урана, который мог бы использоваться для создания так называемой «грязной бомбы».

«Это не воображаемый риск. К проблеме кибератак на ядерные объекты нужно отнестись очень серьезно. Мы никогда не знаем, владеем мы всей информацией или это только верхушка айсберга», – заметил Ю. Амано.

Руководитель МАГАТЭ отказался раскрыть подробности инцидентов, отметив лишь, что в результате кибератаки работа атомной электростанции не была нарушена. По его словам, ранее об атаке не сообщалось широкой публике.

Опасения, связанные с кибератаками на ядерные объекты, возникли после появления сообщений о вредоносной программе, предназначенной для внедрения в производственные системы управления.

Как утверждает ряд опрошенных Reuters экспертов по безопасности, террористы не смогут подорвать ядерный реактор, однако программное обеспечение, используемое на ядерных объектах, содержит уязвимости, которые могут быть проэксплуатированы.

***

12.10.2016
Adobe закрывает 12 критических уязвимостей Flash

Многие специалисты по информационной безопасности призывают отказаться от технологии Adobe Flash для избавления от лишних проблем, однако компания продолжает поддерживать свой продукт. 11 октября она выпустила очередной патч безопасности, где закрыто сразу 12 критических уязвимостей. В этот же день свои программные продукты обновила компания Microsoft (InternetUA).

Поскольку патч содержит столько важных обновлений, пользователям рекомендуется установить его как можно скорее. Помогли закрыть уязвимости исследователи из компаний Tencent, Palo Alto Networks, COSIG, CloverSec Labs и Trend Micro.

11 из 12 закрытых уязвимостей относились к дистанционному выполнению кода на компьютерах пользователей, что позволяло захватить контроль над ними. Adobe закрыла уязвимость несоответствия типов (Type Confusion, CVE-2016-6992), уязвимости use-after-free (CVE-2016-6981, CVE-2016-6987), повреждения памяти (CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6989, CVE-2016-6990). 12-я позволяет обходить механизм безопасности Flash (CVE-2016-4286). Нет никаких свидетельств того, что эти уязвимости ранее были использованы.

Обновления Flash доступны на Windows, macOS и Linux. Последние версии Flash Player - 23.0.0.185 на Windows и Mac, 11.2.202.637 на Linux.

Были обновлены и другие продукты Adobe. Ими стали Creative Cloud Desktop Application, Adobe Acrobat и Reader. Для Creative Cloud Desktop

Application закрыта уязвимость CVE-2016-6935, позволяющая повышать привилегии в системе. В Acrobat и Reader закрыты 71 уязвимость.

***

12.10.2016

Олеся Блащук

Ассоциация ЕМА назвала три новых сайта, обманом выманивающих у жертв тысячи гривен

Эксперты Украинской межбанковской ассоциации платежных систем ЕМА в рамках программы Safe Card рассказала о трех обнаруженных ими сайтах, созданных для обмана пользователей. Также специалисты объяснили схемы, которые используют мошенники для ограбления украинцев (AIN.UA).

Поддельный платежный сервис pupulca.top

Сайт pupulca.top имитировал платежный сервис для перевода средств с карты на карту и пополнения мобильных счетов. Всего за один день работы сайт обманул более сотни украинцев на общую сумму в несколько тысяч гривен.

Мошенническая схема работает следующим образом: чтобы пополнить счет мобильного или осуществить перевод с карты на карту, пользователь заполняет форму на сайте. В процессе он вводит реквизиты своей карты, включая номер, срок ее действия и трехзначный секретный код (CVV) на обратной стороне карты. Затем фальшивый сервис информирует о том, что операция не успешна. Однако данные карты уже скомпрометированы, и мошенники могут ими воспользоваться.

«Пойманный с поличным» фишинговый сайт стал популярным благодаря контекстной рекламе, повысившей его рейтинг так, что он оказался в первых строках по запросу «пополнить мобильный».

«На иллюстрации – часть файла, который в конце дня получил мошенник (данные стали доступны специалистам ЕМА после обнаружения опасного сайта). Как видим, в файле присутствует информация о картах пользователей, включая трехзначный секретный код, или CVV, указанный на оборотной стороне карты», – сообщили в компании.

Многоликий сервис popolnya.top

По похожей схеме обманывает пользователей и псевдо-платежный сервис popolnya.top. Ресурс уже давно в черном списке фишинговых сайтов, созданном ЕМА, но постоянно возвращается к работе с новым дизайном. В настоящее время работает уже третья версия сайта-мошенника.

Поддельный сервис онлайн-кредитов grenmoney.org

Некоторые сайты выманивают реквизиты карт под предлогом выдачи онлайн-кредита. «Предложения в духе “дайте нам номер карты и получите кредит на минимальную сумму” следует считать подозрительными», – предупреждают в ЕМА.

На http://www.grenmoney.org/ предлагали заплатить всего 6 грн комиссии за каждую тычячу гривен «кредита». Пользователей просили ввести реквизиты платежной карты, якобы для получения займа, а затем сервис под разными предлогами отказывал в кредите. Мошенники же использовали полученные карточные данные для ограбления пользователей.

***

13.10.2016
Хакеры взломали Twitter главы избирательного штаба Клинтон

Страница главы избирательного штаба Х. Клинтон Дж. Подесты в Twitter была взломана хакерами, призвавшими голосовать за ее соперника-республиканца Д. Трампа. Об этом сообщает газета The Hill (InternetUA).

«Я поменял команду. Голосуйте за Трампа-2016», – говорилось в сообщении, которое, как отмечает издание, было быстро удалено.

Информацию о взломе подтвердил пресс-секретарь Х. Клинтон Н. Меррилл, передает The Washington Post. Сейчас на странице Дж. Подесты нет ничего необычного, последнее сообщение датировано 12 октября.

***

15.10.2016
Facebook заплатил хакерам 5 млн долл. за найденные баги

За найденные уязвимости в системе компания Facebook заплатила хакерам 5 млн долл. (InternetUA).

В течение последних пяти лет награды получили более 900 человек. Эту информацию обнародовали в корпоративном блоге компании.

В первом полугодии 2016 г. компания Facebook получила более 9 тыс. отчетов об уязвимости системы. Большинство из них поступили от хакеров из Индии, США и Мексики. За этот период компания выплатила 611,7 тыс. долл., награды получили 149 человек.

Как стало известно, в Facebook решили обнародовать эти данные по случаю пятилетия программы Facebook Bug Bounty program, в рамках которой компания привлекает к поиску багов в своей системе хакеров со всего мира.

***

16.10.2016
Обнаружен «няшный» Linux-троян для IoT-устройств

Как показала сентябрьская DDoS-атака на сайт журналиста Б. Кребса, ставшая самой мощной за всю историю, устройства «Интернета вещей» (IoT) представляют собой плодородную почву для создания ботнетов. Ярким доказательством является ботнет Mirai (исходный код трояна недавно был опубликован в открытом доступе), поэтому неудивительно, что вирусописатели

принялись активно разрабатывать вредоносное ПО для IoT-устройств (InternetUA).

Как сообщает исследователь безопасности MalwareMustDie, в свое время обнаруживший Mirai, одним из новейших троянов подобного рода является Linux/NyaDrop. Вредонос появился еще в мае текущего года, но был очень простым и не пользовался популярностью. Тем не менее, после атаки на сайт Б. Кребса авторы выпустили новую версию NyaDrop.

Как и в случае с большинством существующих в настоящее время вредоносов для IoT-устройств, авторы NyaDrop полагаются на брутфорс-атаки. Злоумышленники находят подключенные к Интернету устройства, а затем подбирают учетные данные из списка дефолтных паролей. Затем запускается скрипт, выполняющий серию автоматизированных команд для загрузки и выполнения NyaDrop.

Размер трояна очень маленький, поскольку он является всего лишь дроппером, загружающим другое, более мощное ПО. Использование дропперов для загрузки – обычная практика для инфицирования десктопных компьютеров, однако для IoT-устройств она применяется нечасто.

Попав на систему, NyaDrop сканирует ее на наличие ловушек (honeypot) и в случае их отсутствия загружает файл с именем «nya» в формате ELF. Загрузка происходит только в случае, если IoT-устройство оснащено процессором на базе 32-разрядной архитектуры MIPS (как правило, это маршрутизаторы, видеорегистраторы, камеры видеонаблюдения и другие встроенные системы).

По словам MalwareMustDie, автором трояна является русский разработчик. Он приложил большие усилия для того, чтобы скрыть свое творение подальше от любопытных глаз. «Добыть образец чрезвычайно сложно. Это большая удача, что мне все-таки удалось узнать, как он работает», – отметил исследователь.

***

16.10.2016

Сайты могут определять сервисы, на которых авторизованы посетители

Немецкий разработчик Р. Волль (Robin Wall) на своей странице GitHub Pages продемонстрировал, как сайты могут снимать «медийный отпечаток», то есть вести учет того, на каких ресурсах зарегистрированы пользователи. Как поясняет специалист, большинство web-платформ могут эксплуатировать механизм аутентификации для определения, залогинен ли пользователь в сервисе. Несмотря на то, что о данной уязвимости известно уже несколько лет, большинство компаний даже не думают ее справлять (InternetUA).

Эксперт пояснил работу эксплоита на примере Facebook. Механизм авторизации работает следующим образом: при переходе по ссылке https://www.facebook.com/bookmarks/pages в инкогнито-режиме, происходит автоматическое перенаправление на страницу авторизации по адресу:

https://www.facebook.com/login.php?next=https%3A%2F%2Fwww.facebook.com%2Fbookmarks%2Fpages.

Параметр http://www.facebook.com%2Fbookmarks%2Fpages – это URL, на который происходит возвращение после завершения процедуры авторизации. Однако, если использовать данный URL для перенаправления на страницу авторизации, когда пользователь уже авторизован на сайте, то он попадет на https://www.facebook.com/bookmarks/pages.

Политика крупных ресурсов не позволяет получать данные самого запроса, поскольку соединение происходит по HTTPS. Тем не менее, возможно получить изображение с домена при указании ссылки на него в login.php?next= . Получить доступ к фотографиям в социальной сети не получится, так как почти все изображения Facebook хранит на серверах по адресу fbcdn.net, однако можно получить доступ к логотипу ресурса – favicon.ico: https://www.facebook.com/login.php?next=https%3A%2F%2Fwww.facebook.com%2Ffavicon.ico.

При помощи простых манипуляций со значками можно собирать данные о том, какими сервисами пользуются посетители сайта без их ведома. По словам Р. Волля, эта атака работает практически на всех крупных платформах, поскольку все они хранят свои иконки на основном домене (Instagram уже удалила иконку со своего домена).

По словам исследователя, такую атаку можно использовать как этап в рамках более серьезных атак, например, деанонимизации, кликджекинга или фишинга.

Соціальні мережі
як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина

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.