СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(31.05–13.06)

2017 № 11

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(31.05–13.06)
№ 11

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 2017

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

2.06.2017
Skype превратился в клон Snapchat

Компания Microsoft модернизировала Skype, заимствовав множество идей у Snapchat и Facebook Messenger. Приложение полностью сменило дизайн, став более красочным, анимированным и «социальным» (IToboz.com).

Новый Skype поделён на три основных раздела: Find, Chat и Capture. В первом можно искать определённый текст из переписки, фотографии, заведения и плагины для добавления контента разных сервисов в чаты. Второй раздел – история чатов и звонков, а в третьем можно найти почти всё, что есть в Snapchat. Пользователям предлагается не просто вести переписку и созваниваться, теперь мессенджер подталкивает их к обмену видеосообщениями, эмотиконами с реакциями (как в Facebook), рисунками и аннотациями поверх фотографий, гифками и стикерами. Обновлённые версии Skype в скором времени появятся на всех поддерживаемых платформах: Android, iOS, Windows 10 и Windows 10 Mobile.

***

2.06.2017
В Twitter теперь можно принимать и отклонять сообщения от незнакомых пользователей

В разделе с личными сообщениями в Twitter появилась вкладка «Запросы». Она позволяет фильтровать входящие и защищает пользователей от оскорбительных и нежелательных сообщений. «Если ваши прямые сообщения открыты, и вам пишет кто-то, на кого вы не подписаны, сообщение появится в запросах, – написала компания. – Через запросы вы можете принять или удалить сообщение. Если вы примете сообщение, то оно появится во входящих» (IToboz.com).

Если удалить сообщение, то в будущем отправитель всё равно сможет вам написать. Чтобы окончательно избавиться от сообщений пользователя, его придётся заблокировать. Если в прошлом вам писал конкретный пользователь, то новые сообщения от него будут появляться сразу во входящих – даже если вы уже на него не подписаны. Если вам пишет незнакомый человек, то прикреплённые файлы от него тоже скрываются. Но картинки и видеоролики можно просмотреть, не принимая сообщение: для этого нужно нажать на кнопку «Просмотреть медиафайл». Нововведение распространяется и на групповые переписки. Если вы прочитали сообщение от нежелательного отправителя, то он не узнает об этом, пока вы не нажмёте кнопку «Принять». Из-за особенностей интерфейса программирования приложений Twitter новая

функция доступна только в официальных клиентах для iOS и Android. В ближайшие несколько месяцев она появится и в веб-версии сервиса.

***

5.06.2017
Стартувала реєстрація в українську соціальну мережу Ukrainians

Від 3 червня реєстрація в українській соціальній мережі Ukrainians відкрита за посиланням www.ukrainians.co. Про це повідомила співзасновниця української соціальної мережі Олександра Струмчинська.

Докладніше

***

5.06.2017
Відома найпопулярніша соціальна мережа серед українців

Заборона в Україні російських соціальних мереж різко змінила смаки користувачів. Ви не повірите, але найпопулярнішою соцмережею став не Facebook (Украинские реалии).

Експерти з TNS Kantar CMeter наводять статистичні дані, згідно з якими, українці найбільше часу тепер проводять на YouTube. Звичайно ж, не варто забувати й про Google, але його складно назвати соціальною мережею. Відповідно, YouTube посунув популярний раніше «ВКонтакте», який тепер посів третє місце в рейтингу, – повідомляють «Українські реалії» з посиланням на maximum.fm.

Додамо, що рекордсменом з відвідувань в останньому місяці весни став сайт Opera. Воно й не дивно, адже цей браузер дозволяє обходити заборону входу в російські соцмережі на території України. За місяць він набрав ще 15,5 % охоплення та увійшов до тридцятки рейтингу.

Доля Facebook зросла на 7,5 %. Тепер мережа Цукерберга посідає четверту позицію замість шостої.

***

5.06.2017
Facebook запустить месенджер для дітей

Соціальна мережа Facebook планує запустити спеціальний месенджер для підлітків (Погляд).

Так, за даними аналізу коду офіційного мобільного додатка соцмережі можна сказати, що йдеться про неанонсований додаток Talk. Ймовірно, це новий месенджер.

Йдеться про те, що додаток дозволяє повністю контролювати свої контакти і, вочевидь, призначений для дітей. Talk дозволить дітям грати в ігри і ділитися фото з рідними та друзями.

Аудиторія буде обмежена користувачами 13 років і трохи старшими. При цьому месенджер не буде вимагати аккаунта в Fcebook, але дозволить батькам контролювати своїх дітей.

***

6.06.2017

С 1 июля Microsoft прекратит поддержку Skype

Microsoft разослала пользователям уведомления о том, что с 1 июля поддержка мессенджера Skype будет прекращена. Сначала решение коснется версий программы для Windows Phone 8 и 8.1, а позднее – Windows RT и Windows 10 Mobile (HiTech-News.ru).

На данный момент Microsoft работает над переходом Skype на платформу P2P. При этом старые приложения прекратят функционировать, что вполне ожидаемо. Еще в прошлом году представители компании объявили о завершении поддержки операционных систем Windows Phone 8 и Windows Phone 8.1. Теперь же IT-гигант откажется и от программ, написанных под эти ОС.

По словам сотрудников Microsoft, версии Skype для вышеперечисленных платформ не пользуются популярностью, их аудитория крайне мала. Что же касается обновленного варианта, он с большой вероятностью понравится большинству пользователей. Этому способствуют не только новые возможности и стабильная работа, но и улучшенный дизайн.

***

7.06.2017

За тиждень у Facebook зареєструвалось ще 300 тисяч українців

Після введення в дію санкцій проти російських соціальних мереж, українська аудиторія Facebook продовжує рости надзвичайно високими темпами. Станом на 7 червня 2017 року, цією соцмережею користувалось вже 8,6 млн українців – про це свідчать дані внутрішньої статистики Facebook для рекламодавців (detector.media).

За перший тиждень червня до Facebook приєднались ще 300 000 українців, пише Watcher.

За методологією Facebook, користувачами соцмережі є люди, які хоча б один раз протягом останніх 30 днів заходили в соцмережу, будучи при цьому залогіненими. Тобто, в цій статистиці не враховуються, наприклад, зареєстровані користувачі, які не заходять в соцмережу протягом останніх 30 днів, а також люди, які не зареєстровані в соцмережі, але переглядають її контент (наприклад, відео).

***

8.06.2017

Украинцы создали соцсеть, построенную на обмене криптовалютой

Украинские стартаперы создали социальную сеть Nimses, похожую на Инстаграм, но от обычной ленты фотографий ее отличает привязка действий к социальному капиталу внутри сервиса.

Докладніше

***

8.06.2017

Число любителей историй «ВКонтакте» превысило 40 миллионов человек

В конце 2016 года социальная сеть «ВКонтакте» предложила вниманию пользователей «Истории» – новый формат общения с друзьями, позволял рассказывать им и подписчикам о происходящих событиях с помощью фотографий, коротких видеороликов с добавлением граффити, стикеров или текста, не публикуя их на своей странице.

Докладніше

***

9.06.2017

Трафік з України в російські соцмережі продовжує падати

Після указу президента України, яким вводилось в дію рішення РНБО про санкції щодо російських соціальних мереж, частина українців почала користуватись VPN-сервісами для обходу заборони (Інформаційна агенція «Вголос»).

Яскравим свідченням цього є зростання трафіку в Рунет одразу після 18 травня з боку користувачів Нідерландів, США та Німеччини – українці почали використовувати VPN сервіси, які перекидають трафік з України в Росію саме через вище названі країни, пише Watcher.

За даними Liveinternet ріст трафіку склав 2,5 млн користувачів. Варто зауважити, що Liveinternet не вміє ідентифікувати одного й того ж користувача, який заходить в інтернет з різних пристроїв. В результаті частина користувачів врахована двічі, а іноді й більше разів. Ймовірно, що реальних користувачів VPN-сервісів є десь від 1,5 до 2 млн.

Чому ж попри очікування багатьох фахівців українці не пішли масово у VPN-сервіси, і частка трафіку з VPN припинила ріст?

Ймовірно на це вплинула тарифна політика мобільних операторів, які мали деякі тарифні пакети 3G-зв’язку, в яких трафік у «ВКонтакте» та «Одноклассники» не тарифікувався. Після блокування операторами доступу до російських соцмереж, використання VPN-сервісів призводило до суттєвого зростання витрат для користувачів на зв’язок. А це для великої частини українців могло стати вагомим аргументом.

До речі, ще один цікавий факт – Україна нарешті поступилась другим місцем Казахстану за кількістю користувачів, які заходять на сайти Рунету (навіть з врахуванням трафіку з VPN-сервісів). І є тенденція до зростання відриву, адже трафік з України продовжує падати.

***

12.06.2017
Соцсеть Ukrainians набрала первые сто тысяч пользователей

Украинская социальная сеть Ukrainians спустя 5 дней после открытия уже насчитывает 100 тысяч пользователей. Теперь разработчики готовятся к расширению функционала. Об этом рассказала соучредитель проекта Александра Струмчинська, сообщает Телеканал новостей «24» (Донбасс).

Пока в Ukrainians можно лишь зарегистрироваться и изменить фотографию профиля. Однако, уже с 22 июня Ukrainians планирует внедрить возможность поиска и добавления друзей, а 30 июня – публикацию контента.

«Сейчас финансированием проекта занимается StartupSoft, но мы также рассматриваем возможность привлечения инвестиций в будущем», – сказала А.Струмчинська.

***

12.06.2017
Ольга Мінченко
Як перетворити «лайк» на веселку у Facebook?

Можливо, ви вже помітили, що у Facebook під деякими постами окрім вже звичних реакій «лайк», «хаха», «серце» і т.д., почали з'являтись реакції у вигляді «веселки». В такий спосіб Facebook пропонує долучитись до Pride Month, який традиційно відбувається у червні (Watcher).

Як перетворити «лайк» на веселку у Facebook?

Щоб увімкнути можливість лайкати веселкою, необхідно перейти на сторінку fb.com/LGBTQ та лайкнути її.

Веселка буде доступною протягом місяця.

Facebook також пропонує долучитись до Pride Month шляхом додавання веселки до вашої картинки профілю. Для цього можна скористатись фото-рамкою.

***

12.06.2017
Facebook определит настроение пользователей в режиме онлайн

Facebook приобрела два патента на технологии, способные распознавать настроение пользователей соцсети. Как уточняет портал CBInsights, компания может использовать для этого несколько способов (InternetUA).

Фронтальная камера мобильного устройства или ноутбука будет делать серию фото во время посещения Facebook, чтобы распознать эмоции в режиме онлайн. Кроме того, разработчики получат информацию о том, как быстро и с какой силой нажимает на кнопки пользователь, меняет ли шрифт и какие смайлы добавляет в текст поста или комментария.

Что это даст? Если соцсеть определит, что вы испытываете радость, глядя на фото друзей или, например, кошек, в ленте появится больше именно этого контента. А количество негативной информации уменьшится.

В Facebook пока не подтвердили намерение использовать эти технологии. «У нас есть ищут патенты на технологии, которые мы никогда не будем использовать, так что их покупку не следует воспринимать как указание на будущие планы», – прокомментировал представитель компании изданию Independent.

***

12.06.2017

Facebook разработала карты для помощи жертвам бедствий

Facebook работает с тремя всемирно известными гуманитарными организациями над новыми картами, которые призваны помочь в борьбе с последствиями катастроф. Эти организации – ЮНИСЕФ, Международное движение Красного Креста и Красного Полумесяца и Всемирная продовольственная программа.

Докладніше

***

13.06.2017

Facebook значительно ускорила тренировку моделей компьютерного зрения

Facebook нашла новый способ тренировать модели компьютерного зрения, который должен значительно ускорить работу компании с искусственным интеллектом. С помощью новой техники Facebook может натренировать модель классификации изображений за час, не навредив её точности.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

6.06.2017

Смерть и больничные слезы: в Украине начался флешмоб в поддержку медицинской реформы

В сети набирает обороты флешмоб в поддержку медицинской реформы. Сотни людей начали рассказывать свои истории о печальном опыте лечения, о том, как на их глазах умирали их дети, родители, родственники, друзья. И добавляя, что систему нужно менять, чтобы таких ситуаций больше не повторялось (Экономические известия).

***

5.06.2017

Українці через Facebook вимагають від Ради медичну реформу

6 червня Верховна Рада має проголосувати за включення до порядку денного низки законів, які стосуються впровадження медичної реформи в Україні («КОММЕНТАРИИ:»)

Користувачі соцмережі Facebook вирішили підтримати впровадження в країні медреформи флешмобом, повідомляє Depo.ua.

Під хештегом #вимагаю_медреформу українці публікують свої відносини із вітчизняною системою охорони здоров'я.

Ініціатором виступив співзасновник Prometheus Іван Примаченко.

Здебільшого озвучуються випадки дачі хабарів, невстановлення правдивих діагнозів та лікарського свавілля.

***

7.06.2017

Вінничан запрошують долучитись до флешмобу на підтримку медреформи

Флешмоб у соціальній мережі #Вимагаю_Медреформу презентував Прем'єр-міністр України на своїй сторінці у мережі Фейсбук (Vinnytsia PressPoint).

«Продовжуючи тему реформи охорони здоров'я. Флешмоб #Вимагаю_Медреформу, який останніми днями поширюється в мережах, став найкращим індикатором проблем медичної сфери в Україні, з якими щодня стикаються сотні тисяч українців.

Сьогодні у нас є реальний шанс змінити стару корупційну систему та провести якісну медичну реформу, головне покликання якої – турбота про здоров'я українських громадян. І навколо цієї мети ми усі маємо об'єднатись!»

***

5.06.2017

Українці у соціальних мережах поширюють новий флешмоб

За допомогою флеш-мобу збирають гроші на допомогу дітям, які мають онкологічні захворювання (0352.ua - сайт міста Тернополя).

У соціальних мережах поширюють новий флешмоб MoneyCanChallenge. Його мета – збирати кошти на допомогу дітям, які мають онкологічні захворювання.

Щоб приєднатися до флешмобу, потрібно обрати грошову банкноту, яку ви готові пожертвувати, зігнути її навпіл та сфотографувати, зіставивши з власним обличчям. Фотографії необхідно опублікувати у Фейсбуці чи Інстаграмі з хештегом #moneycanchallenge та вказати трьох друзів, яким передається виклик. Якщо хоча б одна зі згаданих осіб приєднується до флеш-мобу – кошти потрібно перерахувати на рахунок благодійного фонду «Таблеточки», що захищає інтереси дітей, які мають онкологічні захворювання.

«Ми хочемо дружно відзначити початок літа та подарувати його тим, хто зараз хворий і потребує допомогти, тим, хто проведе своє літо в лікарні, але завдяки нашій допомозі отримає багато літніх днів у майбутньому», – пише команда фонду.

***

13.06.2017

Підслухано у соцмережі, або Про що кажуть 84 тисячі лайків нардепів

Роман Супрун, керівник проекту PolitEyes

З поширенням використання соцмереж, зокрема Facebook, позиції парламентських фракцій стало визначати значно легше. Варто лише стежити за їх лайками – і все видно як на долоні.

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

1.06.2017

Ольга Мінченко

Закриваються офіси українських представництв «ВКонтакте», Mail.ru та «Одноклассники»

Введені Україною санкції щодо російських компаній примусили Mail.Ru Group прийняти рішення про закриття своїх офісів в Україні – повідомив гендиректор компанії Борис Добродєєв (Watcher).

«Наявність представництва на ринку втрачає сенс з урахуванням тих санкцій, які ввела Україна проти нас», – пояснив гендиректор Mail.Ru Group.

До Mail.Ru Group входить низка відомих онлайн-ресурсів, в т.ч. соцмережі «ВКонтакте» та «Одноклассники» і поштовий сервіс Mail.ru.

***

5.06.2017

Google будет отслеживать оффлайн-покупки, совершенные через банковские карты

Google намерен отслеживать расходы кредитных и дебетовых карт в розничных магазинах, чтобы оценить, как онлайн-реклама влияет на продажи. Об этом сообщает Banks.eu (Минфин).

Google Attribution позволит рекламодателям узнать, насколько эффективно онлайн-реклама стимулирует оффлайн-продажи. Новая функция предоставляет технической компании доступ к данным 70 % всех операций с кредитными и дебетовыми картами в США.

Компания планирует отслеживать стоимость всех покупок в течение определенного периода времени, без доступа к деталям об индивидуальных затратах. Что касается конфиденциальности, данные, собранные в результате посещения магазина, а также данные о местоположении, останутся анонимными и не будут переданы рекламодателям.

Новая функция не является обязательной. Пользователи могут отказаться от обслуживания, перейдя на страницу своих настроек и сняв флажок, рядом с пунктом: «Использовать информацию учетной записи Google для персонализации рекламы на веб-сайтах и в приложениях и сохранять эти данные в своей учетной записи Google».

Услуга доступна только в США, но есть планы по ее расширению в Европу.

***

9.06.2017

Google і Facebook шукають менеджерів для взаємодії з російською владою

Компанії Facebook і Google відкрили вакансії менеджерів по взаємодії з російською владою (detector.media).

Відповідні оголошення з'явилися на сайтах компаній. У вакансії Facebook йдеться, що новий працівник має займатися розробкою проектів в області державної політики, вивчатиме російське законодавство та спілкуватиметься з представниками влади та іншими організаціями. При цьому, працюватме менеджер у варшавському офісі Facebook.

Google шукає кандидата, який буде взаємодіяти з урядом і регулюючими органами, а також керуватиме стратегією компанії і займатиметься «правилами використання сервісів компанії в Росії». Менеджеру Google запропонують роботу в московському офісі Google.

***

12.06.2017

Facebook: пользователи заходят в сеть во время рекламных пауз на ТВ

Компания выпустила новое исследование, проанализировав активность группы пользователей во время просмотра сезонной премьеры сериала. Во время каждой рекламной паузы группа из 537 респондентов обращалась к Facebook. К примеру, в то время как от 7 до 11 % пользователей активно пользовались сетью во время просмотра премьеры, от 13 % до 25 % заходили в сеть во время рекламных пауз. (от 9 до 13 % были активны в сети до и после сериала). Среди тех респондентов, которые не смотрели премьеру, активность оставалась низкой – от 8 до 10 %. В блоге Facebook представитель компании отметил, что «важно помнить следующее о видео-рекламе в эпоху мобильных девайсов: смартфоны не являются уменьшенной копией телевизоров. Как ТВ не было визуальным радио, и радио – аудио-газетой, так и мобильные девайсы должны признаваться новым медиа, которое требует нового контента, основанном на опыте, присущему платформе: скорость, выбор и релевантность». Также Facebook представил данные, как пользователи смотрят видео в самой сети. Компания обнаружила, что пользователи смотрят видео с автопроизведением в три раза дольше, чем аналогичную видео-рекламу: 16,7 секунд против 5,7 секунд. Напомним, в этом месяце Facebook откроет собственную лабораторию по маркетингу в Нью-Йорке, где позволит брендам, агентствам и медиа-партнерам лучше узнать, как пользователи используют мобильные девайся и большие экраны (Marketing Media Review).

***

13.06.2017

Ольга Карпенко

Александр Колб, Promodo: Блокировки отбросили нас на 6 месяцев в развитии, оборот упал на 15 %

В середине мая президент подписал указ о блокировке российских интернет-ресурсов в Украине. В первые же недели после блокировки объем украинского трафика на такие ресурсы просел вдвое. Мы ранее уже писали о том, как блокировка «Яндекса», «ВКонтакте» и Mail.ru повлияет на украинский средний и малый бизнес. Чтобы узнать, как это отразилось на отдельных компаниях, редакция AIN.UA поговорила с Александром Колбом – директором известного украинского маркетингового агентства Promodo.

Докладніше

***

13.06.2017

Соцмережа Ukrainians хоче монетизувати контент користувачів без розміщення реклами

Українська соціальна мережа Ukrainians, яка створюється командою з 30 програмістів із канадської компанії StartupSoft разом з українкою Олександрою Струмчинською і поки що працює в режимі реєстрації, збирається надати користувачам можливість монетизувати унікальний контент. Про це Струмчинська розповіла в інтерв'ю LIGA.net.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

8.06.2017

Соцмережі викликають клінічну депресію у підлітків

У недавньому американському дослідженні, опублікованому в журналі Pediatrics, зафіксовано значний стрибок захворювання на депресію у юних дівчат за останні 6 років. Вчені пов'язують цей факт зі зростаючою залежністю від соціальних медіа у цій віковій групі.

Докладніше

***

9.06.2017

Появился первый бот-психотерапевт, который поможет справиться с депрессией

Галина Струс

Бот-психотерапевт Woebot, согласно медицинским исследованиям помогает людям преодолеть симптомы тревоги и депрессии. «Поговорить» с сетевым стартапом можно через Messenger в соцсети Facebook.

Woebot – это стартап о разработчиков из Сан-Франциско. Создатели уверяют, что бот-психотерапевт помогает людям справится с депрессией два раза быстрее, чем обычная терапия в реальности. Это подтверждают медицинские исследования. Об этом сообщает Naked Science.

Сообщается, что в тестировании эффективности Woebot приняли участие 70 студентов в возрастной категории 18-28 лет. Молодых людей в случайном порядке разделили на две группы – экспериментальную и контрольную. Первой предоставили доступ к общению с ботом-психотерапевтом в течение двух недель. Вторая группа получила для изучения журналы Национального института психического здоровья на тот же период.

Спустя 14 дней студенты, которые все это время общались с Woebot, заявили о значительном снижении симптомов тревоги и депрессии, по сравнению с контрольной группой.

Маніпулятивні технології

8.06.2017

Российские журналисты узнали, куда тянутся нити управления ботами и троллями в соцсетях и на сайтах

Как устроен рынок «серого трафика» в российских СМИ, и почему об этом не принято говорить. Об этом в расследовании российской «Новой газеты».

Докладніше

***

13.06.2017

Дарина Шварцман

Более половины украинцев называют онлайн-медиа и соцсети главными источниками пропаганды

Почти 55 % украинцев считают главным источником российской пропаганды онлайн-медиа и социальные сети. Таковы результаты общенационального исследования «Осведомленность и отношение к проблемам дезинформации и пропаганды в СМИ», инициированного проектом StopFake.

Докладніше

***

12.06.2017

Спецслужбы РФ использовали «ВКонтакте» и «Одноклассники» при подготовке к вторжению в Украину – СБУ

Российские спецслужбы активно применяли информационно-психологические операции против нашей страны через соцсети «ВКонтакте» и «Одноклассники» в период подготовки к военному вторжению. Как сообщает УНИАН, об этом во время круглого стола в Киеве сказала замначальника департамента контрразведывательной защиты в сфере информационной безопасности СБУ Юлия Лапутина (Телекритика).

«Период подготовки к военному вторжению сопровождался активным применением спецслужбами РФ специальных информационных и информационно-психологических операций против Украины. В частности, путем создания, администрирования, искусственного наращивания

посещаемости антиукраинских и пророссийских групп в украинском сегменте российских соцсетей «ВКонтакте» и «Одноклассники»», – рассказала она.

По словам Лапутиной, значительная часть этих групп администрировалась с территории России, также применялись меры привлечения спецслужбами РФ граждан Украины, которые, в некоторых случаях за денежное вознаграждение, проводимое через сервис «Яндекс.Деньги», «осуществляли акции во вред территориальной целостности, суверенитету и безопасности Украины».

***

13.06.2017

Журналисты раскрыли целую фабрику по производству лайков и комментов

Когда количество лайков и подписчиков легко переводится в деньги, возникает спрос на фейковые лайки и подписчиков (From-UA Новости Украины).

Сетевую популярность делают примерно так же, как магнитики на холодильник – и то, и другое производится на азиатских фабриках, сообщает ПМ.

В старом доме на камбоджийской границе стоит лист металла, украшенный 500 смартфонами. Каждый подключен к компьютеру. На складе хранится 35000 SIM-карт. Так выглядит обычная фабрика кликов – нелегальное предприятие, основной продукт которого – показатели популярности заказчика в интернете. Корреспондентам американского издания Motherboard удалось побывать на такой клик-фабрике и рассказать о том, как устроен этот бизнес.

Телефоны и симкарты поставляет в Тайланд китайская компания; китайцы же платят немаленькие деньги (4 тысячи долларов в месяц) обслуживающему персоналу фабрики. Перенести производство в Тайланд из Китая решили, по всей видимости, из-за выгодных тайских тарифов, а также потому, что купить SIM-карту без документов в Китае – большая проблема.

С этих смартфонов операторы фабрики создают фейковые аккаунты, которыми пользуются в основном для того, чтобы поднимать рейтинги сайтам, отдельным аккаунтам в соцсетях и платным мобильным приложениям. Тысяча фейковых подписчиков в Twitter или Instagram стоит не больше двадцати долларов.

Спецслужби і технології «соціального контролю»

31.05.2017

Не одна сотня наших хлопців загинула через «ВКонтакте» і «Одноклассники», - Артем Семеніхін

Через російські соціальні мережі на сході України гинули українські військові (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»). Про це в інтерв'ю «Вголосу» розповів колишній боєць АТО, мер Конотопа Артем Семеніхін.

«Якщо взяти ці ж самі російські соціальні мережі – я не розумію цих неадекватних молодих людей, які виходять з різними мітингами, пікетами, мовляв, поверніть нам «вкантактє», «однакласнікі». Якщо ці молоді люди мають багато вільного часу, то хай виходять на вулицю, займаються спортом, стають суспільно активними. Адже саме завдяки цим «однакласнікам» та «вкантактє» було вбито чимало наших хлопців. Раніше багато хто з українських військовослужбовців мав у телефоні мобільні додатки цих соцмереж і за допомогою них та геолокації російські окупанти визначали скупчення наших військових та наносили по них артилерійські або ракетні удари. Не одна сотня наших хлопців загинула через ці соцмережі», – сказав Артем Семеніхін.

***

1.06.2017

Facebook, Twitter и YouTube не справляются с удалением разжигающих ненависть постов

Социальные сети в среднем удаляют только шесть разжигающих ненависть постов из десяти. В основном публикации содержат ксенофобские и исламофобские высказывания.

Facebook, Twitter и YouTube в Европе не справляются с задачей удалять в течение 24 часов разжигающие ненависть посты в социальных сетях.

Докладніше

***

31.05.2017

В украинской блокировке соцсетей России есть смысл – WSJ

Украина пошла на радикальный шаг в кибервойне с Россией, когда заблокировала российскую версию Facebook для своих пользователей. «ВКонтакте» и «Одноклассники» были популярны в Украине, как и в других постсоветских странах. В Киеве свое решение объяснили тем, что эти сайты служат российской пропаганде.

Докладніше

***

31.05.2017

Евгения Подгайная

Нацполицию не интересуют наработки Совета Европы по киберпреступности

Нормы скандального законопроекта Нацполиции «О внесении изменений в некоторые законодательные акты относительно имплементации отдельных норм Конвенции о киберпреступности» необоснованно расширяют полномочия силовиков, полагают в ИнаУ.

Докладніше

***

31.05.2017

СМИ: Силовики повально читают переписку украинцев

Силовики все чаще стали просить доступ к электронным ящикам украинцев. В них ищут как доказательства вины подозреваемых в мошенничестве, так и смотрят переписку чиновников, а также тех, кого винят в разглашении коммерческой тайны.

Докладніше

***

31.05.2017

Интернет в Украине может оказаться под жестким контролем

В Украине подготовлен законопроект о контроле за украинским Интернетом. Эксперты говорят, что принятие документа вынудит основную часть неподконтрольных и независимых компаний уйти с рынка.

Докладніше

***

1.06.2017

Через лайки у Facebook українців почали викликати на допити в поліцію

Українські поліцейські почала викликати на допити людей, за лайки і репости в Facebook. Як передає replyua.net, таку інформацію на своїй сторінці в соцмережі повідомила волонтер Діана Макарова (From-UA).

Вона зазначила, їй зателефонували з Шевченківського УП ГУ Нацполіції Києва та запросили дати свідчення з приводу розгрому скандальної виставки про Майдан художника Давида Чічкана в лютому поточного року. Макарова наголосила, що не відвідувала виставку, а лише лайкнула пост про її розгром. Автором допису був ветеран АТО, громадський активіст Дмитро Резніченко.

«Я точно знаю, що з Шевченківського РВВС міста Києва, вулиця Герцена, 9, кабінет 330, зателефонували не лише мені. Слідчий Воробйова, ім’я та по батькові не повідомила – викликала користувачів як свідків, які поставили лайк під постом», – написала вона, нагадавши, що підставою для виклику на допит, відповідно до закону, може бути лише повістка.

У той же час, дружина Дмитра Резніченка, Вікторія, розповіла, що її також викликали на допит в поліцію через пост в соцмережі відносно скандальної виставки. За її словами, слідчі почали досить агресивно розпитувати її, з якою метою вона писала в Facebook про лютневий інцидент.

***

1.06.2017

Власти США ужесточили правила выдачи виз

Власти Соединенных Штатов Америки решили ужесточить правила проверки для выдачи виз, пишет Корреспондент (Mignews.com.ua).

По полученным данным, новая анкета для соискателей включает несколько новых пунктов, в частности, предлагается указать имена, под которыми заявитель зарегистрирован в соцсетях.

В соответствии с новыми правилами работники американских консульств будут запрашивать у желающих получить визу номера всех их прошлых загранпаспортов, имена профилей в социальных сетях, которыми они пользовались в последние пять лет, а также подробную биографию за последние 15 лет – данные о работе и перемещениях по миру.

Стоит отметить, что ответы на все эти вопросы не обязательны, однако их отсутствие может повлиять на решение о выдаче визы.

Как сообщал MIGnews.com.ua ранее, спикер украинского внешнеполитического ведомства Марьяна Беца заявила, что вопрос введения визового режима между Украиной и Российской Федерация является довольно сложным и требует изучения и учета политических, юридических и технических факторов.

***

4.06.2017

В ЕС намерены ужесточить контроль соцсетей

Социальные сети не успевают удалять комментарии и посты, разжигающие ненависть. К такому выводу пришли эксперты Еврокомисии, которые проанализировали контроль за публикациями в европейском сегменте интернета. В специальном докладе организации говорится – в среднем соцсети блокируют только 6 из 10-и подобных материалов.

Докладніше

***

8.06.2017

У Держдуму внесли законопроект про заборону обходу блокування сайтів

У Держдуму Росії внесено законопроект, який забороняє використання технологій, що дозволяють обходити блокування сайтів. Відповідний документ опубліковано на сайті нижньої палати російського парламенту. Крім того, пропонують зобов'язати пошукові системи «припиняти видачу посилань на заблоковані в Росії інформаційні ресурси».

Докладніше

***

12.06.2017

Дуров рассказал о попытке подкупить его сотрудников в США

Один из основателей «ВКонтакте» и создатель Telegram Павел Дуров рассказал о попытке американских правительственных учреждений подкупить его сотрудников. Об этом он написал в своем Twitter (InternetUA).

«Во время недельного визита нашей команды в США в прошлом году было две попытки подкупить наших разработчиков американскими ведомствами. Плюс давление на меня со стороны ФБР», – пояснил Дуров.

Так предприниматель ответил на комментарий одного из подписчиков, который утверждал, что между создателями приложения для шифрования CryptoApp (в соцсети «ВКонтакте» – прим. «Ленты.ру») и правительством США существует тайный сговор. «Было бы наивно думать, что в США можно запустить независимую и безопасную программу для шифрования», – добавил бизнесмен.

***

13.06.2017

Блокировка «ВКонтакте»: Нацкомиссия утвердила инструкцию для провайдеров

Национальная комиссия, осуществляющая государственное регулирование в сфере связи и информатизации (НКРСИ), утвердила проект постановления Кабмина, разъясняющий сроки и механизмы закрытия доступа к российским веб-ресурсам (Апостроф).

Согласно тексту документа, имеющегося в распоряжении агентства, операторы и провайдеры телекоммуникаций обязаны блокировать доступ к российским ресурсам в течение 5 дней после вступления его в силу.

«Блокирование доступа к информационным ресурсам временно осуществлять за доменным именем, указанным в санкционном списке и соответствующим ему IP-адресом», – говорится в документе.

При этом Государственая служба специальной связи и защиты информации (Госспецсвязи) должна приобрести комплексы кибербезопасности и вместе со Службой безопасности Украины (СБУ) установить их у операторов и провайдеров телекоммуникаций, использующих каналы международной электросвязи, списки которых им предоставит НКРСИ. Соответствующие

комплексы будут обеспечивать мониторинг блокирования доступа к подсанкционным ресурсам.

Проблема захисту даних. DDOS та вірусні атаки

31.05.2017
«ВКонтакте» выплатила свыше $148 тыс. за найденные уязвимости

За два года участия в программе по поиску уязвимостей HackerOne соцсеть «ВКонтакте» выплатила более $148 тыс. 282 специалистам по информационной безопасности за выявление уязвимостей в сервисе, сообщила пресс-служба Mail.Ru Group (InternetUA).

С мая 2015 года соцсеть получила в общей сложности более 3 тыс. сообщений об уязвимостях, из которых авторы 385 отчетов получили вознаграждение. Размер вознаграждения пропорционален опасности уязвимости, минимальная награда составляет $100. Выплата производится только первому исследователю, сообщившему о проблеме. В случае эксплуатации уязвимости против пользователей вознаграждение не выплачивается.

HackerOne – платформа, благодаря которой специалисты в области кибербезопасности могут проинформировать компании об обнаруженных уязвимостях и получить за это вознаграждение. Участниками программы HackerOne являются крупные мировые IT-компании, в том числе Adobe, Twitter, Uber, Snapchat, Pornhub, Dropbox.

***

31.05.2017
WSJ: «ВКонтакте» стала майданчиком для хакерських атак

Видання Wall Street Journal випустило статтю, в якій розповідається про загрози російських соцмереж «ВКонтакте» і «Одноклассники». Експерти з кібербезпеки вважають, що соцмережі представляють ще більшу небезпеку, ніж пропаганда, ставши стартовими майданчиками для хакерських атак, стверджує видання.

Докладніше

***

31.05.2017
Хакеры слили в Сеть 25 тыс. фотографий клиентов клиники пластической хирургии

30 мая хакеры из Tsar Team опубликовали в интернете архив литовской сети клиник пластической хирургии Grozio Chirurgija – 25000 фотографий (в

том числе в обнаженном виде) и персональные данные клиентов. Среди них оказались жители более чем 60 стран мира; многие из них получили от хакеров сообщения с требованием выкупа, сообщает The Guardian.

Докладніше

***

1.06.2017

Windows 10 следит за пользователями даже при отключенной телеметрии

Microsoft неоднократно подвергалась критике за сбор большого количества телеметрических данных в Windows 10. Компания доказала, что прислушивается к мнению своих клиентов и с выходом обновлений предоставила пользователям больший контроль над конфиденциальностью. Тем не менее, по словам ИБ-эксперта Марка Барнетта (Mark Burnett), многие годы посвятившего разработке Windows, даже ограничительные настройки не мешают Windows 10 Enterprise Edition отправлять данные на серверы Microsoft.

Докладніше

***

1.06.2017

Украинцам объяснили, чем опасно обходить блокировку «Яндекса» и «ВКонтакте»: появилось видео

Не только простые украинцы, но уже и крупные компании осваивают способ обхода блокировки российских сайтов – VPN-сервисы (подменяют реальный ip-адрес). При этом они не учитывают, что таким образом информация на их компьютерах становятся открытой для держателей VPN – серверов.

Докладніше

***

2.06.2017

WikiLeaks опубликовал весьма необычный хакерский инструмент ЦРУ

Портал WikiLeaks опубликовал очередной хакерский инструмент из арсенала ЦРУ. Вредоносное ПО Pandemic предназначено для взлома компьютеров с общими папками, откуда пользователи загружают файлы с помощью протокола SMB. Pandemic отличается необычным, оригинальным принципом работы и не похож ни на один другой вредонос.

Докладніше

***

4.06.2017

В киберполиции рассказали провайдерам, как блокировать санкционные сайты

Департамент киберполиции Национальной полиции Украины разработал ряд рекомендаций для предприятий, учреждений и организаций всех форм собственности, как заблокировать доступ к запрещенным веб-ресурсам.

Докладніше

***

5.06.2017

Троян заблокировал тысячам пользователей доступ к Active Directory

Исследователи из IBM X-Force Research зафиксировали всплеск активности банковского трояна QakBot (другое название PinkSlip). Как сообщают эксперты, вредонос заблокировал тысячам пользователей Active Directory доступ к доменам их компаний, из-за чего они не могли авторизоваться на серверах своих работодателей (InternetUA).

QakBot появился в 2009 году и с тех пор регулярно совершенствуется. Вредонос представляет собой модульный многофункциональный троян. В частности, QakBot способен похищать банковские данные, цифровые сертификаты, токены авторизации, файлы cookie и выполнять функции кейлоггера, бэкдора и SOCKS прокси. Последняя версия трояна также получила функцию обхода обнаружения антивирусными продуктами.

Вредонос используется для атак на коммерческие организации с целью похищения средств с их банковских счетов. QakBot распространяется подобно сетевому червю путем самовоспроизведения на устройствах общего пользования и съемных накопителях. Последняя вредоносная кампания в основном затронула финансовые организации в США. По словам исследователей IBM, они впервые столкнулись с тем, что вредоносное ПО заблокировало пользователям доступ к Active Directory в корпоративных сетях.

Active Directory – службы каталогов корпорации Microsoft для операционных систем семейства Windows Server.

***

5.06.2017

Китайский вирус заразил более 250 млн компьютеров

Новый вирус Fireball способен управлять браузерами жертв, заменяя стартовые страницы и поисковые машины на фейковые поисковики-шпионы. После этого начинается отслеживание трафика и передача хакерам личных данных человека, сообщает The hacker news (ria-m.tv).

Специалисты в области кибербезопасности убеждены, что китайские программисты создали вирус Fireball с целью увеличения прибыли от интернет-рекламы.

В соответствии с тем аналитическим комплексом данных, что уже размещен по всей планете Fireball заразил, по меньшей мере, 250 млн. компьютеров.

Больше всего зараженных компьютеров в Индии – 25,3 млн. Это 10 % от всех компьютеров страны.

Далее следуют Бразилия – 24,1 млн (9.6 %), Мексика – 16,1 млн (6.4 %), Индонезия – 13.1 млн (5.2 %), США – 5,5 млн (2.2 %).

***

6.06.2017

Лучшие браузеры для анонимного веб-серфинга

Используемый Вами браузер знает многое о Вас и предоставляет эту информацию посещаемым сайтам, если Вы разрешаете это делать. Однако существуют специальные веб-обозреватели, которые предназначены для того, чтобы обезопасить Ваши данные и сделать интернет-сёрфинг, насколько возможно, защищённым. В этой статье представлено несколько известных веб-браузеров, которые помогут оставаться в сети инкогнито, рассмотрим их по очереди.

Докладніше

***

6.06.2017

Через соцсети распространяется очередной опасный вирус

Компьютеры и телефоны заражают с помощью сайтов-прокладок, а пользователей заманивают бесплатными билетами.

Киберпреступники стали заманивать пользователей интернета через социальные сети, привлекая их бесплатными билетами.

Докладніше

***

6.06.2017

Теракты онлайн: эксперт рассказала, как экстремисты подстроились под интернет

Террористические организации активно проникают в виртуальное пространство и используют интернет для распространения своих взглядов и вербовки потенциальных смертников (Обозреватель), рассказала эксперт по психологической кибербезопасности, кандидат психологических наук Наталья Бугаева.

«В 2000 году в виртуальном пространстве было представлено всего лишь 30 террористических организаций. На сегодняшний день – 5 тысяч. Самое интересное то, что и они трансформировались. Например, те теракты, которые произошли во Франции в конце прошлого года, чем интересны? Тем, что заказчик и исполнитель никогда не видели друг друга», – отметила она.

Бугаева подчеркнула, что они общались через виртуальное пространство, а теракты были спланированы и велись тоже с помощью интернета.

«Таким образом мы сталкиваемся сейчас с тем, что идет вербовка, которая не предполагает общение между исполнителем и заказчиком», – добавила эксперт.

По ее словам, жертвами вербовки могут стать в первую очередь выходцы из бедных стран. Хотя обработка сознания зависит от конкретной страны.

«Что особенно важно, что сейчас делается ставка на молодежь Особенность молодежи как-то проявиться. Поэтому они становятся легкой добычей террористических организаций. Обрабатывают их достаточно быстро и очень профессионально, а вот такие сайты запретить практически невозможно», – подытожила она.

***

7.06.2017
США підозрюють російських хакерів у зломі агентства в Катарі
Ігор Чорний

Американське слідство вважає, що російські хакери зламали державне інформаційне агентство Катару і опублікували підроблене новинне повідомлення, яке посприяло кризи серед найближчих союзників США в районі Перської затоки. Про це повідомляє УНН з посиланням на CNN (Інформаційне агентство «Українські Національні Новини»).

Повідомляється, що ФБР недавно направило в Доху слідчу групу для надання допомоги уряду Катару в розслідуванні передбачуваного інциденту за участю хакерів.

«Дані, зібрані службами безпеки США, вказують на те, що російські хакери причетні до атаки, про яку вперше повідомив уряд Катару два тижні тому», – повідомляє телеканал.

Посольство Катару в Вашингтоні повідомило, що розслідування триває, його результати обіцяють оприлюднити найближчим часом.

***

7.06.2017
У США довели кібератаку російських хакерів на Чорногорію

Пов’язані з російською розвідкою хакери здійснили кібератаку на Чорногорію на початку 2017 року. Про це свідчать дані компанії з питань комп’ютерної безпеки FireEye (ВинницаОК).

Компанія пов’язала кібератаку саме з Росією, адже виявила інфраструктуру та програми, які використовує виключно хакерська група APT 28, яку також підозрюють у втручанні в президентські вибори у США 2016 року.

За словами віце-президента і головного технічного директора FireEye Тоні Коула, розширення НАТО часто розглядається Кремлем як загроза для безпеки держави. Зокрема, заявка Чорногорії на членство в Альянсі сильно оскаржувалася Росією і проросійськими політичними партіями в Чорногорії.

«Цілком ймовірно, що ця діяльність є частиною постійної спрямованості APT 28 на ураження різних держав-членів НАТО, а також самої організації», – пояснив Коул.

***

8.06.2017

Впроваджено нові шляхи оперативного реагування на кіберзлочини

На базі Департаменту кіберполіції Національної поліції України вже впроваджені новітні технології та сервіси, які дозволяють миттєво реагувати на звернення громадян про кіберзлочин чи кібератаку (Сайт Департаменту Кіберполіції України).

У 2017 році на базі Департаменту кіберполіції створено цілодобовий «call-центр» для прийому заяв та звернень від громадян про злочини та правопорушення, що вчиняються в глобальній мережі. Функціонування такого зворотного зв’язку вже дає свої результати. Так, у 2017 році до кіберполіції за допомогою вже звернулось 9817 громадян із повідомленнями про вчинені правопорушення у кіберпросторі. 90 % з цих звернень вже розглянуто та опрацьовано підрозділом у межах своєї компетенції. Нагадаємо, інформацію до «call-центру» Департаменту кіберполіції громадяни мають змогу направити каналами Інтернет, а з початку 2017 року – працює безкоштовна «cyber» гаряча телефонна лінія за номерами: 0672186367, 0636198495 та 0681508601. За допомогою цього ресурсу, громадяни отримують необхідну допомогу від працівників кіберполіції не пізніше ніж за три години після надходження звернення. Важливо відмітити, що у випадку надходження до «call-центру» інформації, що не відноситься до компетенції кіберполіції, вона автоматично перенаправляється до лінійного підрозділу поліції. Найближчим часом, для охоплення більш ширшої аудиторії та виявлення кіберзлочинів, заплановано включення «call-центру» Департаменту кіберполіції в єдину мережу «call-центру» Національної поліції України. Також на сайті кіберполіції громадяни, за допомогою інформаційного антишахрайського майданчика „stop fraud”, мають змогу в режимі онлайн ознайомитися з поширеними випадками шахрайства, повідомити інформацію щодо шахраїв, вчасно не допустити списання або втрати грошей зі свого рахунку та оперативно заблокувати незаконно проведену транзакцію.

***

8.06.2017

Хакери із США атакують сайт Путіна

Хакерські атаки, які здійснюються із території Сполучених Штатів Америки, фіксуються щодня (Інформаційна агенція «Вголос»).

У Кремлі заявили, що з території США здійснюються хакерські атаки на сайт президента РФ Володимира Путіна. Про це журналістам у Москві сказав прес-секретар Путіна Дмитро Пєсков, – передає УНІАН.

«…Це дійсно так, власне, атаки йдуть з території багатьох країн світу», – сказав Пєсков, відповідаючи на питання, чи мають у Кремлі докази, що США нібито намагалися вплинути на вибори в РФ.

«Що стосується втручання у внутрішні справи, то такі випадки також добре відомі», – додав він.

На прохання журналістів пояснити, чи йдеться про причетність спецслужб США до хакерських атак на РФ, Пєсков відповів: «Це я говорю про територію США. Я не хотів би смішити публіку заявами про те, що за цим стоїть офіційний Вашингтон. Бо вчинення хакерської атаки з території будь-якої країни не може означати причетності офіційної влади до цього».

Президент РФ Володимир Путін 3 червня заявив, що хакери, які могли вплинути на хід голосування в США, могли бути американцями.

***

8.06.2017

В инстаграме Бритни Спирс обнаружены инструкции для «российских хакеров»

В инстраграме певицы Бритни Спирс обнаружены комментарии, которые, по данным исследователей из компании ESET, являются инструкциями для вредоносного программного обеспечения русскоязычной хакерской группы Turla.

Докладніше

***

8.06.2017

Обнародована новая технологию слежки за персональными компьютерами

1 июня на сайте компании WikiLeaks были опубликованы документы, которые раскрывают особенности так называемого проекта «Pandemic».

Данная технология заключается в том, что она дает возможность заражать компьютеры, на которые установлена ОС Microsoft Windows, по локальным сетям. И удаленные пользователи могут совместно применять ту или иную программу (Донбасс).

Если считать программу с зараженной машины, то код приложения сразу заменяет специфический «троян». Исходный файл маскируется и модифицируется, когда происходит его скачивание с файлового сервера, что и позволяет работать на компьютере удаленному пользователю.

Троянская закладка дает возможность заменять до 20 программ, которые имеют размер до 800 мегабайт из списка пользователей, которых выбирает оператор.

***

8.06.2017

В браузере Google Chrome нашли неизвестную «шпионскую» уязвимость

Специалисты по IT-безопасности обнаружили в браузере Google Chrome ранее неизвестную «шпионскую уязвимость», позволяющую совершать аудио- и видеозаписи без уведомления пользователя. Сведения появились в профильном издании (Grifonsoft).

Как рассказал Ран Бар-Зик, представитель компании AOL, во время использования проекта по передаче данных между браузерами – WEBRtc стало известно об отключенном индикаторе, предназначенном для уведомления пользователя о записи данных. Сама по себе уязвимость неопасна, поскольку сайты все равно запрашивают разрешение на выполнение дополнительных операций, но хакеры могут ей воспользоваться.

Разработчики Google уже приступили к устранению проблемы, предупредив, что хакеры могут воспользоваться камерой и микрофоном и без браузера, установив на ПК вредоносную программу.

***

9.06.2017

Большинство уязвимостей сначала раскрываются online и в даркнете

Каждая 20-я уязвимость появляется в даркнете до того, как попадает в Национальную базу уязвимостей.

Более трех четвертей уязвимостей раскрываются online до внесения в Национальную базу уязвимостей (National Vulnerability Database, NVD). На новостных сайтах, в блогах и соцсетях, а также в даркнете подробности о проблемах безопасности в ПО публикуются чаще, чем в NVD. К такому выводу пришли эксперты компании Recorded Future на основании анализа собранных в начале 2016 года данных о свыше 12,5 тыс. уязвимостей (Центр информационной безопасности).

По словам исследователей, в среднем разница между раскрытием уязвимости в интернете и ее внесением в NVD составляет семь дней. В эти семь дней организации подвергаются большому риску кибератак, что ставит под сомнение надежность официальных каналов раскрытия уязвимостей, считают

эксперты. Промежуток между выходом уведомления об уязвимости от производителя и внесением ее в NVD может быть еще больше.

Каждая 20-я уязвимость (5 %) появляется в даркнете до того, как попадает в NVD. К примеру, PoC-эксплоит для уязвимости Dirty Cow (CVE-2016-5195) был опубликован на Pastebin за 15 дней до NVD. Спустя всего два дня с момента публикации на Pastebin пост был переведен на русский язык и опубликован на хакерском форуме. Более 500 раскрытых в прошлом году уязвимостей до сих пор не внесены в NVD.

Национальная база уязвимостей – разработанный Институтом стандартов и технологий США правительственный централизованный репозиторий данных об управлении уязвимостями.

***

12.06.2017

Чем для компаний оборачиваются недочеты в киберзащите индустриальных систем

За последние 12 месяцев каждая вторая промышленная компания в мире пережила от одного до пяти киберинцидентов – они затронули критически важные инфраструктуры или автоматизированные системы управления технологическими процессами (АСУ ТП) на этих предприятиях.

Докладніше

***

12.06.2017

Российские хакеры забросали украинские СМИ письмами от имени СНБО

11 июня редакциям украинских СМИ было разослано сообщение бессмысленного содержания с IP-адреса, зарегистрированного в России от имени пресс-службы Совета национальной безопасности и обороны. Об этом сообщает пресс-служба СНБО (From-UA).

В СНБО также обратились к журналистам с просьбой быть внимательными к контенту сообщений и отправителям.

***

12.06.2017

Microsoft закрывает «убийцу» Google Docs, созданного совместно с Facebook

Сервис Docs.com, принадлежащий Microsoft и предназначенный для обмена документами, завершит работу в декабре 2017 г. К этому времени компания советует пользователям мигрировать на SlideShare или OneDrive.

Закрытие последовало вскоре после того, как выяснилось, что поисковик сайта предоставляет публичный доступ к конфиденциальным файлам.

Докладніше

***

13.06.2017

Хакеры разработали новый способ распространения вредоносного ПО

Киберпреступники разработали новую технику распространения троянов при помощи PowerPoint и Mouseover: «заражённая» PowerPoint-презентация распространяется посредством спам-рассылки с темой писем Purchase Order #, Invoice или Confirmation.

Докладніше

***

13.06.2017

Атаки російських хакерів під час виборів у США торкнулися 39 штатів, – Bloomberg

Під час минулорічних виборів президента США атаки російських хакерів торкнулися 39 штатів. Про це повідомляє видання Bloomberg (LB.ua).

«Загалом російські хакери вразили систему в 39 штатах», – наголошено в повідомленні.

Про хвилі атак улітку та восени 2016 року розповіли три джерела, безпосередньо знайомі з розслідуванням.

Наголошують, що кібератаки Росії в виборчу систему США були набагато ширші, ніж про це було публічно повідомлено. Зокрема, мова про вторгнення в бази даних виборців і програмних систем, кількість яких виявилася вдвічі більшою.

Так, дослідники виявили докази того, що в штаті Іллінойс кіберзлочинці намагалися видалити або змінити дані виборців. Хакери зламували програмне забезпечення, призначене для опитування в день виборів, і принаймні в одному штаті отримали доступ до бази даних.

Як пише видання, масштаби втручання були такими, що представники адміністрації Барака Обами зробили безпрецедентний крок - поскаржилися безпосередньо Москві, зателефонувавши по «червоному телефону».

Два джерела розповіли, що в жовтні Білий дім зв’язався з Кремлем, щоб надати докладні документи про втручання Росії у вибори і попередити, що кібератаки можуть призвести до широкого конфлікту.

Як повідомляли раніше, генпрокурор США Джефф Сешнс вирішив виступити перед комітетом Сенату з розвідки після свідчень екс-керівника ФБР Джеймса Комі.

***

13.06.2017

Дослідники Dragos запідозрили російських хакерів в атаці на енергосистему Києва

Хакерська група Electrum причетна до атаки на енергосистему компанії «Укренерго» в грудні 2016 року. Про це йдеться у звіті фахівців з інформаційної безпеки Dragos (LB.ua).

За даними дослідників, ця група безпосередньо пов'язана з хакерською групою Sandworm Team, яку неодноразово звинувачували в роботі на російські спецслужби.

У звіті сказано, що хакери створили шкідливе програмне забезпечення Crash Override, головним завданням якого була атака на енергосистеми. Crash Override в разі незначного допрацювання здатна атакувати енергосистеми не тільки України, а й європейських країн, а також теоретично для неї вразлива інфраструктура в США.

Dragos провели аналіз Crash Override разом зі словацьким виробником антивірусів ESET. У дослідженні йдеться, що шкідливе ПЗ здатне атакувати відразу кілька енергопідстанцій одночасно, але його характер роботи дозволяє викликати тільки тимчасові перебої з електрикою, які можуть тривати кілька годин або днів, але не тижнів.

У звіті також детально розбирається, як з технічного погляду влаштована атака за допомогою Crash Override.

ДОДАТКИ

Додаток 1

5.06.2017

Стартувала реєстрація в українську соціальну мережу Ukrainians

Від 3 червня реєстрація в українській соціальній мережі Ukrainians відкрита за посиланням www.ukrainians.co. Про це повідомила співзасновниця української соціальної мережі Олександра Струмчинська («Репортер»).

Відповіді на найактуальніші запитання, які були поставлені Олександрі особисто та на офіційних сторінках Ukrainians протягом 24 годин після запуску співзасновниця соцмережі описала максимально змістовно у своєму дописі:

1. Чому доступна лише реєстрація профайлу, а всі інші кнопки не працюють?

Повноцінна реалізація проекту – 4 місяці. Протягом зазначеного періоду плануємо поступово презентувати для Вас частини функціоналу української соціально мережі. Очікуйте наступний функціонал «Друзі» та «Новини» після досягнення 100 000 зареєстрованих користувачів.

2. Чому в українській соціальній мережі можна зареєструватись через ВК?

Функція реєстрації можлива через перенесення основних персональних даних з соціальних мереж ФБ та ВК для того, щоб спростити користувачам процес заповнення профілю та в майбутньому пришвидшити можливість пошуку друзів, з якими Ви спілкувались. Доступна можливість реєстрації через соціальні мережі ФБ та ВК, або ж через підтвердження нового профілю через електронну скриньку.

3. Навіщо для запуску наступного функціоналу необхідно, щоб на сайті було зареєстровано 100 000 чоловік?

Успіх Ukrainians напряму залежить від Вас та Вашої активності. Саме тому нам потрібна Ваша допомога на кожному з етапів розвитку. Не очікуйте дива в перший же день від нас – допоможіть його зробити разом. Заходьте, реєструйтеся, запрошуйте друзів – швидкість реалізації та представлення нового функціоналу у Ваших руках.

4. Куди звертатись, якщо виникають складності з реєстрацією і я маю ідеї та побажання для Ukrainians?

Рекомендації щодо розробки Ukrainians, резюме та пропозиції відносно співпраці надсилайте на пошту: ukrainiansofficial@gmail.com або залишайте у коментарях

«Заходьте, реєструйтесь, запрошуйте своїх друзів! Успіх Ukrainians напряму залежить від вас та вашої активності», – написала Олександра.

(вгору)

Додаток 2

8.06.2017

Украинцы создали соцсеть, построенную на обмене криптовалютой

Украинские стартаперы создали социальную сеть Nimses, похожую на Инстаграм, но от обычной ленты фотографий ее отличает привязка действий к социальному капиталу внутри сервиса (Take-profit.org).

Согласно сообщению, Nimses называют криптовалютой. Но, трекер рыночной капитализации от CoinmarketCap, такой криптовалюты не знает.

«Социальный капитал в Nimses исчисляется нимами, и он постоянно увеличивается – на один ним каждую минуту (вероятно, nim – анаграмма сокращения «min»). Действия в приложении тоже стоят нимы: опубликовать запись – 100 нимов, лайкнуть чужую – от 10 до 100. Авторы устанавливают ценник сами», – говорится в сообщении.

Кроме того, нимами можно обмениваться с другими пользователями, а искать их можно через рейтинги популярных записей или прямо на карте поблизости.

Как сообщается, профили, где можно листать фотографии пользователей, напоминают Badoo, а каждому человеку можно написать напрямую, поэтому отчасти Nimses – дейтинговый сервис.

В Nimses утверждают, что в июне нимы можно будет менять на товары или услуги.

«Позднее их можно будет обналичивать, обещают разработчики – но только с февраля 2018 года и только если у пользователя наберется более 43 тысяч нимов. Сейчас один доллар равен 1822 нимам, однако это ничего не значит: ним постоянно падает в цене, еще утром 6 июня доллар равнялся 1300 нимам. Каким курс будет к февралю, никто не знает», – пишет издание.

Издание отмечает, что Nimses действительно находится на первом месте среди бесплатных приложений в российском App Store.

Согласно статистике App Annie, еще 1 июня его не было в общем чарте, а 4 июня он уже закрепился на лидерской позиции. В Google Play он пока на 11-м месте, но тоже быстро растёт.

(вгору)

Додаток 3

8.06.2017

Число любителей историй «ВКонтакте» превысило 40 миллионов человек

В конце 2016 года социальная сеть «ВКонтакте» предложила вниманию пользователей «Истории» – новый формат общения с друзьями, позволял рассказывать им и подписчикам о происходящих событиях с помощью фотографий, коротких видеороликов с добавлением граффити, стикеров или текста, не публикуя их на своей странице (Grifonsoft).

Для продвижения нового формата был запущен специальный проект «Лис». По условиям акции, пользователи в течение месяца каждый день выполняли задания и публиковали истории, получая за это эксклюзивные стикеры. Менее чем за сутки с первым заданием – опубликовать историю – справилось 99 % участников конкурса.

Как отмечено в пресс-релизе, за время акции «Лис» число авторов историй увеличилось в 4 раза, количество опубликованных историй за месяц выросло в 9 раз, а общая месячная аудитория сервиса в итоге увеличилась с 25 до 40 млн человек.

По словам Евгения Красникова, пресс-секретаря «ВКонтакте», новый сервис получил популярность, и после завершения акции пользователи продолжают им пользоваться.

«Аудитория паблишеров сервиса стала старше и разнообразнее. 60 % авторов, которые публикуют истории, продолжают использовать сервис и месяц спустя. Если в первое время работы аудитория была преимущественно женской, то сейчас треть авторов историй – мужчины. Кроме того, женщины и мужчины старше 21 года стали чаще рассказывать друзьям о своих событиях с помощью историй», – сообщается в пресс-релизе Mail.Ru Group.

(вгору)

Додаток 4

12.06.2017

Facebook разработала карты для помощи жертвам бедствий

Facebook работает с тремя всемирно известными гуманитарными организациями над новыми картами, которые призваны помочь в борьбе с последствиями катастроф. Эти организации – ЮНИСЕФ, Международное движение Красного Креста и Красного Полумесяца и Всемирная продовольственная программа (InternetUA).

В так называемых картах бедствий используются «совокупные анонимные» данные из Facebook. С помощью них, упомянутые организации могут получать информацию, полезную в реагировании и оказании помощи в ближайшие часы после происшествий.

Есть три типа карт. Карты плотности местоположения показывают, где люди находились до, во время и после бедствия. На них данные сравниваются с историческими записями – например, с оценками заселённости. Карты передвижений демонстрируют схемы перемещения людей в рамках нескольких часов. Так организациям проще определять, куда направлять ресурсы. На картах проверки безопасности отмечено, где люди отчитались о том, что находятся в безопасности после катастрофы, и где остались нуждающиеся в помощи.

Эти данные могут сильно помочь в оказании помощи пострадавшим. «Мы можем знать, где находится дом, но мы не знаем, где находятся люди, – сказал Дейл Кунс (Dale Kunce), глобальный руководитель по информационным коммуникационным технологиям и аналитике Американского Красного Креста. – Первым же делом мы можем отправиться туда, где произошло бедствие, но большинство людей со своими семьями уже могут быть в 10 милях оттуда».

Раньше профессионалы в области быстрого реагирования использовали Facebook Live и другие похожие инструменты для сбора актуальной информации о бедствиях. В будущем Facebook собирается предоставить доступ к картам властям и другим организациям.

(вгору)

Додаток 5

13.06.2017

Facebook значительно ускорила тренировку моделей компьютерного зрения

Facebook нашла новый способ тренировать модели компьютерного зрения, который должен значительно ускорить работу компании с искусственным интеллектом. С помощью новой техники Facebook может натренировать модель классификации изображений за час, не навредив её точности (InternetUA).

При максимальной производительности с помощью 256 графических процессоров новая система может обрабатывать 40 тысяч картинок в секунду, не жертвуя качеством итоговой модели. Это достижение поможет улучшить качество будущих исследований, поскольку научные сотрудники смогут быстрее проверять свои гипотезы.

Ускорение тренировки моделей машинного зрения важно для Facebook, поскольку она считает дополненную реальность и машинное обучение очень важными элементами для будущего своего бизнеса. Скоро сотрудники компании смогут проводить гораздо больше исследований.

«Они могут сказать: “Ладно, начнём свой день с одного из тренировочных прогонов, выпьем по чашке кофе и посмотрим, как всё прошло”, – говорит Питер Нордхейс (Pieter Noordhuis), инженер-программист команды Facebook по прикладному машинному обучению. – И используя то, что получили, они формируют новую гипотезу, начинают новый эксперимент и занимаются этим, пока день не подойдёт к концу. Так они, возможно, могут провести шесть последовательных экспериментов за день, хотя в противном случае у них могла уйти на это неделя».

Система работает быстрее, поскольку Facebook увеличила размер партий изображений, которые обрабатываются во время тренировки. Это позволяет производить вычисления на большем количестве графических процессоров. Но увеличение партии требует увеличения скорости обучения, что раньше приводило к снижению точности.

Теперь исследователи ввели фазу подогрева, в которой скорость обучения и размер партии картинок медленно увеличивается. Это позволило Facebook достичь при работе с партией из 8192 изображений примерно того же коэффициента ошибок, что и при одновременной обработке 256 изображений.

(вгору)

Додаток 6

13.06.2017

Підслухано у соцмережі, або Про що кажуть 84 тисячі лайків нардепів

Роман Супрун, керівник проекту PolitEyes

З поширенням використання соцмереж, зокрема Facebook, позиції парламентських фракцій стало визначати значно легше. Варто лише стежити за їх лайками – і все видно як на долоні (Українська правда).

Якщо можна виявити злочинців за особливостями їхньої банківської активності, то такі ж непов’язані на перший погляд деталі можуть «вистрілити» й в інших сферах.

Так подумали ми – і застосували цей принцип з бестселеру «Суперфрікономіка» до аналізу роботи Верховної Ради. Вирішили дізнатися, хто є явним (або прихованим) авторитетом українського парламенту за

допомогою досить нетривіального показника – активності депутатів різних фракцій у Facebook.

На користь саме цієї бази даних свідчать декілька речей. По-перше, 72 % депутатів вже є користувачами соціальної мережі, тому інформація буде репрезентативною. Ну а по-друге, у Facebook ти можеш скільки завгодно переглядати власну історію активності, проте відслідкувати чужі дії протягом тривалого періоду часу, як мінімум, не зручно. Більше того, далеко не кожен знає, що їхню «лайко-активність» у соцмережі може переглянути будь-хто.

Тож користувачі, якщо вже й ставлять лайки, то схильні виказувати свої справжні уподобання.

Що ми очікували від отриманої інформації?

По-перше, пости у Facebook зазвичай містять певні меседжі. Тож лайк під будь-яким з них – щось на кшталт відвертого зізнання членів фракцій з приводу того чи іншого політичного питання.

По-друге, така інформація має дати уявлення, наскільки визначеними та однорідними є погляди всередині фракцій.

І по-третє, можна прослідкувати спільні інтереси між членами різних фракцій та мати змогу спрогнозувати, хто кому союзник у тих чи інших питаннях.

Активісти Facebook

Для цього ми проаналізували активність у Facebook всіх зареєстрованих в соцмережі депутатів кожної фракції/групи Верховної Ради. З січня по травень 2017 року вони встигли поставити трохи більше восьмидесяті чотирьох тисяч лайків.

Оскільки кількість депутатів відрізняється залежно від фракції чи групи, ми врахували цей показник, щоб визначити найактивніші фракції: активність у Facebook = загальна кількість лайків депутатів фракції / кількість депутатів фракції, зареєстрованих у Facebook.

Абсолютним лідером виявилася Радикальна партія Олега Ляшка. 19 членів фракції є активними користувачами Facebook і за п’ять місяців вподобали в середньому по 397 постів кожен.

На другому місці за активністю в соцмережі – фракція «Самопоміч» з 21 депутатом у соцмережі та 340 лайками на кожного з них.

Замикає трійку лідерів «Народний фронт» – на кожного з її 64 активних членів припадає в середньому по 321 лайку за обраний період.

Тож якщо ці три об’єднання поставлять собі за мету просувати законодавчу ініціативу у Facebook, вони точно знають, як популяризувати ідею принаймні серед своїх друзів та підписників.

Загальні тенденції

Серед вподобань членів фракцій більшість популярних авторів складають їхні колеги-депутати Верховної Ради. Саме вони становлять більше половини ТОП-10 фаворитів для таких фракцій, як «Народний фронт» (60 %), Блок Петра Порошенка (70 %), «Батьківщина», «Самопоміч» (по 80 %) та РПЛ (90 %).

Найменше дописами колег у соцмережах цікавляться група «Відродження», Опозиційний Блок та «Воля народу».

Досить мало уваги фракції приділяють журналістам. Лише 9 журналістів потрапили у ТОП-10 восьми фракцій/груп та позафракційних депутатів. Причому жодного журналіста немає серед десятки фаворитів БПП та РПЛ.

Кого ж читають інші фракції серед представників центральних ЗМІ?

До ТОП-10 авторів фракцій потрапили журналісти телеканалу 1+1 («Батьківщина»), інтернет-видань LB.ua («Відродження»), Strana.ua («Воля народу»), Цензор.НЕТ («Самопоміч») та газети «День» (позафракційні депутати).

Серед представників державної влади найбільш популярними виявилися генеральний прокурор Юрій Луценко (БПП та позафракційні депутати) та міністр економіки Степан Кубів (БПП та «Народний фронт»). Вони зустрічаються у ТОП-10 більш ніж однієї фракції.

Однак щоб краще зрозуміти орієнтири, варто розглянути більш детально особливості та тенденції вподобань кожної фракції/групи.

Один за всіх

Почнемо, мабуть, з «найпатріотичніших», які переважну кількість лайків віддають постам колег по фракції. Трійку цих лідерів очолює РПЛ. В десятку найпопулярніших авторів серед «не-радикалів» пробився тільки мер Дніпра Борис Філатов.

Трохи менш «егоїстичними» виявилися депутати фракції «Самопоміч». Окрім членів фракції, до ТОП-10 авторів входять прес-секретар уповноваженого Верховної Ради з питань прав людини Михайло Чаплига та редактор онлайн-видання «Цензор.НЕТ» Юрій Бутусов.

Замикає трійку лідерів фракція БПП. Рівно половина найулюбленіших авторів фракції – це її члени. До іншої половини потрапив все той же пан Чаплига, позафракційні депутати Борислав Береза та Вікторія Пташник, а також генпрокурор Юрій Луценко та міністр економіки Степан Кубів.

Беззаперечні авторитети

Як виявилося, уподобання депутатів з різних об’єднань щодо авторів у Facebook досить часто перетинаються.

Так, наприклад, мер Дніпра Борис Філатов входить до ТОП-20 авторів одразу чотирьох фракцій – БПП, «Батьківщина», «Відродження», Радикальна партія, – а також групи позафракційних депутатів.

Пости голови фракції БПП Ірини Геращенко подобаються депутатам від БПП, «Батьківщини», «Народного фронту» та групи позафракційних депутатів.

Схожий рівень популярності має й заступник голови фракції Радикальної партії Ляшка Андрій Лозовий. Він входить до ТОП-20 авторів серед членів РПЛ, «Народного фронту», «Відродження», а також позафракційних депутатів.

«Маленька незалежність»

За, так би мовити, «оригінальністю суджень» лідером серед фракцій є Опозиційний блок – інтереси народних депутатів цього осередку

перекликаються лише у чотирьох з двадцяти випадків – з колегами з «Відродження» та «Волі народу».

Радикальна партія Ляшка також відрізняється значною кількістю унікальних вподобань – тільки 5 з 20 уподобань можна знайти у представників інших фракцій. Більше всього спільних улюблених авторів фракція має з «Народним фронтом» (4 користувачі). По два автори потрапили одразу до списку фаворитів як РПЛ, так і «Відродження» та позафракційних депутатів. Ще по одному спільному популярному автору члени РПЛ мають з «Батьківщиною» та БПП.

У фракції «Самопоміч» налічується 6 спільних фаворитів – по три з БПП і позафракційними депутатами та два з «Волею народу».

Спільні інтереси

Найбільшу загальну кількість спільних авторів з іншими фракціями має БПП. При цьому вподобання її депутатів найбільш близькі до позафракційних депутатів – 7 авторів з 20 (35 %) in common.

Це – голова фракції БПП Ірина Геращенко, «депутати-антикорупціонери» фракції БПП Оксана Юринець, Мустафа Найєм та Сергій Лещенко, а також позафракційний депутат Ганна Гопко. Крім того, і депутати БПП, і позафракційні схильні підтримувати лайками пости мера Дніпра Бориса Філатова, генерального прокурора Юрія Луценка та радника Міністра економіки Ярослава Железняка.

Схожі з БПП переваги у джерелах інформації мають і члени фракції «Батьківщина». До їхнього ТОП-20 у Facebook входить п’ятеро авторів, яких поважають і в БПП. До цього списку увійшли Ірина Геращенко, Сергій Лещенко, Борис Філатов, а також позафракційні депутати Борислав Береза та Вікторія Пташник.

По чотири спільних автори мають позафракційні депутати з «Батьківщиною» та «Народним фронтом», а також НФ з радикалами.

Цікавинки

Наше дослідження не обійшлося й без декількох несподіваних знахідок.

Наприклад, з ТОП-10 «найлайковіших» сторінок депутатів «Волі народу» – 2 сторінки є пабліками. Так, депутати часто вподобають блог про Ізраїль «IsraLove» та російську інтернет-спільноту про сучасну культуру «Культурологія».

«Потішив» і Опоблок – першість у вподобаннях депутатів отримала блогер, яка пише на зовсім далекі від політики та державних справ теми.

Звичайно, до лайків у Facebook можна ставитися по-різному. Ми переконані, що цей показник стає дедалі більш вагомим. Нещодавнє рішення швейцарського суду про застосування штрафних санкцій на основі лайку людини – яскраве тому підтвердження.

Як інтерпретувати та використовувати дані активності українських парламентарів у соцмережі – кожен вирішує сам. Ми ж переконані, що розуміння цих схованих від неозброєного ока зв’язків дає можливість краще зрозуміти важелі впливу для формування позицій народних обранців.

Це допоможе залучати до онлайн-адвокації лідерів парламентських думок усвідомлено, не навмання.

(вгору)

Додаток 7

13.06.2017

Ольга Карпенко

Александр Колб, Promodo: Блокировки отбросили нас на 6 месяцев в развитии, оборот упал на 15 %

В середине мая президент подписал указ о блокировке российских интернет-ресурсов в Украине. В первые же недели после блокировки объем украинского трафика на такие ресурсы просел вдвое. Мы ранее уже писали о том, как блокировка «Яндекса», «ВКонтакте» и Mail.ru повлияет на украинский средний и малый бизнес. Чтобы узнать, как это отразилось на отдельных компаниях, редакция AIN.UA поговорила с Александром Колбом – директором известного украинского маркетингового агентства Promodo. О том, как нужно было действовать маркетологам в такой ситуации, а также о развитии рынка в целом он рассказал в интервью AIN.UA.

Новость о блокировке была не очень прогнозируемой. Как нужно было бы реагировать маркетологу в такой ситуации и что предприняли вы? Как среагировали клиенты (AIN.UA)?

Наш народ после Майдана уже трудно удивить, но это было и правда неожиданно. Наверное, о плохом думаешь всегда в отдельности от себя. Что нужно делать, когда ты получил по лицу? Забыть о стратегии и начать выживать.

Клиенты, нужно сказать, отреагировали спокойно. Мы сообщили об остановке сопровождения всех сервисов, за два дня мне позвонил всего лишь один клиент.

Если говорить о бизнесе, то само отключение рекламных площадок кого-то коснулось сильно, кого-то вообще не затронуло. У каждого бизнеса была своя стратегия: кто-то выжимал трафик из площадок на максимум, кто-то не использовал вообще. В целом доли продаж в общей структуре «чистого» онлайн-ритейла (а это самые большие рекламодатели санкционных площадок), упали в районе 10-20 %. Кирпичному же ритейлу легче, у них общие доли продаж просели на 2-5 % за счет больших долей в офлайн.

Но не стоит смотреть на площадки, как только на источники трафика, не исключайте поисковый маркетинг, трафик из социальных сетей, группы и приложения в них, огромные потери в email-базах, которые неохотно сейчас восстанавливаются. А в среднем mail давал ритейлу процентов 10 % в онлайн-доли продаж, а у многих «отвалилось» более 50 % базы (речь о блокировке доступа к почтовым сервисам, которые принадлежали санкционным компаниям – ред.).

Пока рано говорить о каком-то переливании аудиторий или же бюджетов. Нужно время, я думаю еще месяц, чтобы понимать ситуацию и потери.

Мы были топовым партнером «Яндекс» в Украине и достаточно много работали с «ВКонтакте», Mail.ru. Это миллионные суммы в месяц. Остановили все рекламные кампании, стали ждать реакции рынка. Я скажу: до сих пор мало кто понимает, как закрывать договорные обязательства с нашими партнерами, никто не дает решений. Мы не хотим «кидать» площадки и хотим закрыть наши договорные отношения в цивилизованном порядке, но процедура неизвестна, у многих у нас были кредитные линии: должны деньги, как и мы, так и нам. Мы написали запросы в органы, ждем официальных разъяснений.

Я практически уверен, что работа в рамках закона с этими площадками в Украине невозможна: нет возможности официально проводить оплаты, реакция рынка, сложные статьи и начавшиеся обыски подтверждают уже, что этот путь в никуда. Я говорю о чистом бизнесе, не рассматриваю возможности оплаты карточками, из других стран и прочее – зрелый бизнес не пойдет на такие вещи. Поэтому мы предлагаем клиентам релокацию в Facebook, Google, строим медиапланы, работаем с их ожиданиями и потребностями.

Мнения многих известных в уанете людей разделились по этому поводу, считаете ли вы блокировку необходимым шагом?

Это сложный вопрос. Наверное, Украина выиграет, если цели блокировки действительно были теми, о которых заявило государство. Но я думаю, что мы стали свидетелями политических игрищ. Остались вопросы по мобильным операторам, остались вопросы по наказанию виновников расстрелов на Майдане, отсутствие реформ в медицине, образовании, коррумпированные суды, отсутствие люстрации как таковой… много чего. Меня многие уже называют пессимистом, но у меня больше вопросов к власти, чем ответов на вопросы. Поэтому, если бы это происходило на фоне реальной помощи IT-бизнесу и беспокойстве о климате в стране, тогда берите – забирайте. А когда так бездумно… у меня нет слов. Впрочем, я сейчас буду выглядеть обиженным.

Даже на предприятиях есть целые программы по релокации и поиску рабочих мест тем, кого сократили. Это нормальная всемирная практика. Людей просто никто на улицу не выставляет. Что мешало дать время на перестройку? А ведь в санкционных компаниях работали крутые IT-специалисты. В одном «Яндексе» 300 человек. Вы думаете, что после увольнения они продолжат верить в Европу и правительство? Я очень сомневаюсь. И самое печальное, в чем я уверен, об этом даже никто не думал.

Как на ваш бизнес повлияла блокировка? Какой была доля бюджетов (раньше говорили о том, что доли Google vs. «Яндекс» в уанете распределялись примерно как 60х40 или 70х30)?

Сильно. Мы отказались от части офисных помещений, от расширения. Компания в стадии возврата. Нас отбросили на 6-8 месяцев в развитии. У нас есть два месяца, чтобы наверстать падение, в противном случае придется пересматривать общие планы, отказываться от ряда важных внутренних проектов, возможно, даже корректировать штат сотрудников.

Если говорить о деньгах в санкционных площадках, то доли «Яндекса» и «ВКонтакте» оставались в рынке, а рекламные обороты в них постоянно росли. Нужно признать, что и у «ВКонтакте» и у «Яндекса» в последние годы появилось достаточно много хороших конверсионных инструментов. «Яндекс» активно шел в медийку. Тяжело, медленно, но шел. Если же возвращаться к вопросу долей в рекламном пироге, то «Яндекс» 10-20 % (ниже Google значительно из-за отсутствия такого широкого инструментария, как YouTube, например), «ВКонтакте» от 0 до 5 % – тут все зависело от KPI и задач рекламируемой площадки.

Наше же падение в оборотах примерно 15 %, в прибыли даже чуть больше. Наши обороты по заблокированным площадкам составляли несколько миллионов гривен в месяц.

На украинский онлайн-бизнес больше повлияла блокировка «Яндекса» или «ВКонтакте»?

Нужно понимать, что это принципиально разные площадки, с различным инструментарием. «Яндекс» больше использовался на привлечение, там хорошая рекламная сеть, с хорошим ремаркетингом и др. Разный бизнес – по разному: тем, у кого поисковый трафик в приоритете, больше пострадали от потери «Яндекса».

Во «ВКонтакте» же другие форматы, модель поведения. Там хорошо догонять аудиторию, есть видеоформаты, тизеры и др. Доля «Яндекса» конечно же была большей в рекламе, я не говорю об историях с приложениями, группами и прочим – это еще одна отдельная большая тема.

Я могу однозначно сказать, что в этой ситуации выиграл Facebook, если говорить об аудитории. Мы видим большой прирост аудитории в Facebook (более 2 млн новых регистраций после блокировки российских сервисов – ред.). Но что касается Facebook для рекламодателя, то там не так все сладко: Facebook всегда был дороже с точки зрения стоимости привлечения покупателя, его тяжело масштабировать из-за достаточно узкой как для Украины аудитории, плюс отсутствие официального офиса в Украине, сложности с технологической поддержкой сильно ограничивают простоту работы с ним.

Естественно, часть аудитории перейдет на Google, но там конкуренция только возрастет, что может сказаться не на увеличении бюджетов, а наоборот – на их снижении, потому что от математики по стоимости привлекаемого клиента не убежишь.

После указа президента малый бизнес начал жаловаться именно на запрет ВК, в меньшей мере – на запрет «Яндекса»…

Это и понятно. Для малого бизнеса во «ВКонтакте» больше возможностей: группы, простые рекламки, handmade, что-то вроде Prom.ua для начинающих. Кто-то зарабатывал на кликах, кто-то на группках по $50, кто-то использовал для чатов и расписания на занятия в школу. Это такое себе окно, где и заработать, и музыку послушать. А «Яндекс» изначально олдскульный, сложный, если хотите: там интерфейс и редактор. Я уверен, что количество операций, проводимых в «ВКонтакте», в разы превышало «Яндекс», и не

удивлюсь, что это суммарно больше всей рекламной доли «Яндекса». Но если говорить о долях агентств в бизнесах «Яндекса» и «ВКонтакте», то «Яндекс» был гораздо «интересней».

Что вы прогнозируете для рынка онлайн-рекламы: постепенное перетекание всех бюджетов в Google и Facebook?

Пока нет глобального переливания. Никто не открыл шкатулку и не начал наливать. Вы ж помните, что продажи-то упали, нужно время оклематься после удара. Постепенно все рассосется между Google, YouTube, Facebook, другими медийными площадками. Back to School (имеется ввиду период перед первым сентября, когда компании активно вкладываются в маркетинг товаров для школы/вузов – ред.) все покажет.

Как поменяется рекламный ландшафт в уанете через 1-2 года, российские сайты вообще перестанут смотреть пользователи и использовать маркетологи?

Вы просто режете. Я думаю, что российские площадки уйдут раз и навсегда. Зрелый бизнес сто раз подумает, прежде чем разворачивать тут что-то («Рамблер» я не считаю). Разумеется, останутся VPN-щики, мелочь, те, кто научатся жить в этих условиях. Но это будет такая себе Северная Корея, на которой будут кормиться CPA-сети, чернушники, мелкий бизнес. Одна из причин – там будет дешево, но «дешева рибка – погана юшка», как говорится. Средний, крупный бизнес сто раз подумает, нужно ли там вообще размещаться, потому что а) некошерно; б) могут прийти; в) как платить? картой? Мы же не в 90-х, нам НДС подавай.

Как в целом на рынок повлияла война с РФ (некоторые интернет-компании отказываются от российских клиентов, перед тем же iForum было обсуждение: звать ли спикеров из РФ, если они не признают аннексию Крыма)?

Вы знаете, я разделяю людей и страны. Вектор страны, ее поведение, если говорить о РФ и Украине – это пока еще не народ, это политика. А в политику я не хочу лезть. И это замечательно демонстрирует общество с обеих сторон. Как только мы говорим о политике, неадекватная реакция с обеих сторон, поэтому я предпочитаю эту тему совсем не подымать. Много перегрето, много намешано, зачем?

А люди есть там и есть у нас. И специалисты есть там хорошие и есть чему учиться. Я говорю сейчас о профессиональных знаниях, экспертизе. Мы недавно привезли Алену Владимирскую к себе на конференцию – шикарный спикер, удовольствие в зале, атмосфера – профессионал с большой буквы. Кому от этого хуже стало? Мне кажется, я научился разделять эти вещи…

Если говорить о том, что будет дальше с клиентами из РФ, то я думаю, что на текущих санкциях это не закончится. Уверен, будут визы, уверен, будут встречные запреты. Есть ли смысл бежать против ветра? Выбирать каждому, это же зависит от куска пирога и степени веры.

Что можно сказать о развитии рынка онлайн-рекламы в Украине за последние несколько лет? Какие тенденции выделяются особенно ярко? Можно ли говорить о зрелости рынка?

Мы были и есть страной третьего мира в этом вопросе. Одни из лучших в центральной и восточной Европе, но все еще достаточно далеки технологически, профессионально, бизнесово. Вы никогда не задумывались, почему тут нет Facebook? А я вам отвечу – потому что один клиент в Англии обладает бюджетом больше, чем тратит вся Украина. Мы в 15 раз в количестве денег в онлайн-рекламе меньше РФ, если уж на то говорить. И это совсем не удивительно – большая часть населения живут на минималку. Для сравнения: рынок цифровой рекламы Украины ~$120 млн, рынок цифровой рекламы РФ ~$2 млрд, Казахстана $10-15 млн, global ~$180 млрд.

Да, рынок изменился, растет mobile, растет персонализация коммуникации, есть отдельные площадки, которые делают на этом всю стратегию 2017 года. YouTube, программатик – все это уже не мечты и не сказки, это уже сегодняшний день. Конечно, никто не заливает площадки бюджетами с прицелом на будущее, все это в прошлом. Немногие компании в 2017 смогли поставить задачи длиною в год.

Наш рынок – зрелый для Украины, для цивилизованных стран – отсталый и ему еще расти и расти. Прорывов, как таковых, с 2013 никто не делает, все растут органически. Но если сравнивать нас с Европой, США, то мы – динозавры. Но это не прорывы и, увы, не Big deal. Мы хороши не потому, что мы хороши, а потому то до нас дела нет никому и мало кто сюда лезет. Здесь нет конкуренции, и как только климат улучшится (если), то все резко изменится.

Несколько лет назад вы говорили о том, что украинские компании уже тратят на продвижение десятки млн долларов – выросли ли бюджеты? Много ли рекламодателей в уанете превышают бюджет в $1 млн? Ваши прогнозы?

Бюджеты выросли, конечно. Они органически растут ежегодно процентов на 20-30 % у каждой площадки, которая развивается. Я говорю сейчас, в первую очередь, о клиентах, составляющих костяк нашего портфеля: ритейле, досках объявлений, площадках сравнения цен и др. Они и до этого так развивались. Если же говорить о бюджетах, то, конечно, $1 млн в год уже вряд ли можно кого-то удивить. Это хорошие цифры, чтобы что-то реальное делать в онлайне, а не находиться в потоке.

Приятно, что в последнее время мы боремся не просто с продажами, а уже оперируем долями в онлайн-продажах, в товарных категориях, вообще говорим о лидерстве в сегментах. Ставятся и такие задачи, а это говорит, кто конкуренция нарастает.

Расскажите о Promodo – растет/падает ли бизнес, появляются ли новые конкуренты, открываете ли представительства, что планируете на ближайшие годы?

С 2013 мы росли на 30-40 % ежегодно. В этом была планка выше, и пока мы ее оставили. Получится ли с новыми изменениями? Посмотрим, нам не впервой. У нас доля 30 % в тех клиентах, которые мы считаем своими, и я понимаю, что с тем портфелем, который остался в Украине, мы не решим свои

амбиции, разве что произойдет как-то переворот в бизнесе, в условиях, в стране. Но я оптимист. Поэтому мы будем разворачивать наш корабль в Европу, это сложно, нас там не ждут, но выхода нет. Представительства не спешим открывать, пока в этом нет большого смысла. Только с определенным уровнем оборота, доли рынка, есть смысл в офисе – наша стратегия про деньги.

Что же касается конкуренции, то сегодня мы, наконец, почувствовали движение большой четверки или же их аффилиатов. Это говорит о том, что мы сталкиваемся, и это так и есть: YouTube, медийная реклама, программатик – это те технологии, платформы, на которых мы часто пересекаемся. Это пожалуй, единое звено, которое мы рассматриваем в своей парадигме, как конкурирующее. Ну и еще есть Google, мы плотно дружим и общаемся со всей украинской командой, командами поддержки в Дублине и других странах, но понимаем, что у нас часто пересекаются интересы и клиенты. Это хорошая конкуренция, сильная и игрок нам нравится, поэтому будем ускоряться.

(вгору)

Додаток 8

13.06.2017

Соцмережа Ukrainians хоче монетизувати контент користувачів без розміщення реклами

Українська соціальна мережа Ukrainians, яка створюється командою з 30 програмістів із канадської компанії StartupSoft разом з українкою Олександрою Струмчинською і поки що працює в режимі реєстрації, збирається надати користувачам можливість монетизувати унікальний контент. Про це Струмчинська розповіла в інтерв'ю LIGA.net (Центр підтримки журналістів).

«Наприклад, ви завантажуєте свою статтю, коли вона ще ніде не опублікована. Тільки в нашій соцмережі. Люди її шерять, лайкають, коментують, а ви отримуєте за це гроші. Ми будемо перерозподіляти прибуток від трафіку», – сказала вона.

Співзасновниця Ukrainians пояснила, що соцмережа існує за рахунок трафіку: переглядів і активностей, які відбуваються всередині неї. Тобто рекламу не потрібно буде розміщувати в своєму контенті. «Соцмережа заробляє гроші за рахунок своєї популярності. А популярність забезпечують користувачі. І ми будемо перерозподіляти гроші серед користувачів, які забезпечують цю популярність. Коли модель буде опрацьована, буде зрозуміліше», – додала Струмчинська.

Причім реклама в Ukrainians усе ж буде, але пізніше.

«Монетизація контенту – це частина функціоналу. І ми теж отримуватимемо частину від перерозподілених серед користувачів грошей. Це як на YouTube: ви отримуєте гроші не тільки за рекламу, а й за перегляди ваших відео. Будемо таким чином мотивувати користувачів створювати унікальний контент», – зазначила співзасновниця Ukrainians.

Першу функцію набору друзів творці соцмережі обіцяють відкрити вже за вісім днів, функція «Новини» повинна з'явитися через 16 днів. Увесь функціонал планується запустити до кінця вересня.

(вгору)

Додаток 9

8.06.2017

Соцмережі викликають клінічну депресію у підлітків

Гормональні сплески і соціальний тиск для багатьох підлітків – непосильна ноша. Стресові ситуації і постійне занепокоєння підвищують ризик розвитку депресії у юнацтва, особливо у дівчаток. У недавньому американському дослідженні, опублікованому в журналі Pediatrics, зафіксовано значний стрибок захворювання на депресію у юних дівчат за останні 6 років. Вчені пов'язують цей факт зі зростаючою залежністю від соціальних медіа у цій віковій групі. Психіатр Рамін Моджтабай і його колеги з Університету Джонса Хопкінса поставили собі за мету дізнатися, чи збільшився рівень депресії серед підлітків за останнє десятиліття. Вони проаналізували федеральні дані в період з 2005 по 2014 роки і виявили, що рівень депресії значно підвищився: цей стан було діагностовано у майже півтора мільйона підлітків, три чверті з яких – дівчата. «Отримані результати стали останньою ланкою в ланцюжку наукових досліджень, які доводять, що жінки будь-якого віку більш схильні до депресії, ніж чоловіки,» – сказала психолог Катрін Штайнер-Адер. Сучасні соціальні мережі і меседжери (Facebook, Instagram і Snapchat) посилюють цю проблему, підвищуючи залежність від громадської думки. Психолог Штайнер-Адер закликає школи проявити ініціативу в профілактиці депресивних станів у підлітків. Медитація, на її думку, є одним із найдієвіших інструментів. Практикувати медитацію Катрін Штайнер-Адер пропонує безпосередньо на шкільних заняттях. «Мозок дітей потребує відпочинку від сучасних технологій, – стверджує Штайнер-Адер, – концентрація уваги, вміння слухати себе показують важливість самотності та допомагають практикуючим відволіктися від смартфонів».+ У той же час, Рамін Моджтабай попереджає батьків, сімейних лікарів і вчителів про те, як важливо не пропустити будь-які зміни в поведінці підлітків. Симптоми депресії можуть включати проблеми зі сном, зниження апетиту та неуважність (ЖивиАктивно).

(вгору)

Додаток 10

8.06.2017

Российские журналисты узнали, куда тянутся нити управления ботами и троллями в соцсетях и на сайтах

Как устроен рынок «серого трафика» в российских СМИ, и почему об этом не принято говорить. Об этом в расследовании российской «Новой газеты» (ВЕРЖЕ).

Кто ведет ботов

Как устроен рынок «серого трафика» в российских СМИ, и почему об этом не принято говорить

На сайте «Новой» установлен счетчик от Mail.ru – благодаря ему мы отслеживаем динамику посещения страниц. Статистика отображается в разделе «СМИ/Газеты», где по числу уникальных пользователей мы находимся где-то между «Известиями» и «Независимой газетой». Рядом с нами в списке – «общественно-политическое издание «Подробности» (podrobnosti.biz/), у которого нет ни одной публикации – это пустая страница. Заглушка на сайте уже в течение нескольких месяцев гласит: «Приветствуем! Сайт только что создан». Тем не менее, счетчики регистрируют у «издания» десятки тысяч уникальных посетителей ежедневно.

Мы обратились к администрации Mail.ru с вопросом: «Каким образом у пустой страницы может фиксироваться такой трафик?» «Этот счетчик используется на сайте https://inforeactor.ru, у которого есть собственный счетчик. Мы снимаем с рейтинга этот дополнительный счетчик, согласно пункту правил», – ответили «Новой». Через несколько часов «Подробности» были удалены из рейтинга.

Архив интернета показывает, что вплоть до 2014 года «Подробности» были севастопольским новостным сайтом. В 2015 году под тем же доменным именем появились другие «Подробности» – работающие из Санкт-Петербурга под руководством Романа Кемеренко. В 2016 году сайт перебрасывал своих посетителей на проект «Инфореактор», существующий до сих пор. Кемеренко прежде сотрудничал с «Инфореактором», а сам этот сайт упоминался в недавнем расследовании РБК о том, что происходит в «рассаднике прокремлевских троллей» Ольгино. «Инфореактор» входит в «фабрику медиа», ассоциированную с небезызвестным «кремлевским поваром», миллиардером Евгением Пригожиным, – конгломерат сайтов с общей аудиторией в 36 млн посетителей в месяц. Так благодаря искусственной генерации трафика (ботов) в рейтингах популярных российских СМИ появляются откровенные фейки. Мы решили разобраться в том, как появляются цифры вроде тех, что до запроса «Новой газеты» показывал счетчик «Подробностей».

«Светлая сторона рынка»

– «Новая» уже наняла вам охрану? Это рынок с большими деньгами. Мало кто хочет писать о фродовом (мошенническом. – Ред.) трафике, – такими словами встречает меня собеседник, которого я с трудом уговорила побеседовать на тему бот-трафика в российских медиа. Окраина Москвы. Я сажусь к нему в машину. Говорить участник рынка согласен только на условиях анонимности.

Кроме ботов-программ существует еще «мусорный трафик» – случайные переходы пользователей, оказавшихся на сайте СМИ, например, через ссылку на порносайте.

Но мой собеседник утверждает, что его компания находится на «светлой стороне рынка»: работает только с живым трафиком. Рассказать о том, как накручивается трафик, его побудила борьба с нечестными конкурентами и нежелание заниматься «продажей воздуха». Схема бизнеса на ботах для человека, который вдруг решил в нем разобраться, выглядит сюрреалистично.

Мне объясняют на рисунке, как все работает. Вот в СМИ приходит живой трафик – реальные посетители. Это пользователи поисковых систем, соцсетей, новостных агрегаторов – и где-то рядом находятся боты, имитирующие поведение людей в интернете. В нормальной ситуации на вашем сайте может присутствовать около 5–10 % ботового трафика: ботам нужно мимикрировать под живой трафик.

Если их количество превышает 10 %, говорят мне представители «светлой стороны», значит, их покупают недобросовестные трафик-менеджеры или боты приходят в СМИ из обменных сетей. Чтобы увеличить свой рейтинг, некоторые СМИ используют партнерские системы обмена – устанавливают на сайт тизерный блок (ссылка, которая должна привлекать внимание пользователя – вроде «Шок! Что случилось с Филиппом Киркоровым»). Кликая на него, пользователь переходит на обменные сайты, например, такие как СМИ2, Lentainform, Infox.sg, 24СМИ, Directadvert и другие. Прямой обмен пользователями между СМИ не так выгоден, обменные сети предоставляют эффективные технологии, за счет которых можно привлечь внимание к контенту и увеличить аудиторию.

«Обменные сети обещают возвращать на СМИ новых пользователей с коэффициентом 1,2–1,5, объясняя это тем, что трафик умножается на промежуточной странице обменки, – продолжают анонимные эксперты. – На самом деле мы знаем, что никакая промежуточная страница не позволяет вернуть более 100 %. И чтобы компенсировать разницу, обменные сети сами закупают трафик и направляют на сайты СМИ. Если СМИ не следят за его качеством, то вместо реальных пользователей им возвращают ботов».

Так называемые CPA-сети (Cost Per Action, плата за действие) – это системы-посредники, которые предлагают рекламодателям оплачивать только целевые действия пользователей. Обменные сети, работающие с CPA, отправляют часть живых людей в воронку тизерных заголовков, похожих на журналистские материалы, но на самом деле ими не являющихся. «CPA-сети продают этих пользователей на страницы, обвешанные рекламой БАДов, порнотоваров и микрокредитов», – объясняют мои собеседники. Так пользователя последовательно ведут к нужному целевому действию.

Эксперты предлагают это легко проверить. Если перейти по тизерам обменной сети на промежуточную страницу и кликнуть на ней по новым тизерным блокам, то на экране может открыться даже поддельный сайт Минздрава с фейковыми «отзывами о лекарствах» и «советами». Мы проверяем

конкретный сайт – все верно. При клике на тизер страница автоматически открывается в новом окне. Текст «новости» прочитать невозможно – пользователь снова должен кликнуть на «Читать подробнее». В новой вкладке открывается текст в окружении рекламы о грибке, похудении народными средствами и омоложении.

«Покупая у обменок пользователя по 2–3 рубля, CPA-сети продают его разным БАДам за 5–10 рублей. Оборот CPA-сетей составляет до полумиллиарда рублей в месяц. Это очень высокорентабельный бизнес, – утверждает эксперт. – Заставить некачественные обменки делиться своими заработками со СМИ сложно. Их аргумент: мы же возвращаем вам больше, с коэффициентом, накручиваем вам рейтинг, помогаем отстраиваться от конкурентов, выполняем сложные трафиковые задачи, а у вас есть медийная реклама – монетизируйтесь сами. Но в реальности объем денег несопоставим, и ответа на вопрос, почему производители дорогого контента до сих пор соглашаются с этой деформацией рынка, нет».

Чем опасен ботовый трафик

Без покупки ботового трафика сегодня «практически невозможно сделать экономику медиапроекта и поднять рейтинг», на который смотрят рекламодатели, – уверен эксперт «светлой стороны». По его словам, рекламные бюджеты сегодня перетекают из традиционной рекламы в контекстную, из-за чего «медиа потеряли практически всех крупных рекламодателей, которых не устраивает эффективность их рекламы в СМИ». В этом они винят рекламодателей, которые предъявляют завышенные показатели для медийной рекламы, и конкурентов из числа самих СМИ, которые всеми возможными способами пытаются продемонстрировать эти показатели, чтобы не потерять бюджеты прямых рекламодателей: «Погоня за уезжающим поездом привела к тому, что накрутка рекламы и трафика стала в СМИ нормой».

Алексей Аметов, издатель Look At Media, считает лукавством утверждение, что все рекламодатели уходят в контекстную рекламу: «Для многих брендов критически важно инвестировать в имиджевую рекламу, и, более того, наличие имиджевой рекламы улучшает результаты в контексте. Это подтверждает и статистика – контекстная реклама растет быстрее, но медийка тоже пока растет, а не падает». С другой стороны, он уверен, что все участники рынка внимательнее относятся к выбору площадок и отслеживанию KPI. Поэтому и СМИ можно и нужно следить за трафиком.

Аметов говорит, что за последние годы ситуация начала улучшаться, крупные издания стали отказываться от таких методов. Но менее разборчивые проекты работают по-старому: «Серые схемы продолжают использовать, чтобы откровенно мошенничать с рекламой. Это проблема «мусорного трафика» из живых пользователей, которых за счет тизеров из громких заголовков гоняют по разным группам сайтов – для откртки показов рекламы или для отчетности перед инвесторами».

Маргинальные «трешевые» издания уровня фейк-ньюз нагоняют трафик и монетизируют его через автоматичекие продажи, в частности, сетей «Гугла»

и «Яндекса», а не через прямые продажи рекламы. Новая медийная империя в Ольгине, о которой написал РБК, – показательный пример, уверен Аметов: «Простых доверчивых людей с низким критическим мышлением вовлекают в аттракцион громких заголовков и «крутят» на нем, пока их не укачает».

Борис Омельницкий, директор по развитию AdFox, компании, входящей в структуру «Яндекса», не видит проблемы в том, что рекламодатели сегодня меньше заинтересованы в медийной рекламе. «80 % российской интернет-рекламы закупается по моделям оплаты за результат, то есть перформанс-рекламы. Оставшиеся 20 % – покупают показы». Омельницкий уверен: если сама площадка хочет показать трафик, которого на самом деле нет, это сработает только один раз, так как существует достаточно метрик, показывающих качество размещений на любых сайтах. «Рекламодатели имеют достаточно инструментов, чтобы защитить эффективность вложений в рекламу. В интернете все очень прозрачно», – заключает он.

«Серый трафик» может быть нужен медиа в двух целях: чтобы обманывать рекламодателя или чтобы рассказать о своей влиятельности, – считает Антонина Самсонова, CEO и основатель TheQuestion. «Если вы государственное медиа и вам надо отчитываться о том, что ваш контент кто-то читает в интернете, чтобы получить очередной госзаказ, тогда, возможно, вы накручиваете цифры просмотров, такие случаи были. На конкурентном негосударственном рынке существуют стандарты, по которым заказчики оценивают объем аудитории площадки. В России принято ссылаться на «Яндекс.Метрику» или Google Analytics, их репутации можно доверять».

По мнению Самсоновой, рекламодатели и рекламные агентства тратят собственные деньги или деньги клиентов, а не государственные средства на продвижение в сети, и потому в первую очередь заинтересованы, чтобы оценка была объективная. «На мой взгляд, проблема ботов не является системообразующей. Возможно, кто-то кого-то при помощи ботов обманывает. Но объем сделок, в которых используется эта технология, настолько незначителен по сравнению с объемом рекламного рынка, что можно сказать: те клиенты, которые не проверяют и не анализируют качество трафика и возврат от инвестиций в рекламу, – просто очень странные люди».

Битва с ботами

Возможность передачи ботов через обменные сети подтвердили «Новой газете» в проекте «Кракен Антибот». Виктор, специалист по анализу трафика, пояснил, что схема уже давно ни для кого не является секретом: «Вы отдаете живых пользователей, а вам приходит такое же количество бот-трафика под видом живых. Полгода назад один крупный портал попросил нас проверить их трафик. Процент бот-трафика оказался небольшим, так как посещаемость портала сама по себе была приличной. Но в том бот-трафике были переходы из 90% всех популярных трафикообменных сетей Рунета». Что это за ресурс, Виктор рассказывать отказался.

Такая схема, как оказалось, никого из интернет-экспертов тоже не удивляет. О том, что некоторые обменные сети вышли из доверия и

подозреваются в генерации бот-трафика, было известно каждому, кто согласился комментировать тему. «Мы изначально отказались от партнерских блоков, потому что мы хотим быть уверены в том, что наши посетители настоящие, — рассказал Иван Засурский, заведующий кафедрой новых медиа и теории коммуникации факультета журналистики МГУ им. М.В. Ломоносова. — Я доверяю своей посещаемости, у меня трафик органический, и мои издания «Частный корреспондент» и «Научный корреспондент» не участвуют ни в каких системах обмена трафика. Чтобы самих себя не обманывать. Пусть посетителей сто тысяч в месяц, зато они реальные. Обменные сети дают трафик, но они и создают риск».

Риски при использовании обменных сетей также подтвердил Алексей Аметов: «Тут важно понимать, что если издатель пытается за три копейки увеличить аудиторию своего сайта, то он получает ботов или людей, которые вообще никак не могут быть аудиторией его СМИ». В то же время Аметов отметил, что если издатель меняется с другими СМИ промоблоками и делает это вдумчиво и адекватно, то проблем нет.

Антон Меркуров, интернет-эксперт, также согласен, что накрутка с помощью некачественного трафика действует на рынке среди прочих технологий: «Процент накрученной рекламы всегда есть. Многие не самые качественные СМИ их используют. И ботовый трафик все равно иногда покупают». Для накрутки трафика сайты используют обменки, подкручивают ботов, чтобы показать кому-то какую-то мнимую статистику. Меркуров советует пользоваться Google Analytics, чтобы разобраться в качестве трафика. «Редакция СМИ на самом деле не всегда влияет на трафик и имеет к нему отношение. Этим занимаются трафик-менеджеры, как правило, – люди со стороны. К ним и должны быть претензии». Об обменных сетях Меркуров также отозвался скептически: «Обменки – не самые красивые рекламные инструменты. Там есть риск накрутки ботами».

«Рынок очищается»

Мы обратились за комментариями к крупнейшему игроку на рынке – СМИ2, включающему в себя обменную сеть и агрегатор новостей. Гендиректор компании Анна Иванова утверждает, что для СМИ2 ботовый трафик также представляет серьезную проблему: «Вся наша модель продаж завязана на действиях, для нас важен живой трафик. Именно поэтому около четырех лет назад мы начали писать собственную систему «Антибот».

По словам Ивановой, год назад СМИ2 разработало собственные процедуры для анализа поведения пользователей, потому что поведение ботов становится все больше похожим на человеческое. «Огромная часть заработанных денег уходит на подобные разработки, то есть борьбу с ботовым трафиком. Мы единственные среди обменных сетей, у кого есть система «Антибот», которую мы постоянно совершенствуем именно для того, чтобы отлавливать накрутчиков и сообщать об этом нашим партнерам», — поясняет Иванова. Она называет СМИ2 официальным агрегатором и подчеркивает, что

он входит в список Роскомнадзора, то есть компания раскрывает статистику, а значит, «не участвует ни в каких накрутках».

Сам бизнес обменной сети Иванова называет тяжелым и в какой-то степени неблагодарным, при условии, если играть честно: «Монетизировать и зарабатывать возможно, только когда у тебя огромный объем трафика. До этого момента нужно все время инвестировать в ресурс или иметь крупного партнера, который будет помогать выйти на нужный уровень, когда ты сможешь отдавать живой трафик и экспериментировать с контентом. У нас этот процесс занял около двух лет, но теперь мы зарабатываем».

Иванова соглашается с тем, что на рынке действительно много недобросовестных игроков среди обменных и тизерных сетей: «Если трафик монетизирован, то начинаются танцы с бубнами – отдавать партнерам нечем, и в ход идут разнообразные методы накрутки. Причем это не обязательно боты. Это могут быть и фреймы (одна интернет-страница встраивается во фрагмент другой страницы), перезагрузка дважды одной страницы». С другой стороны, в СМИ2 не считают, что проблема ботов стоит слишком уж остро. Как и другие участники рынка и эксперты, Анна Иванова поинтересовалась, не заказал ли «Новой» кто-нибудь этот текст. И отметила, что ботовый трафик осложнял жизнь участникам рынка несколько лет назад, но сейчас писать об этом, возможно, уже поздно.

Ботоводы и ботоловы

Следующим шагом было найти экспертов на рынке ботоводов и ботоловов. Нам повезло найти такого эксперта в одном лице.

Ботоловы смотрят в первую очередь, с какого IP-адреса или с какого обменника заходил бот. Бот может представиться сайту девушкой, которая ищет губную помаду, или мужчиной в поисках автомобиля. При этом боты работают на особом ПО. «Если по определенному протоколу «постучаться» к этой программе и спросить ее: «Ты бот?» – она ответит положительно. А если не бот – промолчит, – объясняют ловцы ботов. – Также у нас двойная верификация: сначала мы сканируем ботов, а потом просто выкупаем одного и заставляем выполнить определенные задачи. Таким образом, всегда можно доказать, что это действительно бот».

Существует три вида ботов: неуправляемые – им дается адрес, и они могут просто зайти на страницу; управляемые – со сценарием: зашел на страницу, кликнул, заполнил форму, зарегистрировался; и мотивированные трафики, в рамках которых живые пользователи, которые что-то получают взамен, совершают действия по типу неуправляемых или управляемых ботов.

Выявить всех ботов в своем трафике СМИ самостоятельно не смогут, уверены ловцы ботов, которые зарабатывают на этом. Мастерство ботовода позволяет подделать даже поведенческий показатель, как микроподергивания мышкой и историю посещения страниц в сети. «Наши специалисты способны так «причесать» бота, что «Яндексом» из 100% ботового трафика будет распознано лишь 5%», – хвастается ботовод.

Уже во время подготовки текста к печати нам поступило предложение от СМИ2 раскрыть трафик сети: «Приезжайте в любой момент в гости, у нас нет ни фрода, ни ботов. Скрывать нам нечего». В целом о ботах в СМИ эксперты отчего-то говорят очень неохотно.

(вгору)

Додаток 11

13.06.2017

Дарина Шварцман

Более половины украинцев называют онлайн-медиа и соцсети главными источниками пропаганды

Почти 55 % украинцев считают главным источником российской пропаганды онлайн-медиа и социальные сети. Таковы результаты общенационального исследования «Осведомленность и отношение к проблемам дезинформации и пропаганды в СМИ», инициированного проектом StopFake (InternetUA).

Об этом в ходе пресс-брифинга рассказала заместитель директора Могилянской школы журналистики по вопросам исследований Дарья Орлова.

Отмечается, что 58 % украинцев признают угрозу российской пропаганды и дезинформации.

При этом, существуют региональные различия в отношении к российской пропаганде. 42 % опрошенных из южного и 46 % из восточного регионов считают, что угрозы не существует. Хотя общенациональный срез показывает, что только треть опрошенных признает угрозы.

Среди главных источников пропаганды 45 % опрошенных отмечают российские телеканалы, 34,5 % – онлайн-медиа, более 20 % – социальные сети.

Всего треть опрошенных испытывают потребность в повышении собственной медиаграмотности. Большинство считает, что способны отличить правдивую информацию от ложной. В восточных и южных областях их процент выше, чем в других регионах. «Несмотря на общий процент неуверенности и растерянности относительно того, откуда идет пропаганда, жители восточных и южных регионов достаточно уверены в своей способности отличить истинные факты от ложных», – говорит Дарья Орлова.

33,8% опрошенных указывают на то, что проблема пропаганды существует также среди украинских СМИ.

Опрос охватил 110 населенных пунктов. Дополнительно опросили 2 фокус-группы в Донецкой области. Исследование провел Киевский международный институт социологии.

(вгору)

Додаток 12

1.06.2017

Facebook, Twitter и YouTube не справляются с удалением разжигающих ненависть постов

Социальные сети в среднем удаляют только шесть разжигающих ненависть постов из десяти. В основном публикации содержат ксенофобские и исламофобские высказывания (Deutsche Welle).

Facebook, Twitter и YouTube в Европе не справляются с задачей удалять в течение 24 часов разжигающие ненависть посты в социальных сетях. Об этом 1 июня сообщает газета Die Welt со ссылкой на специальный доклад Еврокомиссии.

В общей сложности удаляется шесть таких постов из десяти. В течение суток – только каждый второй пост, еще 20 процентов – в течение 48 часов, 15 процентов остаются опубликованными около недели. 13 процентов – еще дольше. Facebook удаляет примерно две трети постов, на которые поступили жалобы, Twitter – 37,5 процента, YouTube – 66 процентов. В декабре 2016 года эти показатели у соцсетей были значительно ниже, как и скорость реакции на такие публикации.

Брюссель критикует Facebook за отсутствие пояснений

Брюссель, зафиксировав прогресс соцсетей в этом направлении, также отметил недостатки – в частности то, что Facebook не сообщает пожаловавшимся на посты пользователям о своих действиях и не поясняет своего решения в том случае, если не удаляет публикацию.

Год назад Еврокомиссия и Facebook, Twitter, YouTube и Microsoft согласовали кодекс поведения, который предполагает борьбу с разжигающими ненависть и пропагандирующими терроризм комментариями в социальных сетях. Еврокомиссар по вопросам юстиции Вера Юрова тогда заявила о необходимости проводить проверку вызывающих подозрение публикаций в течение 24 часов.

Темы постов

Среди разжигающих ненависть постов по 18,1 процента приходятся на ксенофобские и исламофобские высказывания, 16,3 процента – об этническом происхождении, в 12,9 процента упоминается сексуальная ориентация, в 9,2 процента – национальность.

Далее идут посты, содержащие антисемитские и расистские высказывания (8,9 и 8,8 процента соответственно), а также разжигание ненависти по признаку религии (4,7 процента) или пола (2,9 процента).

Еврокомиссия исследовала поведение интернет-компаний в 24 странах Европы в период с марта по май 2017 года на примере более 1,5 тысяч случаев.

В Германии могут ужесточить ответственность соцсетей

В июне немецкий бундестаг рассмотрит законопроект об ужесточении ответственности администрации социальных сетей за появление на их сайтах разжигающих ненависть комментариев и фейковых новостей, пишет Die Welt.

Документ обязывает операторов соцсетей удалять или блокировать посты, содержащие клевету или разжигающие ненависть, в течение 24 часов

после получения жалобы. Предполагается также, что администраторы социальных сетей ежеквартально должны представлять отчет о том, каким образом они отреагировали на поступившие в этот период жалобы. Документ предусматривает штрафы для физических лиц, ответственных за нарушения, в размере до пяти миллионов евро, фирмам может грозить штраф до 50 млн евро.

Законопроект предложил министр юстиции и защиты прав потребителей ФРГ Хайко Маас (Heiko Maas). По его словам, пока что не все социальные платформы серьезно относятся к жалобам пользователей о появлении противоправных комментариев или постов.

Соцсеть Facebook выступила против закона, заявив, что за подобные вещи ответственность должно нести государство. Инициативу Мааса также раскритиковали журналистские организации.

(вгору)

Додаток 13

31.05.2017

В украинской блокировке соцсетей России есть смысл – WSJ

Украина пошла на радикальный шаг в кибервойне с Россией, когда заблокировала российскую версию Facebook для своих пользователей (Finance.Ua).

«ВКонтакте» и «Одноклассники» были популярны в Украине, как и в других постсоветских странах. В Киеве свое решение объяснили тем, что эти сайты служат российской пропаганде.

Эксперты по кибербезопасности, со своей стороны, добавляют, что соцсети представляют еще большую опасность, став стартовыми площадками для хакерских атак. По словам специалистов, социальные сети позволяют хакерам собирать личные данные о людях, которых собираются атаковать, а также использовать как платформу для размещения вредоносных программ.

«В Украине подобные атаки могли иметь смертельный характер», – говорится в статье.

После того, как на Востоке Украины началась война, американская компания по кибербезопасности CrowdStrike обнаружила, что российские хакеры, связанные с группой APT 28, распространили через «ВКонтакте» вирус для приложения для Android. Вредная программа проникла в программное обеспечение для украинских артиллеристов, которое разработал Ярослав Шерстюк.

Программа позволяла рассчитать данные для наведения украинских гаубиц. Однако российский вирус позволил сломать программу и определять местоположение украинской артиллерии, чтобы потом российские силы могли нанести по ним удар.

Издание пишет, что в прошлом году российские хакеры пытались даже вывести из строя электроподстанцию в Киеве.

Другая кибершпионская группа из России Sandworm устроила атаку на электросеть в Западной Украине. Об этом изданию рассказал аналитик компании FireEye Джон Халтквист. «Случаи в Украине дают возможность получить информацию о противнике до того, как он устроит новые атаки на Западе», – отметил американский эксперт.

По его словам, вредоносный код Sandworm, который обнаружили в Украине, был замечен и в электроэнергетической сети США.

(вгору)

Додаток 14

31.05.2017

Евгения Подгайная

Нацполицию не интересуют наработки Совета Европы по киберпреступности

Нормы скандального законопроекта Нацполиции «О внесении изменений в некоторые законодательные акты относительно имплементации отдельных норм Конвенции о киберпреступности» необоснованно расширяют полномочия силовиков, полагают в ИнаУ (InternetUA).

Интернет ассоциация направила в Кабмин целый ряд замечаний к проекту.

Выдержки:

– У проекті Закону пропонується: «у разі неможливості здійснення копіювання інформації з технічних причин, у тому числі зашифрованої» проводити вилучення інформаційних систем або їх частин, мобільних терміналів систем зв'язку на строк, достатній для дешифровки та/або огляду інформації, після чого вони повинні бути якнайшвидше повернуті володільцю, окрім випадків, визначених у частині першій статті 100 КПК України. Необхідно встановити чіткі строки вилучення інформаційних систем або їх частин, мобільних терміналів систем зв'язку. Застосування таких виразів як «достатній строк», «якнайшвидше» буде незрозумілим та нечітким у їх застосуванні та матиме наслідком порушення прав операторів, провайдерів телекомунікацій.

– Змінами пропонується запровадити тимчасове обмеження доступу до інформації, яке полягає в блокуванні (обмеженні) провайдерами та операторами телекомунікацій передачі інформації з/чи на визначений (ідентифікований) інформаційний ресурс (інформаційний сервіс), адреси мережі Інтернет, домену тощо на підставі ухвали слідчого судді. Проте, ІнАУ вже неодноразово наголошувала, звертаючись до державних органів, що блокуванню (обмеженню) повинна підлягати саме заборонена інформація, що має взаємодію та вплив на припинення злочину, а не весь інформаційний ресурс, на якому може бути розміщена така інформація.

– Пропонується надати слідчому та прокурору право до постановлення ухвали слідчого судді звернутися з письмовою вимогою до оператора,

провайдера телекомунікацій про здійснення строком на 24 години негайного тимчасового обмеження доступу до інформації та/або термінову фіксацію інформації в електронній (цифровій) формі, лише у невідкладних випадках, пов'язаних із врятуванням життя людей та майна чи припинення тяжкого чи особливо тяжкого злочину з подальшим зверненням з відповідним клопотанням до слідчого судді. Однак, відповідно до пункту 4.5 Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.2016 № 96, передбачено запровадження блокування операторами та провайдерами телекомунікацій відповідних ресурсів за рішенням суду.

Самое интересное, что при финансировании Совета Европы разработан более качественный проект изменений в УПК по имплементации нашего законодательства с нормами Конвенции о киберпреступности.

Зачем тратить средства и проталкивать достаточно спорный законопроект Нацполиции – вопрос риторический.

В направленном в Кабмин обращении ИнАУ настаивает использовать законодательные предложения, разработанные группой экспертов Совета Европы и отечественных специалистов в рамках проекта «Киберпреступность@Восточное партнерство».

(вгору)

Додаток 15

31.05.2017
СМИ: Силовики повально читают переписку украинцев

Силовики все чаще стали просить доступ к электронным ящикам украинцев. В них ищут как доказательства вины подозреваемых в мошенничестве, так и смотрят переписку чиновников, а также тех, кого винят в разглашении коммерческой тайны. А недавно силовики хотели порыться в ящике пользователя «Яндекса», который, по их мнению, был причастен к организации крестного хода в прошлом году. Юристы говорят: зачастую следствие не имеет никаких оснований на доступ к почте, пишут Вести (From-UA. Новости Украины).

В Реестре судебных решений можно найти немало дел, когда силовики просят доступ к электронной почте. Например, в 2015 году следователь в Полтавской области ходатайствовал о вскрытии ящика сотрудника «Укртатнафты». По мнению следствия, мужчина разглашал коммерческую тайну через свою электронку на «Яндексе», а затем публиковал ее в интернете в искаженном виде. Суд пошел навстречу следствию.

Также правоохранители просили доступ к почтовым ящикам «Яндекса» и Mail.Ru львовянина, который торговал базами данных (паролями и логинами) и получал за это вознаграждение через систему WebMoney. А СБУ затребовала доступ к почтовому ящику секретаря Лисовской сельрады Донецкой области, которая со своего личного ящика отправляла почту с данными граждан, хотя должна была делать это только с официальной почты gov.ua или .укр.

Насколько легко силовики могут добраться до наших почтовых ящиков, имея решение суда? Президент холдинга «Интернет Инвест» Александр Ольшанский считает, что даже решение суда не всегда дает зеленый свет. «Смотря, на каком сервисе находится ваш почтовый ящик. Если это Google, то как вы себе представляете, что американская компания так просто даст доступ.

Что для них решение украинского суда? Силовому органу, тем более СБУ или прокуратуре, придется серьезно обосновать свой интерес, и это сложно сделать. А Google и правоохранительные органы его страны будут задавать следователям встречные вопросы: в чем вы подозреваете, какие у вас основания. И если это не связано с убийством, наркотиками или оружием, то силовикам вряд ли удастся достичь цели», – говорит Ольшанский.

Руководитель Лаборатории компьютерной криминалистики Сергей Прокопенко также полагает, что тяжелее всего силовикам проникнуть в ящики, которые расположены на доменах Google.

«Если это дело не связано с терроризмом или детской порнографией, то получить доступ у Google практически невозможно. Там будут просить все новые и новые доказательства вины человека. Также они могут предоставить только данные IP, но не дать содержание этого ящика. Что касается почты на украинских сервисах, то тут силовикам легче – в соответствии с законом наши компании должны предоставить информацию в течение 30 дней. Кроме того, если вы переписку удаляете, а еще и регулярно чистите корзину, то восстановить информацию невозможно», – советует Прокопенко.

По его словам, силовики действительно в последнее время все чаще интересуются почтовыми ящиками украинцев, поскольку там можно найти много нужного. Но существует способ, когда силовики могут вскрыть вашу переписку и, мягко говоря, незаконным способом. «Например, когда вам на почту приходит письмо, вы его открываете, и отправителю становятся доступны все ваши данные. Вы и не поймете, кто это сделал. Также в интернете иногда появляются сливы адресов, паролей и логинов – их также могут использовать силовики для незаконного входа в вашу переписку. Потом уже могут через суд все, как нужно, оформить, вы и не догадаетесь», – говорит на условиях анонимности представитель IT-компании.

Адвокат Ростислав Кравец подтверждает, что в последнее время обращение силовиков в суды с просьбой дать доступ к электронным ящикам стало нормой. «Прослеживается весьма нехорошая тенденция: у налоговиков, следователей, полиции, СБУ, прокуратуры нет особых доказательств вины человека, и они, роясь в переписке, ищут, за что им зацепиться. Даже бывает такое, что ходатайство вскрыть почту появляется в суде раньше, чем человека в чем-то подозревают. Для таких решений силовики выбирают суды не в Киеве, а в провинции. Причем в исках они даже свой интерес к почте ничем не обосновывают. Просто просят: дайте – и все!» – рассказал Кравец.

Адвокат Виталий Наум добавляет: «У меня десятки таких дел, где оперативники используют доступ к электронной почте. Правда, о том, что вашу переписку читали, вы узнаете тогда, когда дело передается в суд. Защититься от

этого невозможно, поскольку, если перед следователями будет стоять задача добыть информацию, они будут добывать ее любым путем».

(вгору)

Додаток 16

31.05.2017

Интернет в Украине может оказаться под жестким контролем

В Украине подготовлен законопроект о контроле за украинским Интернетом. (IPnews).

Эксперты говорят, что принятие документа вынудит основную часть неподконтрольных и независимых компаний уйти с рынка.

Последнее время участники телеком-рынка негодуют из-за готовящегося законопроекта Нацполиции о контроле за украинским Интернетом. Скан проекта выложил на Facebook-странице глава Пиратской партии Украины Сергей Ярыгин. Этот же скан опубликовал и основатель компании Адамант Иван Петухов.

В проекте говорится, что провайдеры должны за свой счет установить оборудование, которое позволит собирать информацию о трафике и предоставлять правоохранительным органам компьютерные данные, необходимые для следственных действий и слежке за украинцами и их политическими предпочтениями в сети.

Согласно проекту, правоохранители смогут приходить к провайдеру и копировать нужную информацию, в том числе зашифрованную. Если копию не получится сделать по техническим причинам, правоохранители имеют право изъять информационные системы на срок, необходимый для дешифровки.

Получать от провайдера данные о трафике правоохранители смогут без решения суда. Следователь или прокурор получат право письменно потребовать от провайдера немедленно ограничить доступ к определенной информации на 24 часа. В проекте уточняется, что делать это можно только в экстренных случаях: чтобы предотвратить тяжкие преступления, защитить человеческую жизнь или имущество.

Также провайдеры должны будут создать реестр веб-ресурсов, через которые осуществляется незаконная деятельность.

Учитывая широкую доступность Интернета и увеличивающееся число пользователей (уже более 3,5 млрд. человек или около половины всего населения планеты), регулирование электронного контента стало важным направлением работы правительств и наднациональных органов по всему миру.

Что запрещают в Интернете разные страны?

Обобщённо можно выделить несколько категорий информации, свободный доступ к которой в Интернете государства пытаются ограничить, а именно: социально-опасную, нарушающую авторские права, угрожающую национальной безопасности, политически нелояльную и позволяющую обойти установленные запреты.

Знаменитая фраза действующего Президента США Била Клинтона, который в 1998 году сравнил усилия Китая по внедрению Интернет-цензуры с «попыткой прибить желе к стене» была опровергнута временем и технологиями. Сегодня можно говорить о наличии технических возможностей многих стран ограничивать доступ к запрещенным ресурсам с приемлемой эффективностью. Доля пользователей, которые готовы терпеть неудобства, используя специальные инструменты, или идти на риск, нарушая закон, ради проникновения на запрещенные сайты, составляет около 2 %.

Используется также метод блокировки на популярных поисковиках. Суть его в том, что по индивидуальным соглашениям правительств с поисковыми сервисами, последние исключают из результатов поиска ссылки на запрещенные материалы. Поисковики блокируют выдачу ссылок на контент, при этом сам контент остаётся доступным. Например, вследствие запрета на распространение неонацистских материалов в Германии и Франции немецкая и французская версии Google исключает из поисковых результатов ссылки на соответствующий контент. При использовании международной версии Google результаты запросов не фильтруются. Таким образом, метод не является очень эффективным, т.к. ручной ввод нужной ссылки позволяет его обойти.

Широко используются также «добровольно-принудительные» способы ограничения доступа к нежелательной, по мнению властей, информации.

Программное и аппаратное обеспечение, позволяющее осуществлять Интернет-цензуру, может устанавливаться: 1) на точках доступа, соединяющих национальную сеть с международными магистралями; 2) на оборудовании провайдеров, предоставляющих доступ к Интернету; 3) на серверах сетевых организаций; 4) на компьютерах пользователей.

В первом случае модель фильтрации позволяет полностью унифицировать подходы и гарантированно охватить всех пользователей, хотя очень финансово-затратна в применении.

Фильтрация на уровне Интернет-провайдеров применяется некоторыми европейскими странами, а также Вьетнамом, Бирмой, Южной Кореей. Она предполагает наличие реестра ресурсов, подлежащих блокировке, который наполняется решениями судов и/или решениями специальных органов.

Цензура на серверах сетевых организаций применяется частными компаниями для контроля за своими сотрудниками, а также используется государствами для регулирования работы школ, библиотек, и правительственных учреждений. В США, например, в соответствии с Актом о защите детей в Интернете условием получения государственных субсидий для школ и библиотек является установка фильтров, ограничивающих доступ несовершеннолетних к порнографии. Поскольку требование не является обязательным для всех учреждений, а закон предусматривает отключение фильтров по просьбе взрослых пользователей, Акт не ограничивает свободу слова, закрепленную в Конституции США.

Установка программного обеспечения непосредственно на компьютеры пользователей не позволяет проконтролировать удаление или отключение

фильтра. Поэтому метод может быть эффективен лишь для родительского контроля за детьми, а также в случаях, когда сисадмины компаний могут технически заблокировать доступ пользователей к определенным настройкам.

(вгору)

Додаток 17

4.06.2017

В ЕС намерены ужесточить контроль соцсетей

А в Европе борются с ксенофобскими и экстремистскими публикациями в соцсетях. Но... практически безуспешно. Почему не справляются и какие штрафы грозят европейским компаниям? Подробнее – Татьяна Логунова (podrobnosti.ua).

Не справляются. Социальные сети не успевают удалять комментарии и посты, разжигающие ненависть. К такому выводу пришли эксперты Еврокомисии, которые проанализировали контроль за публикациями в европейском сегменте интернета. В специальном докладе организации говорится – в среднем соцсети блокируют только 6 из 10-и подобных материалов.

Ксенофобские, исламофобские и прочие, разжигающие ненависть публикации, должны быть удалены – об этом европейские чиновники и руководители соцсетей договорились еще прошлым летом. И установили срок – в течение суток с момента появления.

Спустя год, подвели первые результаты – прогресс есть, но пока недостаточный.

Соцсети блокируют чуть больше половины постов и комментариев, и те – в течение недели. И это при том, что для контроля за контентом компании набирают дополнительный штат сотрудников. Так, например, Facebook в следующем году возьмет на работу три тысячи «контролеров». Они будут следить, чтобы пользователи не публиковали видео со сценами насилия, фейковые новости и так далее. Об этом на своей странице объявил основатель сайта Марк Цукерберг.

«Facebook делает все возможное для того, чтобы на его страницах не появлялись видео со сценами насилия, фековые новости. Это важно как для акционеров, так и для имиджа компании», – говорит Хиллари Крамер, инвестиционный аналитик.

Заставить соцсети эффективнее контролировать свой контент – пытаются и отдельные страны ЕС. Например, в Германии планируют штрафовать компании, которые не будут своевременно удалять разжигающие ненависть материалы.

Не удалили – заплатите штраф. Уже в этом месяце немецкий Бундестаг рассмотрит законопроект, который ужесточит ответственность соцсетей за появление на их страницах подобных публикаций. Документ предлагает наказывать компании финансово. Штраф баснословный – 50 миллионов евро.

(вгору)

Додаток 18

8.06.2017

У Держдуму внесли законопроект про заборону обходу блокування сайтів

У Держдуму Росії внесено законопроект, який забороняє використання технологій, що дозволяють обходити блокування сайтів. Відповідний документ опубліковано на сайті нижньої палати російського парламенту (LB.ua).

Крім того, пропонують зобов'язати пошукові системи «припиняти видачу посилань на заблоковані в Росії інформаційні ресурси».

Авторами документа виступили депутати Максим Кудрявцев («Єдина Росія»), Микола Рижак («Справедлива Росія») і Олександр Ющенко (КПРФ).

У квітні «Ведомости» повідомляли, що в Росії розробили законопроект, який забороняє використовувати інформаційні системи і програми, що дозволяють користувачам обходити блокування сайтів із забороненим контентом.

Джерела видання відзначали, що автор проекту – Роскомнагляд, документ підготовлено з ініціативи Радбезу РФ. Він пояснив, що суть законопроекту в тому, щоб зобов'язати анонімайзери і VPN-сервіси блокувати сайти з реєстру заборонених ресурсів.

Оновлено: Уповноважений із захисту прав підприємців в інтернеті Дмитро Мариничев назвав «безумством» законопроект про заборону використання технологій, які дозволяють обходити блокування сайтів, передає РБК.

«Усе це йде врозріз зі здоровим глуздом. У законопроекті йдеться про технології, які дозволяють обходити блокування. Передусім це VPN і анонімайзери. Як вони будуть відокремлювати VPN, який використовується в комерційних цілях, від VPN, який використовується для обходу блокування? Це неможливо визначити», – сказав Маринич.

Він зазначив, що технічно можна заборонити використовувати VPN на кінцевих пристроях. Однак омбудсмен назвав це «переслідуванням власних громадян» і порівняв із забороною «вставляти у двері замки».

(вгору)

Додаток 19

31.05.2017

WSJ: «ВКонтакте» стала майданчиком для хакерських атак

Видання Wall Street Journal випустило статтю, в якій розповідається про загрози російських соцмереж «ВКонтакте» і «Одноклассники» (Корреспондент.net).

Експерти з кібербезпеки вважають, що соцмережі представляють ще більшу небезпеку, ніж пропаганда, ставши стартовими майданчиками для хакерських атак, стверджує видання.

Соціальні мережі дозволяють хакерам збирати особисті дані про людей, яких збираються атакувати, а також як платформу для розміщення шкідливих програм.

«В Україні подібні атаки могли мати фатальний характер», – йдеться в статті.

Після того, як на сході України почалася війна, американська компанія з кібербезпеки CrowdStrike виявила, що російські хакери, пов'язані з групою APT 28, поширили через «ВКонтакте» вірус для додатка для Android. Шкідлива програма проникла в програмне забезпечення для українських артилеристів, яке розробив Ярослав Шерстюк. Програма дозволяла розрахувати дані для наведення українських гаубиць. Однак, російський вірус дозволив зламати програму і визначати місце розташування української артилерії, щоб потім російські сили могли завдати по них удару.

Видання пише, що торік російські хакери намагалися навіть вивести з ладу електропідстанцію в Києві. Інша кібершпигунська група з Росії Sandworm влаштувала атаку на електромережу в Західній Україні. Про це виданню розповів аналітик компанії FireEye Джон Халтквіст.

«Випадки в Україні дають можливість отримати інформацію про противника до того, як він влаштує нові атаки на Заході», – зазначив американський експерт.

За його словами, шкідливий код Sandworm, який виявили в Україні, був помічений і в елетроенергетичній мережі США.

(вгору)

Додаток 20

31.05.2017

Хакеры слили в Сеть 25 тыс. фотографий клиентов клиники пластической хирургии

30 мая хакеры из Tsar Team опубликовали в интернете архив литовской сети клиник пластической хирургии Grozio Chirurgija – 25000 фотографий (в том числе в обнаженном виде) и персональные данные клиентов. Среди них оказались жители более чем 60 стран мира; многие из них получили от хакеров сообщения с требованием выкупа, сообщает The Guardian (InfoResist).

Базу данных похитили еще несколько месяцев назад: сначала хакеры потребовали от клиники выкуп в размере 300 биткоинов (то есть 650 тысяч долларов), затем сделали скидку до пятидесяти биткоинов (чуть больше 100 тысяч долларов). После того как представители клиники отказались сотрудничать с преступниками, те опубликовали архив: первую часть в марте, оставшуюся – 30 мая.

Все это время хакеры шантажировали людей, сделавших пластические операции в клинике: преступники угрожали опубликовать их фото из медицинских карт (как правило, это до и после коррекции внешности). В качестве выкупа они требовали сумму в биткоинах, эквивалентную 50–2000 евро.

Литовская полиция предупредила, что все скачавшие архив также могут стать участниками дела, которое расценивается как вымогательство. Представители клиники просят клиентов не поддаваться на угрозы шантажистов и немедленно обращаться в полицию, если с ними на связь выйдут хакеры.

Tsar Team – одно из названий хакерской группировки, также известной как APT28, Sednit, Fancy Bear, Sofacy и Pawn Storm. Она, предположительно, стоит за атаками на американских демократов; по некоторым данным, ее следы ведут в Россию. Пока неизвестно, кто именно атаковал литовскую клинику и ее клиентов: сами Tsar Team или же не связанные с ними хакеры, прикрывшиеся их именем.

(вгору)

Додаток 21

1.06.2017

Windows 10 следит за пользователями даже при отключенной телеметрии

Microsoft неоднократно подвергалась критике за сбор большого количества телеметрических данных в Windows 10. Компания доказала, что прислушивается к мнению своих клиентов и с выходом обновлений предоставила пользователям больший контроль над конфиденциальностью. Тем не менее, по словам ИБ-эксперта Марка Барнетта (Mark Burnett), многие годы посвятившего разработке Windows, даже ограничительные настройки не мешают Windows 10 Enterprise Edition отправлять данные на серверы Microsoft (InternetUA).

Как пояснил Барнетт, пользователи Windows 10 Enterprise Edition действительно могут отключить телеметрию, однако даже с инструкцией это не так легко сделать. Пользователям придется изменить практически все установленные по умолчанию настройки, иногда сразу по несколько для одной и той же функции. В инструкциях подобные изменения не приветствуются, поскольку они уменьшают производительность. «Скорее всего, они просто не хотят, чтобы вы сами устанавливали настройки», – отметил эксперт.

Барнетт установил Windows 10 на компьютер с виртуальной машиной VirtualBox (с ОС хоста CentOS) без сетевой платы и применил Windows Restricted Traffic Limited Functionality Baseline – разработанную Microsoft конфигурацию для Windows 10, отключающую большую часть отслеживающих функций. Затем эксперт отключил виртуальную машину, активировал отслеживание сетевого трафика и оставил на ночь.

Как оказалось, большая часть трафика действительно была урезана, однако некоторые данные все же пересылались на сервер Microsoft. Windows по-прежнему отправляла телеметрические данные об используемых программах, диагностике приложений, Windows DRM, а также о том, к чему есть доступ у «Календаря» и «Почты».

(вгору)

Додаток 22

1.06.2017

Украинцам объяснили, чем опасно обходить блокировку «Яндекса» и «ВКонтакте»: появилось видео

Не только простые украинцы, но уже и крупные компании осваивают способ обхода блокировки российских сайтов – VPN-сервисы (подменяют реальный ip-адрес). При этом они не учитывают, что таким образом информация на их компьютерах становятся открытой для держателей VPN – серверов (Обозреватель).

Об этом рассказал глава Интернет Ассоциации Украины Александр Федиенко в интервью UBR.ua.

Говоря о количестве украинцев, которые использует VPN-сервисы, эксперт отметил, что точные цифры назвать сложно, но речь идет «о каких-то миллионах». Федиенко привел пример, когда только одно из украинских юрлиц «обратилось к провайдеру с просьбой, что у него будет 17 тысяч VPN-соединений».

«Используя непроверенное VPN-приложение и посещая непроверенные ресурсы, вы становитесь заложником той ситуации, когда в ваш компьютер будет положена какая-то закладка, и в последующем при организации каких-либо кибератак внутри Украины ваш компьютер будет использован для кибератак в общей сети. Вы даже знать об этом не будете», – подчеркнул он.

«Казалось бы, вы хотели посмотреть фотографии, которые еще не удалили со своих аккаунтов, но при этом ваш компьютер будет использован как элемент кибератаки», – объяснил Федиенко.

Кроме того, по словам эксперта, «все, что есть в вашем компьютере, однозначно станет доступно держателю того VPN-сервера, через который вы будете куда-то ходить».

«Что такое VPN-сервер? Это такое устройство, через которое вы подключаетесь к чему-то. Когда вы подключились к чему-то через это устройство, тот, кто его вам подсунул, попадает сразу в ваш компьютер, к вашим дискам, к вашей информации – ко всему, что есть на вашем компьютере. Мало того, через ваш компьютер он может попасть, например, дальше в виртуальную сеть того предприятия, с которого вы зашли на эту VPN-систему», – подчеркнул эксперт.

По словам Федиенко, украинским интернет-пользователям сейчас широко предлагают скачивать VPN-системы, которые могут быть встроены в браузер.

«Сейчас санкционные браузеры стали предлагать гражданам нашей страны использовать “Яндекс” с функцией VPN, но мы понимаем однозначно, что это будет российский VPN», – отметил он.

«В самом VPN нет ничего плохого, но учитывая нынешнюю ситуацию, мы можем прогнозировать что агрессия извне на нашу страну возрастет», – заключил Федиенко.

(вгору)

Додаток 23

2.06.2017

WikiLeaks опубликовал весьма необычный хакерский инструмент ЦРУ

После двухнедельного молчания портал WikiLeaks опубликовал очередной хакерский инструмент из арсенала ЦРУ. Вредоносное ПО Pandemic предназначено для взлома компьютеров с общими папками, откуда пользователи загружают файлы с помощью протокола SMB. Pandemic отличается необычным, оригинальным принципом работы и не похож ни на один другой вредонос (Центр информационной безопасности).

Согласно опубликованной WikiLeaks инструкции, программа устанавливается на атакуемую систему в качестве «фильтра-драйвера файловой системы». Его задачей является прослушивание SMB-трафика и определение попыток пользователей загрузить общие файлы с зараженного компьютера. Pandemic перехватывает запросы на загрузку и отвечает от имени инфицированной системы, но вместо легитимных файлов отправляет пользователю зараженные.

Если верить инструкции, за один заход программа способна заменить до 20 файлов (как 32-битных, так и 64-битных) с максимальным размером одного файла 800 МБ. Установка Pandemic занимает всего 15 секунд. Инструмент был специально разработан для замены исполняемых файлов, в особенности тех, что хранятся в общих папках в корпоративных сетях. Предназначением Pandemic является заражение корпоративных файлообменных серверов и установка вредоносного ПО на компьютеры сотрудников.

Когда вредонос попадает в сеть, определить источник заражения и первую инфицированную систему весьма затруднительно. Это связано с тем, что драйвер файловой системы Pandemic определяет, когда локальный пользователь вручную получает доступ к одному из общих файлов, и выполняет чистую версию файла, а не вредоносную, которую передает по SMB. Таким образом, для обнаружения зараженных устройств системные администраторы должны загружать и сканировать файлы с других компьютеров по SMB.

(вгору)

Додаток 24

4.06.2017

В киберполиции рассказали провайдерам, как блокировать санкционные сайты

Наиболее эффективным методом работники полиции выделяют блокировку IP-адреса (Экономические известия).

Департамент киберполиции Национальной полиции Украины разработал ряд рекомендаций для предприятий, учреждений и организаций всех форм собственности, как заблокировать доступ к запрещенным веб-ресурсам, информирует news.eizvestia.com.

Так, сотрудники Департамента киберполиции отмечают такие методы, как блокировка по IP-адресам, с помощью DNS и по URL.

Наиболее эффективным методом среди них работники полиции выделяют именно блокировку ресурсов с помощью IP-адреса. Более того, настройка оборудования по таким рекомендациям не требует дополнительных финансовых затрат и приобретения техники.

Киберполиция обращает внимание пользователей, что в последнее время в сети, с использованием приемов агрессивного маркетинга, быстро распространяются специализированные браузеры. «Они, под легендой предоставления возможности преодолеть ограничение доступа к заблокированным ресурсам, на самом деле получают полный доступ к операционной системе и персональным данным пользователя», – сообщают в Киберполиции.

Отмечается, что пользователи, которые установили браузеры FreeU и Yandex Browser with protect, подвергают свои компьютеры риску заражения, а также удаленного доступа к ним со стороны российских спецслужб.

«В дальнейшем полученная злоумышленниками информация может использоваться ими по собственному усмотрению. Кроме того, они, таким образом, получат возможность использовать компьютеры пользователей в противоправных действиях», – отметили в Киберполиции.

(вгору)

Додаток 25

6.06.2017

Лучшие браузеры для анонимного веб-серфинга

Используемый Вами браузер знает многое о Вас и предоставляет эту информацию посещаемым сайтам, если Вы разрешаете это делать. Однако существуют специальные веб-обозреватели, которые предназначены для того, чтобы обезопасить Ваши данные и сделать интернет-сёрфинг, насколько возможно, защищённым. В этой статье представлено несколько известных веб-браузеров, которые помогут оставаться в сети инкогнито, рассмотрим их по очереди (InternetUA).

Популярные анонимные браузеры

Анонимный веб-обозреватель – одна из основ безопасности в интернете. Поэтому важно выбрать себе не обычный обозреватель типа Chrome, Opera, Firefox, IE, а защищённый – Tor, VPN/TOR Globus, Epic Privacy Browser, PirateBrowser. Давайте посмотрим, что представляет из себя каждое из этих защищённых решений.

Tor Browser

Этот веб-обозреватель доступен для Windows, Mac OS и Linux. Разработчики Tor максимально упростили его использование. Всё очень просто, необходимо лишь скачать браузер, запустить его, и Вы уже будете использовать сеть Tor.

Сейчас этот обозреватель даёт доступ к сайтам со вполне хорошей скоростью, хотя годами ранее сеть ещё была медленной. Браузер позволяет посещать сайты инкогнито, отправлять сообщения, вести блог и работать с приложениями, использующими протокол TCP.

Анонимность трафика обеспечивается за счёт того, что данные проходят через несколько серверов Tor, а уже после попадают во внешний мир через выходной сервер. Однако это работает не идеально, но если анонимность – это главный критерий, то Tor отлично подойдёт. Многие встроенные плагины и услуги будут отключены. Необходимо всё так и оставить, чтобы не допустить утечки информации.

VPN/TOR Browser Globus

Веб-браузер предоставляет конфиденциальный поиск в Интернете. VPN & TOR Globus даёт возможность использовать интернет-ресурсы, которые недоступны с Вашего IP-адреса или на территории Вашей страны.

Globus работает так: VPN-агент направляет трафик через серверы Globus в США, России, Германии и других странах. Пользователь сам выбирает, какой сервер он будет использовать.

Epic Privacy Browser

С 2013 года Epic Browser перешёл на движок Chromium и основным его направлением стала защита конфиденциальности пользователей.

Этот обозреватель блокирует рекламные объявления, модули загрузки и отслеживание cookies. Шифрование соединения в Epic происходит в основном за счет HTTPS / SSL. Дополнительно браузер направляет весь трафик через прокси-серверы. Здесь нет таких функций, которые могут привести к раскрытию действий пользователей, например, нет сохраняемой истории, не записывается кэш и удаляется информация о сессии, при выходе с Epic.

Также в одну из возможностей обозревателя входит встроенный прокси-сервер, но эту функцию необходимо активировать вручную. Дальше Вашим местоположением по умолчанию будет Нью-Джерси. То есть, все Ваши запросы в браузере сначала направляются через прокси-сервер, а после идут в поисковые системы. Это не даёт поисковикам сохранять и сопоставлять запросы пользователя по его IP.

PirateBrowser

PirateBrowser основан на Mozilla Firefox и поэтому они внешне похожи. Веб-обозреватель оборудован Tor-клиентом, а также расширенным комплектом средств работы с прокси-серверами.

PirateBrowser не предназначен для анонимного сёрфинга в Интернете, а используется для обхода блокировки сайтов и защищает от слежения. То есть, браузер просто предоставляет доступ к запрещённому контенту.

Какой из трех вышеприведённых браузеров предпочесть, решайте, исходя из личных потребностей.

(вгору)

Додаток 26

6.06.2017

Через соцсети распространяется очередной опасный вирус

Компьютеры и телефоны заражают с помощью сайтов-прокладок, а пользователей заманивают бесплатными билетами.

Киберпреступники стали заманивать пользователей интернета через социальные сети, привлекая их бесплатными билетами (IToboz.com).

Новый вирус был замечен в России и Франции: российским пользователям соцсетей предлагалось выиграть два билета от «Аэрофлота» или авиакомпании Emirates, а жителям Франции – от Air France.

При переходе пользователей по ссылке на их компьютерные устройства загружался вирус троян. После этого, пройдя авторизацию через свои личные кабинеты в Facebook, мошенникам отдавали доступ к своим личным данным, а также хакеры получали доступ к рассылкам по контактам пользователя вредоносных ссылок.

Эксперт по кибербезопасности компании Group-IB Руслан Юсуфов на своей странице в Facebook предостерегает от копирования таких сообщений: размещая ссылки мошенники получают доступ к гаджетам и компьютерам доверчивых пользователей, их онлайн-счетам, личным данным, включая информацию интимного характера.

«Когда вы переходите по подобной ссылке, вас проведут через несколько сайтов-прокладок. В процессе вы посмотрите рекламу, вероятнее всего будет предпринята попытка заразить ваше устройство трояном или другой вредоносной программой. Параллельно вы будете отвечать на вопросы типа "Вы действительно хотите получить 2 бесплатных билета?» и «Подтвердите, что вы совершеннолетний(ая)», – пишет эксперт.

После заражения устройства с него могут украсть деньги через онлайн-банк, в случае, если это компьютер компании – с него также могут украсть деньги или коммерческие данные, отмечает Юсуфов.

«Ваш компьютер будет подключен к ботнету для организации автоматических DDOS-атак или спама. Ваш компьютер будет использован для майнинга биткоинов, для хранения запрещенных материалов (например, не совсем законной порнографии), для сокрытия следов преступлений (например,

как proxy-сервер); совсем не обязательно, что этим будут заниматься одни и те же люди – доступ к вашему компьютеру может быть продан на черном рынке за 1-2 доллара», – пишет он.

(вгору)

Додаток 27

8.06.2017

В инстаграме Бритни Спирс обнаружены инструкции для «российских хакеров»

В инстраграме певицы Бритни Спирс обнаружены комментарии, которые, по данным исследователей из компании ESET, являются инструкциями для вредоносного программного обеспечения русскоязычной хакерской группы Turla (InfoResist).

Как говорится в публикации ESET, «троян», который использовала Turla, искал в комментариях к одной фотографии Бритни Спирс запись, в которой содержался зашифрованный адрес для связи с разработчиками шпионской программы. Такая схема позволяла хакерам оставаться незамеченными и постоянно менять адреса, с которых они связывались с зараженным компьютером.

Шпионская программа существовала в виде расширения для браузера Firefox, которое имитировало приложение для безопасной работы в интернете. В исходном коде расширения не было адреса, по которому программа связывалась с сервером создателей, его можно было добыть только из комментариев в инстаграме Спирс.

К примеру, один из оставленных хакерами комментариев, который при дешифровке превращался в URL-адрес, выглядел так: #2hot make loved to her, uupss #Hot #X. Подобный комментарий легко принять за обычную запись в инстаграме певицы. По ссылке, которая скрывалась за комментарием, перешли только 17 раз. В ESET предполагают, что хакеры только тестировали новую систему.

В первую очередь, подозрительный трафик в социальных сетях тяжело отличить от легитимного, Во-вторых, такая схема дает злоумышленникам больше гибкости, когда речь заходит о смене адреса или уничтожения всех следов.

Многие специалисты по компьютерной безопасности считают, что хакерская группировка Turla может быть связана с российскими спецслужбами и осуществляет взломы по их заказу. Turla, как считают исследователи, может быть причастна к взлому многих правительственных объектов в США, Европе и других странах. Эта хакерская группа, как утверждает «Лаборатория Касперского», получала доступ к данным с коммерческих спутников для слежки за своими целями.

(вгору)

12.06.2017

Чем для компаний оборачиваются недочеты в киберзащите индустриальных систем

За последние 12 месяцев каждая вторая промышленная компания в мире пережила от одного до пяти киберинцидентов – они затронули критически важные инфраструктуры или автоматизированные системы управления технологическими процессами (АСУ ТП) на этих предприятиях (ITnews).

Такие данные Kaspersky Lab получила в ходе исследования, в котором приняли участие более 350 представителей индустриальных организаций по всему миру. На устранение последствий этих инцидентов, случившихся в течение года, каждая компания потратила в среднем 497 тысяч долларов США.

Опрос также показал, что столкновение с киберугрозами не стало неожиданностью для промышленных предприятий – три четверти компаний допускают вероятность пострадать от кибератаки. Более того, 83 % респондентов считают себя хорошо подготовленными к тому, что в их промышленных инфраструктурах может произойти какой-либо инцидент.

Больше всего на сегодняшний день компании опасаются возможности заражения вредоносным ПО. И реальность показывает, что это не напрасно – 53 % пострадавших от инцидентов предприятий подтвердили случаи столкновения с различными зловредами. Более того, около трети компаний (36 %) подвергались таргетированным атакам. Таким образом, вредоносные программы и хорошо спланированные целенаправленные операции стали доминирующими угрозами для промышленных и критически важных инфраструктур.

В то же время исследование показало, что компании зачастую недооценивают внутренние угрозы, опасаясь рисков извне. Так, 44 % организаций полагают, что их кибербезопасности с большой долей вероятности будут угрожать какие-либо третьи лица, например, поставщики. А 33 % считают, что наибольшую опасность для них представляют программы-вымогатели. Однако чаще киберинциденты в промышленных сетях случаются из-за ошибок и непреднамеренных действий персонала – именно этот фактор угрожал почти трети (29 %) компаний.

«Мы наблюдаем все большую взаимную интеграцию корпоративных и индустриальных сетей, которые сегодня нередко образуют единую инфраструктуру промышленного предприятия. А это значит, что компаниям следует скорректировать подход к управлению и защите киберфизических систем, – отмечает Андрей Суворов, директор по развитию бизнеса безопасности критической инфраструктуры Kaspersky Lab. – Для этого важно понимать актуальный ландшафт угроз, знать возможные риски, оценивать, какие методы обеспечения защиты наиболее эффективны, и, конечно же, работать над повышением осведомленности сотрудников о новых киберопасностях».

(вгору)

Додаток 29

12.06.2017

Microsoft закрывает «убийцу» Google Docs, созданного совместно с Facebook

Сервис Docs.com, принадлежащий Microsoft и предназначенный для обмена документами, завершит работу в декабре 2017 г. К этому времени компания советует пользователям мигрировать на SlideShare или OneDrive. Закрытие последовало вскоре после того, как выяснилось, что поисковик сайта предоставляет публичный доступ к конфиденциальным файлам (InternetUA).

Docs.com будет закрыт

Microsoft закрывает сайт-файлообменник Docs.com, поскольку функционально он дублирует ресурс SlideShare, принадлежащий LinkedIn, и ее собственное хранилище OneDrive. Об этом компания сообщила в официальном заявлении. После покупки LinkedIn за рекордные $26,2 млрд в прошлом году, в распоряжении Microsoft оказалось сразу три сервиса похожего назначения.

С сегодняшнего дня на Docs.com нельзя будет создать новый аккаунт, однако окончательно сайт закроется 15 декабря. До этого момента пользователи могут просматривать, редактировать, скачивать, публиковать и удалять файлы в обычном режиме. Microsoft советует посетителям сайта как можно быстрее переместить свои данные в SlideShare или OneDrive, или же просто удалить файлы.

До 15 мая 2018 г. для перенесенных файлов будет работать система автоматического перенаправления с Docs.com на OneDrive. В своем заявлении Microsoft описывает преимущества миграции на OneDrive: дополнительные инструменты, расширенные настройки доступа и повышенная безопасность. Кроме того, компания составила и опубликовала инструкцию по миграции на OneDrive или OneDrive for Business.

Скандал с конфиденциальными файлами

Закрытие Docs.com последовало вскоре после резонансного происшествия, имевшего место в марте 2017 г. Исследователь кибербезопасности Кевин Бимонт (Kevin Beaumount) обнаружил, что некоторые пользователи Docs.com по неосмотрительности выкладывают на сайт файлы, содержащие конфиденциальную информацию: пароли, номера социального страхования, банковские выписки, медицинские данные и т. д. Пользователи делились этими файлами только с друзьями или коллегами, однако поисковая система сайта обеспечивала к ним публичный доступ, о чем владельцы файлов не знали.

Более того, к файлам Docs.com имели доступ Google, Bing и другие поисковые системы, которые к тому же сохраняли их копии. Microsoft попробовала отключить поиск и фильтровать запросы из Google, но мера не оказалась эффективной. В итоге компания отговорилась тем, что сервис

предназначен для того, чтобы «делиться со всем миром», и посоветовала пользователям изменить настройки аккаунтов.

Проект Docs.com

Docs.com – это сервис для хостинга файлов, запущенный Microsoft в 2010 г. в рамках сотрудничества с соцсетью Facebook. Является частью системы Microsoft Office Online. На сайте можно размещать файлы Word, Excel, PowerPoint, Mix и Sway, а также PDF-документы и URL-страницы. Просматривать эти документы можно в браузере, не устанавливая на устройстве пакет Microsoft Office. Все внесенные изменения сохраняются сразу в облако.

Предполагалось, что с помощью Docs.com пользователи Facebook будут делиться файлами друг с другом. Сервис должен был составить конкуренцию Google Docs. О запуске Docs.com объявил лично Марк Цукерберг (Mark Zuckerberg) на конференции Facebook. Сайт был рассчитан в основном на использование частными пользователями, в первую очередь студентами. Для корпоративных пользователей больше подходил Microsoft Office Live.

Docs.com изначально был создан по примеру Facebook Photos, с похожими настройками обмена файлами и возможностью пригласить друзей. Авторизация на Docs.com проходила с помощью Facebook Connect, также действовала упрощенная система публикации файлов на страницах соцсети.

В 2015 г. Microsoft модифицировала Docs.com, интегрировав в него систему подбора контента Curah! и возможность быстро загрузить файлы из OneDrive. Однако возможность совместной работы с файлами, которая есть в Google Docs, так и не была добавлена.

(вгору)

Додаток 30

13.06.2017

Хакеры разработали новый способ распространения вредоносного ПО

Довольно долго одним из самых действенных методов защиты пользователей от вредоносного программного обеспечения являлась бдительность: для того, чтобы уберечь себя от вируса, нужно было просто не кликать на подозрительные кнопки и не переходить по непроверенным ссылкам. Однако киберпреступники разработали новую технику распространения троянов при помощи PowerPoint и Mouseover: «заражённая» PowerPoint-презентация распространяется посредством спам-рассылки с темой писем Purchase Order #, Invoice или Confirmation (Grifonsoft).

После открытия приложенного файла на экране появляется строка Loading… Please Wait (Загрузка… Пожалуйста, подождите), которая отображается в виде гиперссылки. И вот тут нужно быть особенно осторожным.

Чтобы «подцепить» Trojan Zusy, нажимать на эту ссылку совершенно необязательно. Ссылка срабатывает (пытается выполнить код PowerShell) после наведения на неё курсора мыши. Если при этом у пользователя включена защитная функция Protected View, то система предупредит его и попытается остановить атаку.

Но если Protected View отключён или просто не работает, вредоносный PowerShell-сценарий активируется, что приведёт к загрузке на компьютер файла c.php с домена ccn.nl (IP: 46.21.169.110). После того, как Trojan Zusy оказывается на компьютере пользователя, он может передать все данные о банковском счёте жертвы третьим лицам.

На данный момент спам-рассылка приостановлена. Однако из-за самого факта существования подобных техник распространения вредоносного программного обеспечения пользователям рекомендуется всегда быть настороже и не терять бдительность ни при каких обстоятельствах.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
Сайт: http://nbuviap.gov.ua/
http://сіаз.укр/
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.