СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(14.06–27.06)

2017 № 12

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(14.06–27.06)
№ 12

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2017

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

17.06.2017
«ВКонтакте» тестирует обход блокировки в приложении для Android

Android-приложение «ВКонтакте» научится обходить блокировку по умолчанию (IGate).

Социальная сеть «ВКонтакте» добавила в свое приложение на Android тестовую функцию соединения через прокси-сервер, заметили участники сообщества Live Express.

Пользователи заметили, что опция доступна в версии приложения 4.10.0 на территории Украины. При её включении становится недоступна загрузка файлов и сохранение изображений.

Представители компании рассказали, что тестируют функцию в последней версии приложения на Android. Подробности о принципах работы сервиса они раскрывать не стали, сославшись на тестирование. Очевидно, что запуск функции связан с блокировкой сервиса в Украине, хотя они это не подтвердили.

В компании добавили, что «тестируют настройку, которая позволит оставаться во “ВКонтакте” с близкими вне зависимости от местонахождения»

***

19.06.2017
Олег Дмитренко
На Facebook вже 9 млн українців

Кількість українських користувачів Facebook продовжує зростати фантастичними темпами. 19 червн, українцям вперше вдалось подолати позначку в 9 млн користувачів. Про це свідчать дані внутрішньої статистики Facebook для рекламодавців (Watcher).

Всього за останній місяць – з 18 травня 2017 року, українська аудиторія Facebook зросла майже на 2,5 млн користувачів. А загальна аудиторія Facebook (будь-хто, хто заходив в соцмережу) перевищила аудиторію ВКонтакте в Україні.

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).

***

20.06.2017

Twitter змінився до невпізнання // Користувачам буде зручніше писати повідомлення зі смартфонів

Програмісти і дизайнери сервісу мікроблогів Twitter випустили масштабне оновлення браузерної та мобільної версій, яке вже стало доступним для більшості користувачів (Знай.ua).

Головною відмінністю від старої версії Twitter стали округлі фото сторінок замість квадратних. Ще одним цікавим нововведенням став підрахунок лайків та ретвітів – тепер він відбувається у реальному часі.

Найбільше змін побачать користувачі iOS. У додатку тепер чотири вкладки знизу, а потрапити на свою сторінку можна через бокове меню. Крім того, посилання на статті та сайти відкриваються у вбудованому засобі перегляду Safari з розширеними можливостями.

***

20.06.2017

10 хитрых функций чата WhatsApp, которые облегчат общение

На днях WhatsApp обновился, получив новые интересные возможности, которые делают общение проще. Но в этой подборке не только они.

Докладніше

***

20.06.2017

Instagram разрешил сохранять трансляции в Историях на сутки

Команда фотосервиса Instagram объявила о запуске новой возможности – живые трансляции в Историях (Stories) теперь можно сохранить на 24 часа для повторного просмотра (InternetUA).

Когда пользователь завершил трансляцию, ему предлагается выбор – сохранить видео на 24 для просмотра или нет. Когда кто-то з друзей пользователя сохраняет трансляцию, под его фото появляется кнопка воспроизведения в панели Историй. Нажав на нее можно просмотреть видео, а также комментарии и лайки из оригинальной трансляции, нажав на правую или левую сторону экрана, можно проматывать видео на 15 секунд вперед или назад.

Сохранение трансляций в Историях появилось в приложении Instagram версии 10.26 и выше для iOS и Android.

Обновленный Instagram для iOS и Android доступен для бесплатной загрузки в App Store и Google Play.

***

21.06.2017

Соцсеть «Одноклассники» обошла запрет и снова работает в Украине

Российская социальная сеть «Одноклассники» нашла способ, как обойти блокировку российских интернет-ресурсов в Украине. Обновленное мобильное приложение позволяет обойти законодательный запрет, передает УНИАН со ссылкой на пресс-службу соцсети (InternetUA).

«Вы снова можете без ограничений общаться в Одноклассниках со своими родными и близкими. Это возможно с помощью официальных мобильных приложений ОК для iPhone и Android», – говорится в сообщении.

Как утверждают разработчики, благодаря последнему обновлению приложения украинцы снова могут заходить в «Одноклассники» и пользоваться всеми сервисами социальной сети.

«Установите приложение ОК на свой смартфон, либо обновите приложение до последней версии в том случае, если оно у вас уже установлено», – рассказали в Одноклассниках.

Последняя версия приложения доступна для скачивания в официальных магазинах приложений AppStore и Google Play.

***

20.06.2017

Мессенджер Google Allo научился звонить через видеочат Duo

Компания Google начала распространение очередного обновления для своего мессенджера Google Allo. Апдейт принесет возможность совершать голосовые и видеозвонки прямо из Allo через видеочат Duo. Об этом сообщил Амит Фулай (Amit Fulay), глава подразделения, занимающегося Google Allo и Duo, а также WebRTC (InternetUA).

Чтобы в мессенджере Google Allo совершить звонок, понадобится коснуться Duo в правом верхнем углу чата. Также в версии для iOS появилась возможность создавать резервные копии чатов.

***

21.06.2017

В Украине появилась новая социальная сеть для соседей «Сусід.Online»

В 2015 году в Киеве запустилася проект «Жители», который должен был объединить жителей многоквартирных домов. Похожую идею решили реализовать и авторы проекта «Сусід.Online», дополнив её возможностью создавать тематические сообщества, календарём локальных событий и рекомендациями. Структура сервиса напоминает Facebook, в «Сусід.Online» также есть лента новостей, можно делиться информацией, комментировать и обмениваться сообщениями (IGate).

При этом есть разделы посвящённые размещению объявлений, аренде вещей и купле/продаже.

Разработчики «Сусід.Online» обещают в скором времени запустить в рамках проекта сервис «МастерОК» для малого бизнеса, который позволит

предпринимателям предлагать услуги и товары пользователям социальной сети. Также заявлены планы по запуску возможности оплачивать коммунальные платежи и собирать деньги на локальные цели, например, на ремонт детской площадки или на установку видеонаблюдения.

На данном этапе «Сусід.Online» доступен только в веб-версии, мобильные приложения для Android и iOS в разработке.

***

22.06.2017

Ночной режим в Twitter для Android стал автоматическим

В апреле разработчики Twitter для Android начали тестировать автоматическое включение и выключение ночного режима. Теперь эта функция полностью внедрена в свежую бета-версию приложения (InternetUA).

При обновлении до Twitter 7.2.0, пользователи с активированным ночным режимом окажутся переключены на светлую тему. При первом переключении ползунка пользователь получит предложение запустить автоматическое переключение режимов. Приложение предлагает включать ночной режим с заходом солнца и отключать с восходом. Как ожидается, эта опция станет доступна для стабильной версии Twitter для Android на следующей неделе.

***

25.06.2017

В мобильном клиенте YouTube появится долгожданная функция

На этой неделе в Лос-Анджелесе прошло ежегодное мероприятие VidCon, где представители YouTube традиционно рассказывают о достижениях и новых функциях сервиса. В этом году посетителей ждало сразу несколько громких анонсов.

Докладніше

***

27.06.2017

Олег Дмитренко

5,6 млн українців вже користуються Instagram, а Facebook просів до 8,9 млн

Аудиторія Instagram за останні півтора місяці виросла майже в півтори рази – з 3,8 млн до 5,6 млн користувачів. Про це свідчать дані внутрішньої статистики Facebook для рекламодавців.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

19.06.2017

Порошенко рассмотрит петицию об отмене блокировки соцсети «ВКонтакте»

Петиция к Президенту Украины Петру Порошенко об отмене блокировки российской социальной сети «ВКонтакте» перешла в статус «на рассмотрении». Она набрала 25,352 голоса из 25 тыс. необходимых для рассмотрения.

Докладніше

***

23.06.2017

«Нет, мне завтра на работу»: в Twitter и Facebook идет флешмоб о взрослой жизни в пяти словах #AdultingIn5Words

Флешмоб #AdultingIn5Words недавно запустился в англоязычных социальных сетях, теперь понемногу распространяется в украинском Twitter и Facebook. Его цель и исполнение – крайне незамысловатые: нужно придумать, как всего в пяти словах выразить суть (и боль) взрослой жизни. Один из самых первых и самых удачных твитов на эту тему звучит, как «Нет, мне завтра на работу» (AIN).

Многие твиты звучат достаточно подавленно и безрадостно, пользователи пишут об ответственности, кредитах, невысыпании, небольших заработках, оплату коммуналки и прочие прелести взрослой жизни. Среди «хитов»: «Боюсь глянуть на банковский счет», «Я должен обо всем знать», «Почему чувствую себя таким уставшим?», «Когда горишь на горящем велосипеде», «Работа, оплата счетов, алкоголь, сон», «Еще бы немножко поспать», «Просто одна сплошная паническая атака». Некоторые участвуют гифками.

Флешмоб не обошли вниманием и украинские госорганы. Министерство финансов, к примеру, любезно напомнило украинцам, что взросление – это в первую очередь, уплата налогов. Как раз заканчивается второй квартал, спасибо за напоминание, твиттер Минфина!

***

26.06.2017

Ольга Мінченко

До Дня кримськотатарського прапору Twitter верифікував офіційний екаунт Криму

26 червня святкується День кримськотатарського прапору, і Twitter верифікував офіційний екаунт Криму – twitter.com/Crimea.

Станом на 26 червня екаунт має 2 повідомлення, і судячи з їх змісту автори проекту відстоюють проукраїнську позицію. В його описі написно, що #CrimeaIsUkraine (Watcher).

Екаунт ведеться англійською мовою.

Згідно з даними Twitter, екаунт запущено в червні 2017 року. Зважаючи на те, що така назва не могла бути нічийною до червня 2017 року, ймовірно, що Twitter допоміг в делегуванні імені.

Хто веде екаунт, наразі не відомо.

***

26.06.2017

МВС ініціювало флешмоб проти наркотиків

26 червня, у Міжнародний день боротьби зі зловживанням наркотиками й їхнім незаконним обігом, Департамент протидії наркозлочинності Національної поліції України запустив флешмоб у соцмережах (ZIK).

Про це у Facebook повідомляє прес-служба МВС України.

«Друзі, запрошуємо взяти участь у ініційованому поліцейськими флешмобі. Хай імпровізована фотосесія стане приводом застерегти дітей. Говоріть з ними про неприпустимість вживання наркотиків, про шкоду й біль, якого вони можуть завдати.

Хай дітлахи з найменшого віку будуть #проти_наркотиків!», – закликали у поліції.

Для участі у флешмобі потрібно сфотографуватися із аркушем паперу, де написано «Проти наркотиків» і виставити світлину із відповідним хештегом у соцмережу.

***

26.06.2017

В Сумах противники подорожания проезда в маршрутках инициируют флешмоб #Повесьдепутата

Общественный активист Александр Такул на своей странице в Facebook предложил сумчанам присоединиться к начатому им флешмобу #Повесьдепутата (Сумской новостной портал).

Для этого гражданам предлагается распечатать листовки с изображением депутата, избранного по своему избирательному округу и попавшего в список голосовавших за подорожание проезда до 4 гривен, и расклеить их в своем районе. Текст листовки предлагается составить в таком ключе: «Я твой депутат. Поблагодари меня за то, что ездишь в маршрутке по 4 гривны».

Сам Александр Такул в рамках флешмоба «повесил» депутатов Сумского горсовета от фракции Оппоблока Игоря и Юрия Перепек.

***

26.06.2017

Depo.ua запустив флешмоб, щоб змусити мера Кличка ремонтувати дороги

Зокрема, Depo.ua розпочинає флешмоб #знайди_яму_для_Кличка.

Для того, щоб взяти участь у флешмобі, потрібно просто опублікувати фото дороги з ямою на своїй сторінці у Facebook з хештегом #знайди_яму_для_Кличка (depo.ua).

Не забувайте вказувати адресу, де виявлена яма на дорозі.

Окрім цього, ви можете надсилати фото ям у повідомленні на сторінці Depo.Київ у Facebook.

Фотографії з виявленими вами ямами, будуть опубліковані на сайті Depo.ua.

Давайте допоможемо Віталію Кличку знайти ями у київському асфальті.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

19.06.2017

64 % пользователей совершают покупки после просмотра видео в сетях

Новые данные исследования Animoto State of Social Video 2017 указывают, что 83 % маркетологов считают, что видео-контент в Facebook будет стимулировать покупки. Большинство покупателей (64 %) признали, что совершили покупки после просмотра видео в Facebook в прошлом месяце. 60 % смотрят видео брендов в Facebook каждый день. Большинство видео (84 %) просматриваются на мобильных девайсах (Marketing Media Review).

Другие данные исследования:

•47 % бренд-менеджеров размещают четыре видео каждый месяц

•81 % бренд-менеджеров оптимизируют видео-контент из сетей под мобильные девайсы

•67 % отметили, что поднимали видео-посты платно в течение года

Ключевые выводы:

1.В онлайне много шума. Ответственность специалистов по маркетингу создавать вовлекающий и качественный контент.

2.Видео эффективно и этот тренд никуда не исчезнет.

3.При создании видео следует ориентироваться на мобильные устройства.

***

20.06.2017

Ogilvy: Facebook захватил лидерство среди поставщиков новостей

Опрошенные журналисты отметили, что главными факторами развития медиа является переупаковывание контента в форматы live-видео, подкасты – так считают 34 % (mResearcher).

По результатам исследования международного коммуникационного агентства Ogilvy, Facebook стал главным поставщиком новостей – так высказались 39 % представителей медиа, среди которых корреспонденты, редакторы, продюсеры по всему миру. Соцсети удалось вытеснить на второй план традиционные медиа (32 %), Google (15 %) и Twitter (4 %).

Опрошенные журналисты отметили, что главными факторами развития медиа является переупаковывание контента в форматы live-видео, подкасты – так считают 34 %. 26 % считают важным переформатирование контента для мобильных устройств.

***

20.06.2017

Google запустила два новых вида таргетинга для рекламы на YouTube

Таргетинг на привычки пользователей позволяет нацелить рекламу на тех, кто чаще посещает (Marketing Media Review):

•Определённые магазины (торговые центры, супермаркеты, продуктовые);

•Рестораны/кафе;

•Парикмахерские;

•Массовые мероприятия.

Таргетинг на важные события позволяет найти людей, которые переживают важный период в жизни. К таким событиям в Google отнесли свадьбу, переезд и окончание учёбы и выход во взрослую жизнь. Оба вида таргетинга основаны на кроссканальных данных, в том числе по поисковым запросам, отмечает searchengines.ru.

***

24.06.2017

Google откажется от сканирования почты для персонализации рекламы. Она и так уже все знает

Весьма неожиданное заявление сделала компания Google. До конца года она прекратит сканировать почту пользователей для персонализации рекламных объявлений, сообщает TechCrunch. Как считают журналисты издания – в компании и так все знают о своих пользователях. В самой же Google говорят, что хотят свести показ рекламы до единого стандарта (AIN).

Почтовым сервисом Gmail пользуется 1,2 млрд человек. В компании отметили, что теперь для показа рекламы они не будут сканировать почту людей. Вместо этого будут использоваться настройки пользователей.

Ранее сканирование почты было отключено для пользователей бизнес-сервиса G Suite, которые платили за его использование. А вот почту пользователей бесплатной версии Gmail сканировали. Когда именно произойдет отключение – не сообщается. К слову, сейчас за G Suite платит уже 3 млн компаний.

Реклама в Gmail останется.

***

26.06.2017

Facebook займется производством сериалов

Социальная сеть Facebook планирует заняться производством сериалов, сообщает The Wall Street Journal со ссылкой на источники (InternetUA).

Как утверждается, Facebook ведет переговоры с голливудскими студиями и агентствами по производству «шоу телевизионного качества» и собирается запустить оригинальную продукцию к концу лета.

По информации WSJ, соцсеть готова вкладывать до $3 млн в создание одной серии, что сопоставимо с дорогими проектами на кабельном ТВ, а также заинтересована в более бюджетных шоу (где на производство одного эпизода требуются шестизначные суммы).

Источники утверждают, что Facebook проявляет интерес и к малому формату. Речь о контенте продолжительностью около 10 минут.

В Facebook отказались комментировать подробности относительно своих планов по контенту.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

26.06.2017

Психологи подтвердили пагубное влияние Facebook на здоровье человека

Постоянное виртуальное общение и пользование соцсетями негативно сказывается на физическом и психическом здоровье людей (SunDayNews).

Исследователи из Калифорнийского университета в Сан-Диего и Йеля в течение двух лет наблюдали за 5000 пользователей Facebook, регулярно проверяя их эмоциональное состояние и даже индекс массы тела.

О том, что соцсети делают пребывание людей в социуме некомфортным, ученые предупреждали и ранее. Новые результаты подтвердили, что частое нахождение в Facebook предвещает скорое ухудшение психического благополучия.

Дело в том, что соцсети создают невидимое давление на человека, который видит там множество историй успеха. Эта среда обманчива и заставляет встраиваться в чуждые рамки.

Кроме негативной самооценки, она отнимает много времени и создает иллюзию близости.

***

22.06.2017

Алжирец вывесил двухлетнего сына из окна 15-го этажа ради лайков в Facebook

Алжирец вывесил сына из окна 15-го этажа (Сегодня).

В Алжире отец двухлетнего мальчика шокировал соцсеть Facebook странным поступком, которым хотел собрать больше лайков.

Мужчина вывесил своего двухлетнего сына из окна квартиры, которая находится на 15-м этаже, держа его при этом лишь за футболку одной рукой. Другой рукой он фотографировал мальчика на телефон, передает Al Arabiya.

В подписи к шокирующему снимку он указал: «1000 лайков или я его бросаю».

Пользователи соцсети были возмущены подобным снимком мужчины, а на пост обратили внимание представители местной власти.

В результате алжирца арестовали и приговорили к двум годам тюремного заключения за жестокое обращение с собственным ребенком.

По словам детского психолога, этот инцидент навсегда может отпечататься в памяти малыша, который в последствии может начать страдать от панических атак и фобий.

***

24.06.2017

По ту сторону монитора: психолог объяснила, как манипулируют людьми в соцсетях

Любой пользователь соцсетей становится легко доступным для манипуляций, если он проводит длительное время за монитором. Когда человек устает, то в этом случае он впадает в состояние транса и его поведение подвержено программированию.

Докладніше

***

25.06.2017

Влияние социальных сетей на психику пользователей

Яркие фотографии из аккаунтов звезд, популярных фитнес-моделей, топ-блогеров, путешественников и прочих «успешных людей» в социальных сетях негативно сказываются на психическом состоянии обычных пользователей. Это проявляется в тревоге, лишении сна и завышенных требованиях к своей внешности у молодых людей, которые являются наиболее активными в интернете.

Докладніше

Маніпулятивні технології

19.06.2017

Facebook разработал программу для борьбы с пропагандой терроризма

Соцсеть Facebook тестирует новое программное обеспечение для противодействия распространению в сети пропаганды экстремизма и терроризма. Эти технологии опираются на элементы искусственного интеллекта и позволяют реже задействовать людей при принятии решения об удалении или блокировании запрещенного контента, сообщает ТАСС (Телекритика).

По словам начальника департамента глобальной политики управления компании Моники Бикерт, для Facebook новая технология является важной составной частью выявления и предупреждения о появлении подобного контента.

***

19.06.2017

Корпорация Google усиливает контроль за экстремистским контентом на YouTube

Компания Google заявила, что намерена усилить контроль за рапространением экстремисткого видео на сервисе YouTube. Корпорация займется улучшением инструментов, которые отвечают за поиск и удаление вредоносного контента (HiTech-News.ru).

Дополнительно, Google собирается нанять сотрудников, которые будут заниматься поиск экстремистких видео и удалять их вручную. Одновременно с этим, будут привлечены сторонние общественные организации для обнаружения пропагандистского видео в интернете.

Так же, пользователям, которые просмотрели ролики такого типа содержания, будет осуществляться рассылка в виде письма, которая направлена на то, чтобы предостеречь людей о связи своих жизней с терроризмом.

В заявлении Google говорится, что экстремисты и террористы хотят не только подорвать безопасность общества, но еще и уничтожить все ценности, которые делают его свободным.

***

20.06.2017

YouTube рассказала о четырёх новых способах борьбы с экстремистскими видео

В последние месяцы на социальные сервисы оказывается особенно сильное давление касательно контента, который содержит террористическую пропаганду. YouTube рассказала о четырёх новых способах борьбы с экстремистами в рамках платформы.

Докладніше

***

21.06.2017

Алексей Симончук

Оксфордский университет: в Украине копируют российскую пропаганду

Почему общественные организации борются с российской пропагандой эффективнее государства, сколько стоит создать армию ботов и как появляются фейковые новости.

Оксфордский университет изучил опыт использования соцсетей в качестве манипуляторов общественного мнения девяти стран (Россия, Бразилия, Канада, Украина, США, Польша, Германия, Китай, Тайвань) и подготовил исследования на эту тему.

Докладніше

***

26.06.2017

Интернет-тролли ФСБ разгоняют в соцсетях фейки о перемещениях подразделений «л/днр», – ИС

По оперативным данным группы ИС, в составе «органов военной разведки» «днр» активизировалась группа по дезинформации, распространяющая в соцсетях, украинских пабликах и чатах нужную командованию оккупантов дезинформацию о перемещении военной техники российско-террористических войск, состоянии военных объектов и пр.

Отмечается активизация такой же группы в составе непосредственно «мгб днр».

Обе группы возглавляют специалисты ФСБ РФ.

***

27.06.2017
Дарина Шварцман
Microsoft, YouTube, Facebook и Twitter заключили антитеррористическое партнерство

Крупнейшие мировые технологические компании, в числе которых Microsoft, YouTube, Facebook и Twitter, анонсировали Глобальный интернет-форум по борьбе с терроризмом, который рассчитан на упрощение совместной работы, поиску технологический решений, а также сотрудничестве правительствами различных стран и общественными с организациями.
Докладніше

Спецслужби і технології «соціального контролю»

16.06.2017
Украинским СМИ отобьют желание подзаработать у Путина

СБУ намерена инициировать изменения в законодательстве и ввести криминальную ответственность за распространений российской пропаганды. Служба безопасности Украины будет жестче бороться с кремлевской пропагандой. Предлагается изменить законодательство и ввести криминальную ответственность за ее проявления в украинских медиаресурсах.
Докладніше

***

16.06.2017
СБУ затримала адміністратора групи «ВКонтакте», який навчав, як обійти блокування соцмережі

Співробітники Служби безпеки України затримали жителя Павлограда Дніпропетровської області, який адміністрував антиукраїнські групи у «ВКонтакте» і поширював інструкції з обходу блокування доступу до російських сайтів через використання VPN.
Докладніше

***

19.06.2017
Голова Роскомнагляду особисто попросить у Дурова відомості про Telegram

Голова Роскомнагляду Олександр Жаров сказав, що протягом тижня особисто звернеться до власника Telegram Павла Дурова і попросить його надати відомству відомості про месенджер (LB.ua).
Про це повідомляє «Интерфакс».

Роскомнагляд планує внести Telegram до реєстру організаторів поширення інформації. За словами Жарова, він звернеться до Дурова особисто, оскільки відомство чекає на інформацію від месенджера, але Дуров поки її не надав.

***

19.06.2017

Евгения Подгайная

Киберполиция продолжает мониторить контент заблокированного «ВКонтакте»

Работниками Киевского управления киберполиции совместно со следственным отделом Броварского отдела полиции ГУНП в Киевской области выявлено и задокументировано группу в социальной сети «ВКонтакте», где проводилось распространение детской порнографии. Администраторами группы оказались 13-летняя жительница Броваров и 12-летняя гражданка, которая в настоящее время находится за пределами страны.

Докладніше

***

19.06.2017

Совет ЕС: Евросоюз может ответить санкциями на кибератаки

Министры иностранных дел Евросоюза в ходе заседания Совета ЕС в Люксембурге договорились разработать «специальный инструментарий кибердипломатии» в качестве ответных мер на широкомасштабные кибернетические атаки (InternetUA).

«Дипломатический ответ ЕС на вредоносную кибернетическую деятельность будет включать полный спектр действий в рамках единой внешней политики и политики в области безопасности, включая, если необходимо, ограничительные меры. Общий ответ ЕС на кибернетические атаки должен быть пропорциональным по своим масштабам, продолжительности, интенсивности, сложности и влиянию на кибернетическую среду», – сказано в заявлении Совета ЕС.

В то же время в документе отмечается, что Евросоюз «привержен разрешению любых международных споров и конфликтов в кибернетической среде мирными средствами», и все его действия «должны способствовать продвижению киберстабильности и кибербезопасности».

***

20.06.2017

Немецкий суд обвинил Google в несоблюдении «права быть забытым»

Прошло уже несколько лет с тех пор, как Европейский Союз принял закон, в соответствии с которым пользователи Сети получили право «забывать» и требовать, чтобы поисковые системы удаляли определённые ссылки, содержащие личную информацию – «неточную, неадекватную, неактуальную или чрезмерную». За это время Google уничтожила в Германии в Интернете более 750 тысяч ссылок. Но немецкие регуляторы по-прежнему недовольны тем, как здесь работает система удаления URL-адресов, позволяя относительно легко найти уже удалённые записи (InternetUA).

Всякий раз, когда компания получает запрос на удаление ссылки, она автоматически отправляет его в базу данных Lumen и заменяет исходное содержимое страницы следующим текстом: «В ответ на юридический запрос, отправленный в Google, мы удалили один результат поиска. Вы можете найти дополнительную информацию на LumenDatabase.org». Однако эта база данных продолжает включать ссылки на исходный URL-адрес, который был удалён. И если кому-то захочется найти удалённую ссылку, он сделает без особого труда.

Высший земельный суд Мюнхена выпустил судебное постановление с требованием, чтобы Google прекратила отправку уведомлений об удалении в Lumen с последующей привязкой к появившимся в итоге записям в базе данных (где ссылки на удалённые страницы все ещё могут храниться).

***

20.06.2017

Власти Мексики обвинили в слежке за журналистами с помощью вредоносного ПО

Правительство Мексики обвинили в шпионаже за журналистами и активистами посредством установки вредоносного ПО на их телефоны. Об этом пишет The Guardian (InternetUA).

Отмечается, что люди получали на свои мобильные устройства SMS-сообщения со ссылками на установку недоброкачественного контента. Затем программа записывала список контактов и полученные сообщения.

Издание пишет, что такой метод использовался против активистов, выступающих за снижение налогообложения, и журналистов, которые освещали якобы зверства армии и судебной системы.

***

26.06.2017

Николай Офицеров

Дуров нашел в требованиях Роскомнадзора нарушение Конституции РФ

Требование, озвученное Роскомнадзором о предоставлении ведомству данных о Telegram, полностью противоречит Конституции России. Об этом заявил Дуров на своей странице «ВК».

Докладніше

***

26.06.2017

Дуров обвинил ФСБ в спекуляции на теме теракта в Петербурге

Основатель мессенджера Telegram Павел Дуров обвинил ФСБ в спекуляциях на тему теракта в метро Санкт-Петербурга. Об этом он заявил во «ВКонтакте» (InternetUA).

По словам Дурова, информация о том, что подготовка теракта осуществлялась с помощью Telegram, вызвала у него ряд вопросов. «Печально, если спецслужбы России эксплуатируют подобную трагедию как предлог для усиления своего влияния и контроля над населением», – отметил он.

Основатель Telegram заявил, что шифрование мессенджера одинаково защищает всех пользователей и не делает коммуникации безопасными только для потенциальных террористов. «Отказ от оконечного шифрования в отдельно взятой стране сделает десятки миллионов людей беззащитными от атак хакеров и шантажа коррумпированных чиновников», – подчеркнул Дуров.

Он также добавил, что ослабление шифрования во всех мессенджерах приведет к подрыву национальной безопасности России и позволит иностранным спецслужбам получить доступ к переписка россиян. «При этом риск терактов не исчезнет – как показали события в Париже, для проведения теракта достаточно одноразовых телефонов и обычных СМС без всякого шифрования», – подытожил он.

Ранее 26 июня в ФСБ сообщили, что смертник, устроивший теракт в подземке Петербурга, использовал Telegram для связи с зарубежными кураторами, чтобы скрыть «свои преступные замыслы на всех стадиях организации и подготовки террористического акта».

***

26.06.2017

У Росії стверджують, що терористи масово використовують Telegram

ФСБ Росії заявила, що терористи на території РФ активно використовують месенджер Telegram «завдяки його можливостям шифрування переданої інформації» (Espreso.tv).

«Найбільш активно членами міжнародних терористичних організацій на території РФ використовується месенджер Telegram, що надає терористам можливість створювати секретні чати з високим рівнем шифрування переданої інформації», – заявили у ФСБ.

Зокрема, як стверджують у ФСБ, теракт в метро Санкт-Петербурга 3 квітня цього року був підготовлений за допомогою месенджера Telegram.

***

27.06.2017

СБУ викрила чотирьох антиукраїнських пропагандистів

Працівники Служби безпеки України викрили чотирьох антиукраїнських пропагандистів у різних регіонах країни, які готували заклики до масових заворушень до Дня Конституції України. Про це 26 червня повідомила прес-служба СБУ (InternetUA).

«Чотирьох антиукраїнських пропагандистів викрила Служба безпеки України в різних регіонах держави. Мешканці Київської, Миколаївської, Хмельницької та Харківської областей на виконання завдань кураторів з російських спецслужб розміщували в соціальних мережах "ВКонтакте" та "Одноклассники" заклики до масових заворушень до Дня Конституції України», – йдеться у повідомленні.

Правоохоронці відкрили кримінальні провадження та проводять слідчі дії.

Проблема захисту даних. DDOS та вірусні атаки

16.06.2017

Facebook случайно раскрыла имена модераторов, которые удаляют страницы потенциальных террористов // Уязвимость затронула около тысячи человек

Компания Facebook случайно раскрыла данные модераторов, которые проверяют и удаляют страницы за несоблюдение правил сайта, в том числе, за использование сексуального контента, разжигание ненависти и пропаганду терроризма, сообщает The Guardian.

Докладніше

***

18.06.2017

Новое вымогательское ПО Sorebrect способно внедрять вредоносный код

С каждым днем злоумышленники становятся все изобретательнее и разрабатывают инновационные, более скрытые техники атак. Ярким примером тому может служить новое семейство бесфайлового вымогательского ПО Sorebrect, недавно обнаруженное специалистами компании Trend Micro.

Докладніше

***

19.06.2017

Сотни программ в магазинах приложений выдают себя за сканеры вирусов

В конце мая специалисты компании McAfee предупредили пользователей платформы Android, что в официальном магазине Google Play Store есть множество приложений, которые якобы обеспечивают защиту от программы-вымогателя WannaCry. Судя по всему, в магазине наблюдается наплыв фальшивых антивирусных решений, которые не защищают устройства, а наоборот атакуют их.

Докладніше

***

19.06.2017

Создан руткит, умещающийся в модулях PHP сервера

Голландский web-разработчик Люк Парис (Luke Paris) создал руткит, который можно спрятать в PHP-модуле и использовать для взлома web-серверов по очень редкому вектору атаки – с помощью модулей Apache.

Докладніше

***

20.06.2017

Приложения из Google Play засоряют смартфоны вирусной рекламой

Злоумышленники продолжают регулярно выпускать вредоносное программное обеспечение для операционной системы Android (iLenta.com).

Специалисты по безопасности компании Sophos сообщили об обнаружении программ в магазине приложений для Android, которые для отображения рекламы используют стороннюю библиотеку Mars Dae-A.

Вредоносное программное обеспечение было выявлено в 47 приложениях, общее число загрузок которых превышает 6 млн. Зловред выводит рекламу прямо на домашний экран устройства.

Интересно, что закрытие или остановка приложения не приводят к прекращению работы вируса, вредоносный код продолжает демонстрировать рекламу.

Специалисты Sophos рассказали, что код запускает несколько процессов, каждый из которых создаёт и блокирует определенный файл. Затем процессы отслеживают друг друга, чтобы обеспечить создание и блокировку необходимых файлов. Как только область данных, созданная определённым процессом, будет разблокирована, она инициирует серию инструкций, которые перезапускают процесс и воссоздают разблокированный файл.

***

20.06.2017

В США произошел крупнейший в истории слив данных пользователей

Персональные данные 198 млн избирателей США были выложены в открытый доступ на сервере Amazon S3. Сервером пользуется аналитическая фирма-подрядчик Республиканской партии, которая собирала эти данные во время президентских выборов. Компания уверяет, что это делалось ради определения лучшего эфирного времени для политической рекламы.

Докладніше

***

20.06.2017

Китайское вредоносное ПО используется для атак на банкоматы в Индии

В Индии злоумышленники используют вредоносное ПО Rufus для атак на банкоматы, работающие под управлением операционной системы Windows XP. По информации издания The Dailymail, нападениям подверглись банкоматы в населенных пунктах штатов Западная Бенгалия, Гуджарат, Одиша и Бихар (InternetUA).

Атаки осуществлялись в ночное время. С помощью вредоносного ПО злоумышленники всего за несколько минут опустошали банкомат. Для инфицирования устройства использовался USB-накопитель, содержащий вредоносный файл. Заразив устройство, вредонос инициировал перезагрузку системы, разрывая соединение с серверами операторов банкоматов.

Далее вредоносная программа генерировала код и отправляла его преступникам, которые преобразовывали его в пароль. Каждый раз при вводе пароля, банкомат выдавал наличные средства, которые преступники забирали и уходили, не привлекая внимания.

По словам правоохранителей, подобные атаки возможны из-за недостаточного обеспечения безопасности банкоматов.

***

20.06.2017

Сотни домашних веб-камер оказались доступны подглядывающим китайцам

Китайские хакеры продают программное обеспечение, способное обнаружить уязвимые веб-камеры с подключением к интернету в любой точке мира и получить к ним доступ. Об этом сообщает Mashable (InternetUA).

Издание отмечает, что инструмент продается за 28 долларов. Кроме того, злоумышленники организовывают групповые чаты в китайских мессенджерах, в которых делятся дополнительной информацией о взломах. В частности, в беседах публикуются логины и пароли для доступа к камерам.

Каждый день в чатах бесплатно публикуются логины и пароли к сотням камер: обычно в списке значится от 200 до 400 позиций.

Эксперты отмечают, что хакеры взламывают в основном системы для наблюдения за домом и камеры для контроля за детьми. При этом их

пользователи чаще всего не меняют системные настройки, поэтому злоумышленники могут легко получить к ним доступ и вести наблюдение без ведома владельца устройства.

***

20.06.2017
Обнаружена новая фишинговая атака на пользователей Facebook

Специалисты компании PhishLabs рассказали о новой фишинговой кампании, затрагивающей исключительно владельцев мобильных устройств. В основном атаки направлены на пользователей Facebook, а также сервисов Apple iCloud, Comcast, Craigslist и OfferUp.

Докладніше

***

21.06.2017
Никита Готский
Хакеры остановили производство на заводе Honda

Фабрика компании Honda в японском городе Саяма прекратила работу из-за атаки хакеров. Об этом пишут местные издания (HiTech-News.ru).

В конце минувшей недели система управления производственной линией Honda на территории Японии и за ее пределами подверглась нападению хакеров, в результате чего один из заводов временно приостановил работу. Сервис был заражен вредоносной программой-шифровальщиком. Все данные оказались заблокированными, за разблокировку киберзлоумышленники потребовали денежную плату. 20 июня система регулировки производства Honda вновь приступила к работе, подробности умалчиваются. Также сообщается, что этот вирус был схож с Wannacry, ранее заблокировавшим тысячи компьютеров по всему миру.

Массовая кибератака в мае этого года затронула 200 000 пользователей со всей планеты. Создатели антивируса Avast рассказали о 57 тысячах нападениях хакеров с применением вируса WannaCrypt0r 2.0. Данное вредоносное приложение распространялось, в основном, в Тайване, России и Украине.

***

21.06.2017
Разработчик опубликовал инструкцию по созданию банковских Android-троянов

В декабре минувшего года эксперты в области безопасности начали фиксировать появление новых банковских Android-троянов после того, как на подпольном форуме Exploit.in появилось руководство по разработке вредоносного ПО для Android, опубликованное русскоязычным вирусописателем, использующим псевдоним Maza-in. Помимо указаний по

разработке базовых версий вредоносных программ, инструкция включала исходный код трояна BankBot, а также web-узел для связи с вредоносным ПО.

Докладніше

***

21.06.2017

Троян Qakbot вызывает проблемы даже после удаления с компьютеров

Банковский троян Qakbot применяет новый метод атак и использует заражённые компьютеры в качестве серверов, даже когда его устраняют антивирусы. Он представляет собой червя, который способен красть логины и пароли, создавать бэкдор и скачивать дополнительное вредоносное ПО, оставаясь незамеченным.

Докладніше

***

22.06.2017

Microsoft признала отключение антивирусов сторонних производителей

Действия компании Microsoft на рынке антивирусов в последнее время привлекают повышенное внимание. Это способствует майская масштабная атака приложения-вымогателя WannaCry и жалоба лаборатории Касперского в антимонопольные органы Евросоюза. Российская компания обвинила Microsoft в отключении своего антивируса на Windows-компьютерах и использовании доминирующего положения для агрессивного продвижения собственного защитника Windows.

Докладніше

***

21.06.2017

Эпидемия WannaCry могла произойти из-за случайной утечки

Ошибки в коде и реализации вымогательского ПО WannaCry, в мае нынешнего года заблокировавшего сотни тысяч компьютеров по всему миру, могут служить подтверждением теории о том, что авторы шифровальщика допустили утечку вредоносной программы, и ее распространение началось до того, как она была полностью завершена. Такой точки зрения придерживается эксперт в области кибербезопасности Джейк Уиллиамс (Jake Williams).

Докладніше

***

22.06.2017

Киберпреступники крадут данные банковских карт

ESET зафиксировала новую фишинговую атаку: злоумышленники обманным путём пытаются завладеть данными банковских карт своих жертв

Киберпреступники прикрываются популярным сервисом Uber, сообщает «3Dnews» («КОММЕНТАРИИ:»).

От имени этой всемирно известной компании рассылаются электронные письма, в которых предлагается получить крупную скидку на следующую поездку в такси. Нажав на баннер в сообщении, пользователь попадает на фишинговый сайт, внешне схожий с официальным ресурсом Uber.

BURL-адресе этой мошеннической страницы фигурирует слово «uber», что может сбить невнимательных посетителей с толку.

Пользователям, попавшим на фишинговый сайт, предлагается создать аккаунт Uber, чтобы скидка была автоматически учтена в следующей поездке. Кнопка «входа» перенаправляет жертву на поддельную страницу регистрации - там нужно ввести личные данные, включая имя, фамилию, номер мобильного телефона, а также номер, срок действия и CVV/CVC банковской карты. Разумеется, вся эта информация сразу же оказывается в руках злоумышленников. Получив запрашиваемые сведения, мошенники попросту перенаправляют пользователя на официальный сайт Uber.

Фишинговая атака началась 17 июня. На 22 июня на фальшивую страницу перешли десятки тысяч пользователей из разных стран. Те, кто оставил злоумышленникам данные банковской карты, рискуют лишиться своих средств.

***

21.06.2017

В ЕС заблокируют крупнейший в мире торрент-трекер

Крупнейший в мире торрент-трекер The Pirate Bay закроют (Судебно-юридическая газета). Торрент-трекер The Pirate Bay нарушает закон об авторском праве.

«Высшая инстанция Суда Европейского союза постановила, что администраторы крупнейшего торрент-трекера The Pirate Bay нарушают закон об авторском праве, позволяя выкладывать на своем сайте ссылки на пиратский контент», – говорится в сообщении.

Указанный торрент-трекер был создан в 2003 году и с этого момента постоянно выдерживал давление правоохранителных органов, которые пытались навсегда закрыть этот сайт.

«Предоставление и управление онлайн-платформой для обмена произведениями, защищенными авторским правом, может являться нарушением авторских прав», – пишется в решении суда.

Так, постановление люксембургского суда может стать прецедентом в музыкальной и киноиндустрии в борьбе с пиратством. Оно стало результатом

разбирательства, инициированного голландской ассоциацией Stichting Brein, которая преследует The Pirate Bay с 2009 года.

Сообщается, что указанная группа подала в суд на двух местных интернет-провайдеров, потребовав заблокировать доступ к «Пиратской бухте».

Голландский суд обратился в Европейский суд с просьбой дать пояснение, нарушает ли Pirate Bay законы Европейского союза об авторском праве. Он постановил, что авторские права таки нарушаются.

Теперь всех интернет-провайдеров Европы могут обязать закрыть доступ к торрент-трекеру.

***

22.06.2017

Екс-секретар Нацбезпеки США: Замовником кібератак під час виборів у США був Путін

Джонсон заявив про мінімальну увагу до спроб злому в розслідуваннях конгресу (112.ua).

Колишній секретар Департаменту внутрішньої безпеки США Джей Джонсон під час слухань у Комітеті з розвідки Палати представників назвав президента РФ Володимира Путіна замовником масштабних кібератак під час виборчої кампанії. Про це повідомляє CNN.

«У 2016 році російський уряд за вказівкою самого Путіна організував кібератаки у нашій країні з метою вплинути на наші вибори. Просто і ясно. Тепер ключове питання для президента і Конгресу: "Що ми збираємося зробити для захисту американського народу та їхньої демократії від такого роду речей у майбутньому?"» – спитав Джонсон.

Він підкреслив, що спроба злому з боку російських хакерів отримала мінімальну увагу в розслідуваннях конгресу про втручання Росії у вибори. Президент Дональд Трамп і його прихильники регулярно відзначають, що російські хакери ніколи не міняли результатів голосування, хоча у своїх свідченнях про це регулярно заявляють співробітники розвідки Обами і Трампа.

***

26.06.2017

Кібератака на парламент Британії: зламано 90 акаунтів

Хакери зламали до 90 акаунтів електронної пошти депутатів або службовців британського парламенту під час кібератаки (Espreso.tv).

Про це повідомляє видання BBC.

Прес-секретар британського парламенту зауважив, що внаслідок кібератаки, що відбулася 23 червня, постраждали менше 1 % з 9000 користувачів сервера. Він зауважив, що «хакнути» акаунти вдалося тому, що парламентарі використовували занадто прості паролі. Зараз у цій справі проводиться розслідування.

В результаті цього інциденту членам палати громад і співробітникам парламенту відключили віддалений доступ до робочої електронної пошти.

***

26.06.2017

Прихильники «ІД» залишили повідомлення для Трампа на урядових сайтах Огайо

Хакери зламали низку сайтів уряду американського штату Огайо і розмістили на них пропаганду терористів «Ісламської держави» (Espreso.tv).

Про це повідомляє видання The Associated Press.

Зазначається, що невідомі здійснили кібератаки на сайт губернатора штату республіканця Джона Кейсіка, його дружини, а також сайти департаментів. Представники губернатора зауважують, що наразі роблять все, аби прибрати повідомлення з сайту.

У залишеному хакерами тексті написано, що «(президент США Дональд, – ред.) Трамп і всі ваші люди будуть притягнуті до відповідальності за кожну краплю крові, пролиту в мусульманських країнах». У посланні також говориться: «Я люблю “Ісламську державу”».

***

26.06.2017

Никогда не входите в чужие учетные записи на своем iPhone

Мошенники и шантажисты существовали всегда, и появление облачных сервисов подарило им еще один инструмент незаконного заработка. В этом материале мы расскажем о новой схеме вымогательства, постаравшись не описывать ее слишком детально, чтобы это не выглядело как инструкция для новых жуликов (InternetUA).

Суть трюка состоит в том, чтобы под тем или иными предлогом (а они могут быть очень изобретательными) заставить вас ввести на своем iOS-устройстве Apple ID и пароль другого пользователя. Нужно понимать, что в этот момент ваш гаджет уже перестает вам принадлежать и становится инструментом шантажа.

Зайдя на iCloud.com и воспользовавшись функцией «Найти iPhone», злоумышленник сможет удаленно включить на вашем устройстве режим пропажи и потребовать выкуп за разблокировку. После этого у вас остается только два варианта: либо пойти у него на поводу, либо отправиться в магазин за новым iPhone или iPad.

Поэтому еще раз призываем вас быть максимально бдительными и не поддаваться на уловки мошенников. Ваше устройство предназначено только для вашего Apple ID, пусть эта простая мысль всегда будет с вами.

***

26.06.2017

На взлом «самой безопасной» Windows 10 S ушло всего три часа

Когда компания Microsoft анонсировала операционную систему Windows 10 S, от ее представителей звучали очень смелые заявления по поводу безопасности новой платформы (InternetUA).

О невозможности взлома Windows 10 S сообщалось еще ни раз, особенно после атаки вируса WannaCry. Однако специалистам издания ZDNet, вместе с исследователем в области безопасности Мэтью Хайкий, удалось доказать обратное.

Результатом их совместной деятельности стал взлом Windows 10 S всего за три часа. Именно столько времени специалистам потребовалось на обход всех защитных механизмов Microsoft.

Хайкий и команда ZDNet достаточно сильно удивились, что взломать Windows 10 S оказалось так просто. Подобраться к ОС удалось за счет использования макросов Word.

Хайкий использовал вредоносный документ Word, содержащий в себе определенные макросы. Они позволили ему провести инъекцию DLL-библиотек и обойти ограничения магазина путем внедрения кода в существующие авторизованные процессы операционной системы. В этом случае Word запускался с правами администратора через Диспетчер задач.

В результате, взломщики смогли получить доступ к системе с администраторскими правами. Они инсталлировали в Windows 10 S софт Metapoilt и смогли удаленно делать с системой все, что душа пожелает.

***

27.06.2017
Описан новый метод взлома почтовых ящиков

Израильские ученые описали новый метод атаки под названием PRMitM (Password Reset Man-in-the-Middle), позволяющей инициировать сброс пароля от электронной почты пользователя при его регистрации на другом сайте. PRMitM предполагает использование методов социальной инженерии, поскольку атакующим потребуется убедить потенциальную жертву зарегистрировать учетную запись на специально созданном сайте.

Докладніше

ДОДАТКИ

Додаток 1

20.06.2017
10 хитрых функций чата WhatsApp, которые облегчат общение

На днях WhatsApp обновился, получив новые интересные возможности, которые делают общение проще. Но в этой подборке не только они (InternetUA).

#1. Отвечай на конкретное сообщение собеседника

Как: свайп слева-направо по сообщению

Эта возможность очень важна в активной переписке – особенно, когда речь о групповом чате.

Когда отвечаешь на конкретное сообщение с помощью этой новой фичи, получаешь блок древовидной формы, в котором сразу понятно о чем вообще речь.

#2. Добавляй любые фильтры при отправке снимков

Как: свайп снизу-вверх во время добавления фото

Вспоминай! Кому принадлежит WhatsApp? Правильно – Facebook. Каким еще интересным сервисом он владеет? Да, Instagram. Поэтому появление такой фишки закономерно.

Теперь во время отправки снимков собеседнику можешь добавить фильтры для каждой фотки.

#3. Не бойся отправлять большое количество фото

Как: шли снимки без разбора

Моделируем ситуацию, во время активного диалога в групповом чате решаешь отправить друзьям подборку фотографий из какого-то интересного места.

Раньше боялся делать это, ведь фотки заполонили бы весь чат так, что до необходимого сообщения нужно было бы листать долго и нудно. А теперь снимки группируются в альбом. Это победа.

#4. Следи за статистикой трафа во время общения

Как: Настройки – Данные и Хранилище – Статистика

Если пользуешься WhatsApp действительно активно – регулярно переписываешься, пересылаешь фотографии и звонишь с помощью сервиса – эта возможность для тебя.

В приложении есть меню со статистикой используемого трафика, который поможет понять, куда уходят твои мегабайты из тарифного плана.

#5. Сохраняй или не сохраняй медиа в фотопленку

Как: Настройки – Чаты – Сохранить в Фотопленку

Все пользователи WhatsApp делятся на два типа: первые хотят видеть все полученные через мессенджер снимки в галерее iPhone, другие – нет.

Поэтому меняй положение этого переключателя по личным потребностям.

#6. Блокируй уведомления собеседников или чатов

Как: Меню диалога – Не беспокоить

Уверен, в твоем WhatsApp достаточно групповых диалогов, которые не можешь удалить, но получать от них уведомления регулярно уже устал – может, у тебя тут работу обсуждают, а ты в отпуске.

Такие можешь временно «успокоить». Для этого разработчики предусмотрели соответствующую возможность.

#7. Получи информацию про сообщения в переписке

Как: свайп справа-налево по сообщению

В этом меню, о котором знают немногие, получишь информацию о том, когда сообщение было доставлено и когда прочитано.

Эта возможность пригодится на случай важных переговоров.

#8. Отправляй сообщения без подключения к инету

Как: вот так

Даже если в данный момент ты не подключен к интернету, можешь отправлять сообщения без проблем.

Все они отмечаются иконкой с изображением часиков и будут отправлены собеседнику, когда подключение к сети появится.

#9. Отмечай записи для своего перечня избранных

Как: длинный тап по сообщению

Редко, но бывают моменты, когда обмениваешься через WhatsApp действительно важной информацией. Если получил что-то такое, можешь добавить в список избранного.

Получить доступ ко всем отмеченным сможешь через настройки программы.

#10. Вспоминай о форматировании, если это нужно

Как: выделяй жирный звездочками, курсив подчеркиванием, а перечеркнутый – фигурными тире

Если серьезно относишься к переписке, всегда выделяешь важную информацию форматированием.

Если нет, рекомендую начать делать это – больше шансов, что собеседник правильно поймет всю необходимую информацию.

(вгору)

Додаток 2

25.06.2017

В мобильном клиенте YouTube появится долгожданная функция

На этой неделе в Лос-Анджелесе прошло ежегодное мероприятие VidCon, где представители YouTube традиционно рассказывают о достижениях и новых функциях сервиса. В этом году посетителей ждало сразу несколько громких анонсов. Во-первых, генеральный директор YouTube Сьюзен Войчицки объявила, что ежемесячная аудитория пользователей YouTube превысила 1,5 миллиарда человек. А если учесть тот факт, что некоторые пользователи смотрят видео без авторизации в сервисе, то их число ещё больше. Это значит, что каждый пятый житель Земли ежемесячно заходит на YouTube, чтобы посмотреть какое-то видео. Но самое главное, что в YouTube появится давно ожидаемая функция (InternetUA).

На мероприятии объявили, что в мобильном клиенте YouTube появится возможность заполнять экран видео независимо от его формата даже в вертикальном положении. Это значит, что снятые вертикально видеозаписи

теперь можно будет смотреть в полноэкранном режиме. При этом пользователь сможет произвольно менять размер окна.

Ещё одним изменением станет новый способ совместного просмотра видео через мобильное приложение. Пользователи смогут поделиться роликом со своими друзьями из списка контактов, а затем вместе обсудить его в специальном чате и добавить туда новое видео.

Также команда разработчиков YouTube объявила, что подписчиков YouTube Red ждут новые эксклюзивные шоу, которые выйдут позже в этом году.

Последним анонсом стала презентация нового формата VR180, разработанного специально для 360-градусных видео. Это формат для тех, кто всё же хочет посмотреть ролик, но не имеет VR-гарнитуры или не хочет крутить смартфоном или планшетом вокруг себя. Как следует из названия, видео в формате VR180 отображают только 180 градусов от сферического ролика.

Все нововведения постепенно станут доступны пользователям по всему миру.

(вгору)

Додаток 3

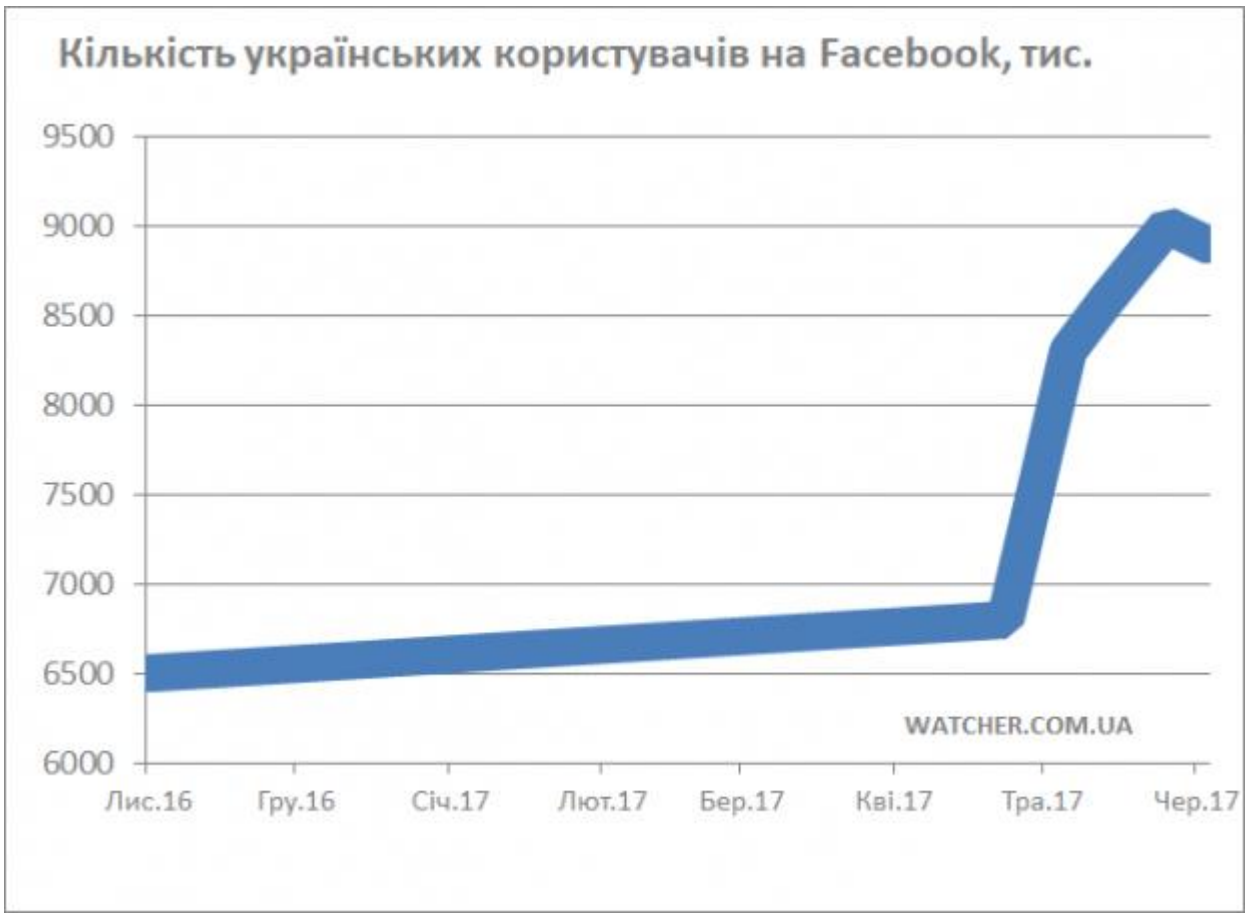
27.06.2017

Олег Дмитренко

5,6 млн українців вже користуються Instagram, а Facebook просів до 8,9 млн

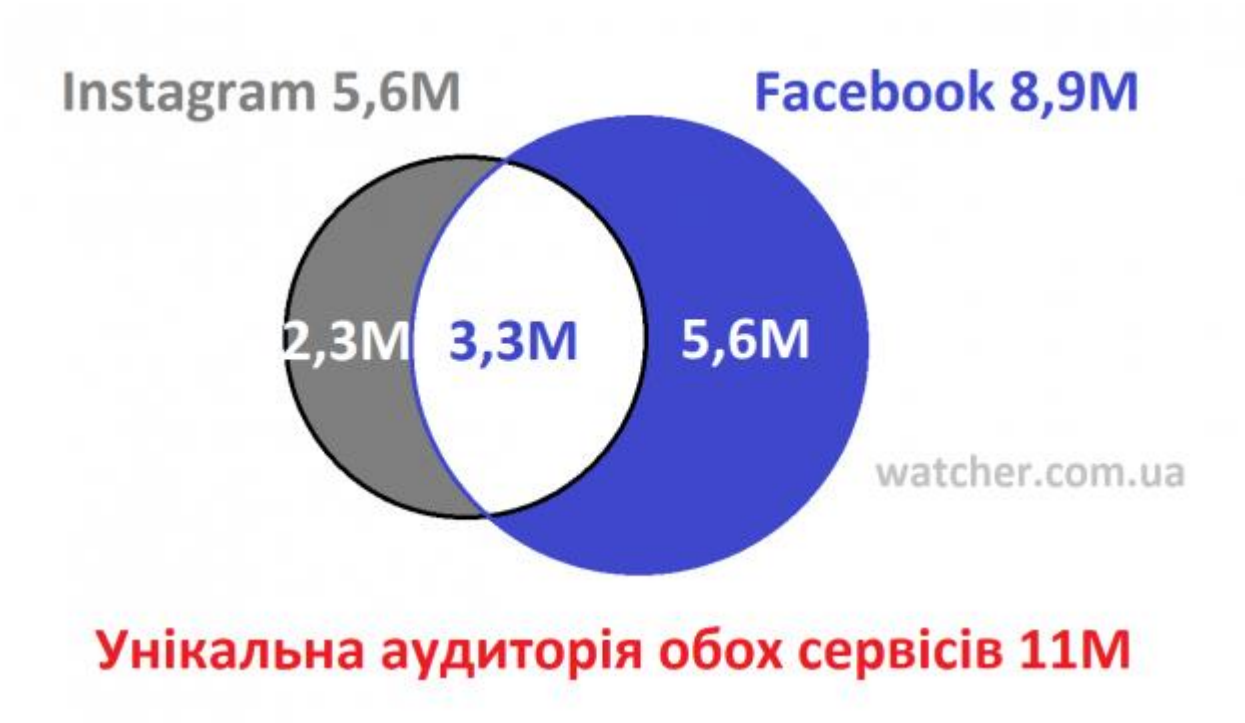
Аудиторія Instagram за останні півтора місяці виросла майже в півтори рази – з 3,8 млн до 5,6 млн користувачів. Про це свідчать дані внутрішньої статистики Facebook для рекламодавців (Watcher).

Цікаво, що за останній тиждень кількість українських користувачів Facebook зменшилась на 100 тис – з 9 млн до 8,9 млн. Рекорд в 9 млн було зареєстровано 19 червня.



Ймовірно, що основна причина цього невеликого падіння полягає в тому, що в перший тиждень після заборони російських соціальних мереж в Україні (з 18 травня), був сильний пік в кількості нових реєстрацій. Звісно, що не всі користувачі, які зареєструвались, стали постійними користувачами соцмережі. А статистика Facebook зараховує до користувачів цієї соцмережі лише тих, хто хоча б раз протягом останніх 30 днів був залогінений в сервіс. Аналогічно рахуються й користувачі Instagram.

Як свідчать дані Facebook, загальна унікальна аудиторія Facebook та Instagram в Україні складає 11 млн. Зважаючи на те, що з цих 11 млн Інстаграмом користуються 5,6 млн, а Facebook – 8,9 млн, це означає, що спільно обома сервісами користується 3,3 мільйони українців. Окремо Facebook користуються 5,6 млн, а Instagram – 2,3 млн:



Що цікаво, саме Instagram та Facebook стали основними реціпієнтами нових користувачів з «ВКонтакте» та «Одноклассників». Сумарна унікальна аудиторія Instagram та Facebook ще на початку травня становила 7,5 млн користувачів. Тобто з моменту введення дії заборони на доступ до російських соцмереж, унікальна аудиторія обох сервісів приросла на 3,5 млн.

(вгору)

Додаток 4

19.06.2017

Порошенко рассмотрит петицию об отмене блокировки соцсети «ВКонтакте»

Петиция к Президенту Украины Петру Порошенко об отмене блокировки российской социальной сети «ВКонтакте» перешла в статус «на рассмотрении», передает УНН со ссылкой на сайт Президента (ЧАС.UA).

Петиция набрала 25,352 голоса из 25 тыс. необходимых для рассмотрения.

«Это огромная рекламная платформа, которая помогает в реализации отечественного продукта, творчества, контента и т. д. Потеря этой платформы крайне негативно скажется на отечественном производителе любого вида товаров, услуг и ивентов. Данное решение администрации президента несет ряд негативных последствий», – говорится в тексте петиции.

Автором петиции выступил Анатолий Ткаченко.

Петиция была зарегистрирована 16 мая. Сейчас сбор подписей завершен.

Отметим, что рассмотрение электронной петиции осуществляется не позднее десяти рабочих дней со дня опубликования информации о начале его рассмотрения.

О поддержке или не поддержке электронной петиции, адресованной Президенту Украины, публично объявляется Президентом Украины на сайте Официального интернет-представительства Президента Украины.

Ответ на электронную петицию не позднее следующего рабочего дня после окончания ее рассмотрения публикуется в разделе электронных петиций на странице «С ответами», а также направляется в письменном виде автору (инициатору) электронной петиции.

(вгору)

Додаток 5

24.06.2017

По ту сторону монитора: психолог объяснила, как манипулируют людьми в соцсетях

Любой пользователь соцсетей становится легко доступным для манипуляций, если он проводит длительное время за монитором. Когда человек устает, то в этом случае он впадает в состояние транса и его поведение подвержено программированию (Обозреватель).

Об этом в эфире «Обозреватель.LIVE» заявила кандидат психологических наук, доктор философии PhD, ведущий научный сотрудник лаборатории общей и этнической психологии Наталья Бугаева.

Так, отвечая на вопрос о стереотипах, нормах и манипуляциях в социальных сетях, она сказала: «Когда человек постоянно смотрит в монитор, то он постепенно утомляется».

«Большое количество информации, которое поступает в мозг, со временем вызывает защитную реакцию – торможение, так называемое полугипнотическое состояние», – пояснила эксперт.

По словам психолога, у детей и подростков такое состояние начинается через 15-20 минут, а у взрослых – через 40-50 минут, проведенных в интернете.

«Вы можете легко определить, что человек впал в такое состояние, по застывшему взгляду», – подчеркнула Бугаева.

«В этом состоянии транса вся информация, которая к нам поступает, уже не анализируется человеком, потому что он утомлен. Однако усиливаются функции ее запечателния. В этом состоянии человек становится легко доступным для манипуляций, для программирования поведения", - рассказала она.

Эксперт посоветовала делать перерывы через каждые 40-50 минут, проведенные за компьютером. «Нужно, чтобы человек менял вид деятельности и таким образом, выходил из этого состояния», – отметила кандидат наук.

«Из этого состояния больного выводит сильный хлопок. Если чувствуете, что с вами что-то происходит, нужно хлопнуть в ладоши и вернуть себя в реальность. Погулять и после снова вернуться к работе», – добавила Бугаева.

(вгору)

Додаток 6

25.06.2017

Влияние социальных сетей на психику пользователей

Яркие фотографии из аккаунтов звезд, популярных фитнес-моделей, топ-блогеров, путешественников и прочих «успешных людей» в социальных сетях негативно сказываются на психическом состоянии обычных пользователей. Это проявляется в тревоге, лишении сна и завышенных требованиях к своей внешности у молодых людей, которые являются наиболее активными в интернете (ПСИ-ФАКТОР).

Хуже всего на душевное состояние влияет Instagram, в котором на данный момент зарегистрированы 700 миллионов человек.

Таковы данные нового исследования, проведенного Королевским обществом здравоохранения Великобритании (RSPH). В докладе приводятся данные ранее опубликованных исследований о влиянии социальных сетей на здоровье, а также результаты собственного социального опроса RSPH, в котором приняли участие около 1,5 тысячи британцев в возрасте от 14 до 24 лет.

Чтобы узнать, как разные социальные сети влияют на здоровье, респондентов спрашивали об ощущениях во время взаимодействия с ними. Вопросы задавали касательно пяти популярных интернет-ресурсов: Instagram, Facebook, Snapchat, YouTube и Twitter.

Положительный эффект участники соцопроса почувствовали только от YouTube, все остальные ресурсы оказывали на них негативное влияние. Порядок соцсетей от менее к более негативной, согласно данным исследования, выглядит следующим образом: Twitter, Facebook, Snapchat и Instagram. Instagram, в частности, вызывал у опрошенных чувство беспокойства и недовольства собственным телом. Один из авторов доклада рассказал CNN, что девушки часто сравнивают себя с оторванными от действительности картинками, созданными в Instagram с помощью специальных фильтров. В исследовании приводятся слова одного из респондентов: «Instagram легко заставляет девушек и женщин чувствовать, что их тела недостаточно хороши, поскольку люди добавляют фильтры и редактируют свои фотографии, чтобы они выглядели «идеально».

Предыдущие исследования показали, что завышенные ожидания и создаваемый соцсетями страх упустить что-то важное могут снизить уровень самооценки человека и послужить причиной возникновения тревоги и депрессии. Эти проблемы только усугубляются психологическим давлением на личность в интернете и отсутствием сна – еще одним вредным последствием длительного времяпрепровождения в соцсетях. В докладе также приводятся данные недавнего исследования, опубликованного в «Журнале молодежных исследований», согласно которому каждый пятый молодой человек просыпается ночью, чтобы проверить сообщения, в результате чего чувствует себя изнуренным в течение дня.

Впрочем, нельзя сказать, что результаты проведенного RSPH опроса говорят только о негативном воздействии социальных медиа. Почти 70 %

респондентов сообщили, что получили в соцсетях эмоциональную поддержку в трудное время; многие заявили, что их аккаунты предоставили им площадку для позитивного самовыражения. Кроме этого, по словам опрошенных, благодаря соцсетям они также могли знакомиться и поддерживать отношения в интернете.

Проблемы у людей возникали в основном из-за того, что они забывали очень важный момент: то, что мы видим, не всегда является реальностью.

Основываясь на результатах проведенного исследования, RSPH составило перечень рекомендаций:

Знаменитости и другие популярные пользователи должны раскрывать информацию о том, что та или иная фотография была обработана.

Социальные сети с помощью всплывающих сообщений должны уведомлять пользователей, когда они превышают определенное время нахождения в сети.

Социальные медиа могут даже обнаруживать людей с возможными психологическими проблемами на основе их пользования ресурсом, и отправлять им конфиденциальное сообщение о том, куда можно обратиться за помощью.

В докладе также отмечается, что для получения более подробных данных о влиянии социальных сетей на здоровье необходимы дополнительные исследования. В конце авторы резюмируют, что сила социальных медиа сегодня слишком велика, чтобы несерьезно относиться к их влиянию на здоровье человека.

(вгору)

Додаток 7

20.06.2017

YouTube рассказала о четырёх новых способах борьбы с экстремистскими видео

В последние месяцы на социальные сервисы оказывается особенно сильное давление касательно контента, который содержит террористическую пропаганду. YouTube рассказала о четырёх новых способах борьбы с экстремистами в рамках платформы (Grifonsoft).

Кент Уокер (Kent Walker), старший вице-президент и генеральный консул Google, написал, что YouTube работает с различными правительственными и правоохранительными органами над поиском и удалением такого содержимого. Вместе они внесли вклад в разработку систем, которые упрощают выполнение этой задачи.

Первый шаг – это расширение возможностей поиска автоматизированными системами видеороликов, связанных с терроризмом. Компания использует машинное обучение для тренировки «классификаторов контента». Они помогают быстрее находить и удалять ролики.

YouTube расширила список участников программы YouTube Heroes, которым доступны особые привилегии. Одна из них – возможность отмечать не

соответствующий правилам сервиса контент. Уокер отметил, что к 63 подписанным на программу неправительственным организациям присоединились ещё 50. При этом Google увеличила размер денежного поощрения за участие в инициативе. Так компания собирается бороться со специфичными группами видео.

Третий шаг – уделить более пристальное внимание видеороликам, в которых нарушение стандартов сообщества довольно условно. Сюда, например, входит контент, который разжигает религиозную ненависть. Такие видео компания удалять не будет: она собирается скрывать их от глаз пользователей. К тому же, через них нельзя будет получать доход с рекламы.

Наконец, YouTube улучшит программу Creators for Change. Через неё авторы создают ролики на важные темы, включая борьбу с терроризмом. Когда пользователь окажется на странице с экстремистским роликом, сервис перенаправит его к одному из видео, созданных в рамках программы.

(вгору)

Додаток 8

21.06.2017

Алексей Симончук

Оксфордский университет: в Украине копируют российскую пропаганду

Почему общественные организации борются с российской пропагандой эффективнее государства, сколько стоит создать армию ботов и как появляются фейковые новости (Телекритика).

Оксфордский университет изучил опыт использования соцсетей в качестве манипуляторов общественного мнения девяти стран (Россия, Бразилия, Канада, Украина, США, Польша, Германия, Китай, Тайвань) и подготовил исследования на эту тему. «Телекритика» ознакомилась с отчетом по Украине и выбрала из него самое главное.

Кто и как проводил исследование

Для того, чтобы провести исследование университет обратился за помощью к Марине Жадановой и Дарье Орловой – участницам проекта StopFake, именно они и составили отчет.

В нем рассматривается состояние пропаганды в Украине. Основное внимание уделяется двум аспектам: ответу Украины на российскую пропаганду и использование пропаганды внутри страны. Отчет создан на основе интервью с украинскими экспертами в СМИ, учеными, разработчиками ботов и т. д. Он исследует масштаб проблемы и определяет наиболее распространенные тактики, инструменты и подходы работы ботов в интернете.

Идеальные площадки для ботов

Все социальные сети в Украине можно использовать для работы ботов. Разница между ними в стоимости производства и популярности таких услуг. Самая простая и дешевая платформа – «ВКонтакте», поскольку у нее нет строгих мер безопасности, что позволяет легко и массово регистрировать

аккаунты. Однако украинские пользователи этой соцсети больше всего сосредотачиваются вокруг своих близких, знаменитостей и развлечений, поэтому политические боты там не так и заметны.

«Через 5 лет в Украине будет с соцсетями ситуация аналогичная российской»

На втором месте стоит Twitter. Там около 48 млн.учетных записей (15 % всех пользователей) являются ботами. Facebook же является наиболее эффективным с точки зрения защиты пользовательских данных, поэтому там тяжелее всего создавать ботов. Поскольку эта сеть является самой популярной среди социальных и политических элит в Украине, боты там самые дорогие для создания и спрос на них регулярно растет.

Как работают боты и тролли

Опрошенные эксперты признали, что в Украине существует целая индустрия различных услуг, разработанных для целей политического общения. Сначала проплаченных ботов использовали для комментирования материалов и новостей на сайтах популярных СМИ, потом перешли к таким платформам как LiveJournal, а теперь используют для этого социальные сети.

Согласно исследованию, дискредитация противников и продвижение определенных вопросов/решений имеет несколько этапов. Обычно это начинается с первоначальной публикации ключевого сообщения, упакованного в какую-то историю. Его постят либо в социальных сетях, либо в онлайн-СМИ за деньги. После чего тему поднимают лидеры общественного мнения, у которых много подписчиков в соцсетях. Как только тему много обсуждают в интернете, о ней начинают говорить телеканалы.

Также в исследовании говорится, что основные политические партии создавали внутренние подразделения в своих штаб-квартирах, которые напрямую занимались социальными сетями. Их возглавляют политические консультанты, которые разрабатывают основные ключевые сообщения и план их распространения по различным каналам связи. Иногда внутренние отделы SMM передают часть своих проектов независимым компаниям, чаще всего это происходит, когда необходима помощь во время кризиса.

Несмотря на то, что многие считают, что боты не могут формировать общественное мнение, исследователи указывают на то, что они создают другие проблемы. Например, PR, маркетинговые и политические исследования не могут качественно оценить рынок из-за большого наличия ботов.

О чем еще исследование

Исследователи считают, что через 5 лет в Украине будет с соцсетями ситуация аналогичная российской. Это связано и с запретом российских ресурсов, массовым использованием провластных ботов, и дискредитацией журналистов. Как пример, приводится ситуация с конфликтом между Министерством обороны и «Громадським».

«Основные политические партии создавали внутренние подразделения в своих штаб-квартирах, которые напрямую занимались социальными сетями»

Также много внимания в исследовании уделяется тому, что у общественных организаций получается эффективнее бороться с российской

пропагандой, чем у государства. В пример приводится организация Stopfake, которая разоблачает мифы российской пропаганды и информационные войска, созданные Министерством информационной политики, которые, согласно исследованию, оказались провальным проектом, ведь его участникам больше не дают новых заданий.

Пропаганду используют не только для манипулирования общественным мнением, но и для дискредитации противников и защиты интересов разных политических и деловых групп. Исследователи также пишут, сколько стоят фейковые аккаунты. Так, в Facebook их стоимость колеблется от $0,9 до $200, а в Twitter – от $0,40 до $90.

(вгору)

Додаток 9

27.06.2017

Дарина Шварцман

Microsoft, YouTube, Facebook и Twitter заключили антитеррористическое партнерство

Крупнейшие мировые технологические компании, в числе которых Microsoft, YouTube, Facebook и Twitter, анонсировали Глобальный интернет-форум по борьбе с терроризмом, который рассчитан на упрощение совместной работы, поиску технологический решений, а также сотрудничестве правительствами различных стран и общественными с организациями. Об этом пишет The Guardian (InternetUA).

Программа основана на нескольких уже существующих инициативах, нацеленных на удаление террористических материалов.

Отмечается, что компании на протяжениидлительного времени пытались сбалансировать поддержку свободы слова с необходимостью удаления и предотвращения распространения террористического контента. Они провели серьезный анализ того, как террористические группы использовали интернет-ресурсы для вербовки и распространения ненавистных и жестоких сообщений.

В рамках нового форума Facebook, YouTube, Twitter и Microsoft обещают делиться передовыми технологиями, касающимися «методов обнаружения и классификации контента с использованием машинного обучения» и «определять стандартные методы отчетности для изъятия террористического контента».

По мере времени масштаб проекта будет расширяться, однако цели останутся неизменными – улучшение технологии для обнаружение террористического контента и создание практик для борьбы с экстремизмом и ненавистью в сети. Также организации будут сотрудничать с ООН, проводя серию воркшопов на контр-террористические темы.

(вгору)

Додаток 10

16.06.2017

Украинским СМИ отобьют желание подзаработать у Путина

СБУ намерена инициировать изменения в законодательстве и ввести криминальную ответственность за распространений российской пропаганды (Знай.ua).

Служба безопасности Украины будет жестче бороться с кремлевской пропагандой. Предлагается изменить законодательство и ввести криминальную ответственность за ее проявления в украинских медиаресурсах.

Об этом сообщил глава спецслужбы Василий Грицак, передает пресс-центр СБУ. Он отметил, что на протяжении всего периода российской агрессии сотрудники спецслужб эффективно борются с разведывательно-диверсионной и информационно-подрывной сетью России. Но все полностью искоренить ее еще не удалось, поскольку Кремль подготавливал пятую колону еще задолго до открытого нападения.

Грицак добавил, что Москва активно манипулирует несовершенством украинского законодательства и свободой слова в Украине.

«Настоящий патриотизм – это не только разговоры о любви к Украине. Адекватный отпор врагу требует решительных совместных действий, сочетание силы права и силы общественного мнения, как оружия против российской агрессии в информационном пространстве. Для этого нам нужно, во-первых, срочно разработать и принять изменения в законодательство Украины об уголовной ответственности. СБУ готова присоединиться к этой работе», – подчеркнул глава СБУ.

Перед Украиной, по его словам, сейчас стоит цель дать адекватную оценку всем формам и методам гибридной войны и прописать это в Уголовном кодексе. Он считает, что украинские журналисты должны совместно противостоять проявлениям пропаганды.

«Для сторонников "путинского русского мира" должна остаться только "киселевско-соловьевская" площадка. Это – сила общественного мнения. Призываем всех патриотов стать с нами плечом к плечу и разделить ответственность за будущее Украинского государства», – резюмировал Грицак.

(вгору)

Додаток 11

16.06.2017

СБУ затримала адміністратора групи «ВКонтакте», який навчав, як обійти блокування соцмережі

Співробітники Служби безпеки України затримали жителя Павлограда Дніпропетровської області, який адміністрував антиукраїнські групи у «ВКонтакте» і поширював інструкції з обходу блокування доступу до російських сайтів через використання VPN (LB.ua).

Про це повідомляє прес-центр СБУ.

Правоохоронці встановили, що в 2016 році на чоловіка «вийшли» представники російських спецслужб, які запропонували йому адмініструвати і наповнювати антиукраїнську спільноту в Інтернеті.

«За вказівкою кураторів адміністратор розміщував статті, фотографії і відеоматеріали із закликами до насильницької зміни або повалення конституційного ладу. У матеріалах, зокрема, стверджувалося, що Україна є частиною Росії, а українська армія – недієздатна», – йдеться в повідомленні.

Серед останніх вказівок, отриманих жителем Павлограда від російських кураторів, було активне поширення актуальної інформації про блокування окремих російських інтернет-ресурсів та інструкцій щодо обходу заборони через використання VPN-сервісів.

Під час обшуків за місцем проживання сепаратистського адміністратора оперативники СБУ виявили мобільні пристрої з доказами співпраці з російськими спецслужбами.

Відкрито кримінальне провадження за ч. 2 ст. 109 Кримінального кодексу України (дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади).

(вгору)

Додаток 12

19.06.2017

Евгения Подгайная

Киберполиция продолжает мониторить контент заблокированного «ВКонтакте»

На сайте киберполиции появилась очередная новость о пресечении распространения порно «ВКонтакте» (InternetUA).

«В социальной сети «ВКонтакте» в последнее время увеличилось число фактов распространения файлов с детской порнографией, – говорится в релизе КП. – Вызывает возмущение, когда администрация сети не идет на сотрудничество в блокировании такого незаконного контента, мотивируя это тем, что они находятся вне юрисдикции украинского законодательства».

По данным сообщения, работниками Киевского управления киберполиции совместно со следственным отделом Броварского отдела полиции ГУНП в Киевской области выявлено и задокументировано группу в социальной сети «ВКонтакте», где проводилось распространение детской порнографии. Администраторами группы оказались 13-летняя жительница Броваров и 12-летняя гражданка, которая в настоящее время находится за пределами страны.

«Во время санкционированного обыска по месту жительства злоумышленницы полицейские изъяли технические средства, с помощью которых 13-летняя жительница Броваров осуществляла администрирование группы и размещала запрещенный контент, – поясняется в релизе. – Изъятую технику направлено в экспертный центр для проведения необходимых экспертиз».

Интересно другое. С одной стороны, в обязанности киберполиции, СБУ, Министерства информационной политики входит мониторинг инфополя, в том числе и контента заблокированных ресурсов. С другой стороны, получается, что не только простые граждане, а и госорганы обходят нормы Указа Президента.

Ранее глава киберполиции Сергей Демедюк сообщил нашему изданию, что провайдер «Инфоком» (который оказывает интернет-услуги КП) уже не предоставляет возможности доступа к веб-ресурсам, указанным в санкционном списке.

(вгору)

Додаток 13

26.06.2017

Николай Офицеров

Дуров нашел в требованиях Роскомнадзора нарушение Конституции РФ

Требование, озвученное Роскомнадзором о предоставлении ведомству данных о Telegram, полностью противоречит Конституции России. Об этом заявил Дуров на своей странице «ВК» (HiTech-News.ru).

«Глава Роскомнадзора почему-то уверен, что Telegram может выдать спецслужбам «ключи для дешифрации», чтобы те смогли читать переписку и заниматься ловлей террористов. Это требование не только лишь противоречит статье Конституции о тайне переписки, но также и демонстрирует незнание того, как именно шифруется коммуникация в 2017 году. Строится обмен секретной информацией на оконечном шифровании, к которому сами владельцы мессенджеров доступа попросту не имеют, потому каких-либо ключей в данном случае просто не существует, ведь они хранятся исключительно на девайсах самих пользователей», – заявил Дуров.

Потенциальная блокировка в России Telegram никак не усложнит задачу террористов, так как в их распоряжении останутся десятки других мессенджеров. По мнению Дурова, ни одна страна мира не идет на блокировку всех подобных мессенджеров, ведь ее руководство понимает, что победа над терроризмом через блокировки возможна только если «заблокировать весь интернет».

Глава правительственного ведомства, участвующего в споре, Александр Жаров лично обращался к Дурову, потребовав от него выдать все данные компании, управляющей мессенджером для внесения в реестр организаторов распространения информации. Только так он сможет работать в России, иные альтернативы пока не существуют.

(вгору)

Додаток 14

16.06.2017

Facebook случайно раскрыла имена модераторов, которые удаляют страницы потенциальных террористов // Уязвимость затронула около тысячи человек

Компания Facebook случайно раскрыла данные модераторов, которые проверяют и удаляют страницы за несоблюдение правил сайта, в том числе, за использование сексуального контента, разжигание ненависти и пропаганду терроризма, сообщает The Guardian (Зеркало недели. Украина).

Как подчеркивает издание, из-за этой уязвимости потенциальные террористы могли узнать личные данные модераторов. Уязвимость затронула около тысячи человек, которые работали в 22 подразделениях Facebook и использовали программное обеспечение для модераторов.

Уязвимость была обнаружена в прошлом году. Она заключалась в следующем: когда модераторы Facebook удаляли профили администраторов сообществ, которые нарушали правила социальной сети, их имена высвечивались в журналах действий этих сообществ и были доступны для других администраторов. Об уязвимости стало известно после того, как модераторы Facebook стали получать запросы на добавление в друзья от людей, которые подозревались в связях с терроризмом.

Из тысяч человек, чьи данные были раскрыты, 40 работали в контртеррористическом подразделении, которое базируется в Дублине. Шесть из них находятся под наибольшей угрозой.

В Facebook признали наличие подобной уязвимости и заявили, что предприняли меры для того, чтобы «лучше выявлять и предотвращать появление подобных вопросов в будущем».

Вместе с тем, по мнению одного из модераторов, который пострадал в результате утечки, действий, предпринятых социальной сетью, недостаточно. Он переехал в Ирландию еще в детстве для того, чтобы избежать терроризма и угроз. После обнаружения утечки, он и его семья были вынуждены временно переехать в Восточную Европу. Мужчина подал к ирландским властям жалобу на Facebook и своего непосредственного работодателя, компанию Cpl Recruitment, с требованием компенсации.

(вгору)

Додаток 15

18.06.2017

Новое вымогательское ПО Sorebrect способно внедрять вредоносный код

С каждым днем злоумышленники становятся все изобретательнее и разрабатывают инновационные, более скрытые техники атак. Ярким примером тому может служить новое семейство бесфайлового вымогательского ПО Sorebrect, недавно обнаруженное специалистами компании Trend Micro (InternetUA).

В отличие от остальных шифровальщиков Sorebrect ориентирован на корпоративные системы. Программа внедряет вредоносный код, инициирующий процесс шифрования, в легитимные системные процессы (svchost.exe) на целевом компьютере, а затем самоуничтожается, чтобы избежать обнаружения.

Sorebrect получает доступ к учетным данным администратора при помощи метода брутфорс или других техник и использует Microsoft Sysinternals PsExec (утилита для удаленого выполнения команд) для шифрования файлов. Как пояснили исследователи, PsExec позволяет атакующим удаленно выполнять команды без необходимости организации авторизации или переноса вручную вредоносного ПО на удаленный компьютер.

Вымогатель также сканирует локальную сеть на наличие компьютеров с общедоступными папками. Затем Sorebrect удаляет все записи в журнале событий (с помощью wevtutil.exe), а также теневые копии файлов на инфицированном компьютере. По аналогии с другими вредоносными программами Sorebrect использует Tor для безопасного взаимодействия с управляющим сервером.

По данным экспертов, Sorebrect разработан для атак на системы предприятий в различных сферах, в том числе промышленной, технологической и телекоммуникационной. До недавнего времени основными мишенями атак являлись организации в странах Ближнего Востока, в частности Кувейта и Ливана, однако с мая нынешнего года эксперты начали фиксировать атаки, направленные на пользователей в Канаде, Китае, Хорватии, Италии, Японии, России, Мексике, Тайване и США.

(вгору)

Додаток 16

19.06.2017

Сотни программ в магазинах приложений выдают себя за сканеры вирусов

В конце мая специалисты компании McAfee предупредили пользователей платформы Android, что в официальном магазине Google Play Store есть множество приложений, которые якобы обеспечивают защиту от программы-вымогателя WannaCry. Судя по всему, в магазине наблюдается наплыв фальшивых антивирусных решений, которые не защищают устройства, а наоборот атакуют их (InternetUA).

В первую очередь нужно вспомнить, что вымогатель WannaCry работает на Windows, а не на Android или других системах. Само существование этого вымогателя стало возможно благодаря уязвимости в Windows. Компания RiskIQ обнаружила в магазине Play Store семь связанных с WannaCry приложений и ещё пару в магазине Apple App Store. Они требуют намного больше разрешений, чем среднестатистические приложения, включая пароль для доступа в систему.

В других магазинах и цифровых рынках также были обнаружены сотни похожих приложений, внутри которых содержится реклама, трояны и вредоносный код. Все они пытаются воспользоваться остатками паники вокруг WannaCry.

Исследователи утверждают, что из 4292 активных антивирусных приложений 525 не прошли проверку, из них 508 найдены в магазине Google Play Store, остальные в сторонних магазинах. Таким образом, механизмы защиты Google не смогли уберечь магазин от попадания в них сомнительных антивирусных приложений. Систему сканирования можно обойти, особенно если приложение работает как шлюз для вредоносных программ и не является такой программой само.

Пользователям рекомендуется скачивать программы проверенных разработчиков, читать отзывы в магазинах и следить за наличием орфографических ошибок в названиях и описаниях.

(вгору)

Додаток 17

19.06.2017

Создан руткит, умещающийся в модулях PHP сервера

Голландский web-разработчик Люк Парис (Luke Paris) создал руткит, который можно спрятать в PHP-модуле и использовать для взлома web-серверов по очень редкому вектору атаки – с помощью модулей Apache (InternetUA).

Как правило, руткит представляет собой код, работающий на самом нижнем уровне операционной системы, способный перехватывать операции ядра и производить вредоносные действия. Большинство современных руткитов работают возле ядра ОС и требуют от хакера наличия серьезных навыков, в частности, умение программировать на C и C++, чтобы не вывести из строя атакуемый компьютер. Однако созданный Парисом руткит взаимодействует не с ядром ОС, а с интерпретатором PHP, что намного упрощает его использование и не требует больших знаний.

«Научиться использовать Zend Engine (фреймворк, на котором построен язык PHP) намного легче, чем научиться писать модули ядра, поскольку сама по себе кодовая база меньше, лучше задокументирована и намного проще. Даже без хорошей документации и инструкций я выучил основы написания модулей PHP всего за один день. Если даже мне (новичку в работе с C) это удалось, то уж плохим парням и подавно», – сообщил Парис.

Разработчик опубликовал исходный код PoC-руткита на GitHub. Инструмент представляет собой 80 строк кода и легко умещается в легитимные модули. С целью обезопасить свою разработку от использования киберпреступниками Парис намеренно обезвредил некоторые его части, усложнив его компиляцию для тех, у кого нет опыта работы с модулями PHP.

(вгору)

Додаток 18

20.06.2017

В США произошел крупнейший в истории слив данных пользователей

Персональные данные 198 млн избирателей США были выложены в открытый доступ на сервере Amazon S3. Сервером пользуется аналитическая фирма-подрядчик Республиканской партии, которая собирала эти данные во время президентских выборов. Компания уверяет, что это делалось ради определения лучшего эфирного времени для политической рекламы (InternetUA).

Крупнейшая утечка в истории

Персональные данные более 198 млн американских избирателей были непреднамеренно выложены в интернет. Их обнаружили на сервере Amazon S3, занятом аналитической компанией Deep Root Analytics (DRA), которая собирает информацию для Национального комитета Республиканской партии США. Данные никак не были защищены и находились в публичном доступе, их можно было свободно скачать.

Ресурс UpGuard назвал происшествие самым крупным инцидентом такого рода, поскольку 198 млн – это почти все зарегистрированные избиратели США, которых в общей сложности около 200 млн. Утечку обнаружил аналитик UpGuard по кибер-рискам Крис Викери (Chris Vickery), он же проверил подлинность данных.

Какие именно данные утекли

Общий объем утечки составляет около 1,1 ТБ. Данные были собраны DRA и еще двумя подрядчиками Республиканской партии: аналитическими фирмами TargetPoint Consulting, Inc. и Data Trust. База содержит сведения об имени, дате рождения, домашнем адресе, телефонных номерах, партийной принадлежности каждого избирателя и подробности его регистрации. Кроме того, указана вероятная этническая и религиозная принадлежность граждан, а также их предположительные политические убеждения, смоделированные аналитиками компаний-подрядчиков.

Утекшая база состоит из десятков таблиц. Информация была собрана в ходе подготовки к президентским выборам 2016 г., после которых президентом США стал Дональд Трамп (Donald Trump), а также во время прошлых предвыборных кампаний. Последний раз данные обновлялись в январе 2017 г., примерно во время инаугурации нового президента. За каждым избирателем в базе закреплен идентификационный номер, присвоенный ему Республиканской партией во время президентских выборов 2008 г. и 2012 г. В таблице, которая посвящена выборам 2016 г., представлены не все избиратели, а только жители штатов Огайо и Флорида, играющих ключевую роль в ходе американских выборов.

Реакция компании

Алекс Ландри (Alex Lundry), со-основатель DRA, сообщил, что компания действительно занимает этот сервер Amazon S3, а также подтвердил факт

утечки. Компания готова взять на себя «полную ответственность за ситуацию». ИТ-отдел DRA уже обновил настройки доступа на сервере и установил протокол, который поможет избежать подобных инцидентов. Расследование происшествия продолжается, однако, по предварительным данным, это не хакерская атака.

DRA сообщает, что собранные ею данные использовались для того, чтобы помочь политикам выбрать лучшее время для показа их рекламных роликов по телевидению. Найденные на том же сервере данные фирмы TargetPoint должны были просто дать кандидатам в президенты представление о политических симпатиях избирателей.

Похожие инциденты

В конце 2015 г. тот же самый Крис Викери сообщил еще об одной утечке данных американских избирателей. База данных, в которой числились 191 млн граждан США, содержала их полные имена и адреса, даты рождения, номера телефонов, адреса электронной почты, данные о политических пристрастиях, ID, историю голосований с 2000 г., а также прогноз голосования избирателей на предстоящих выборах.

Эксперты возложили вину за утечку на компанию NationBuilder, разрабатывающую ПО для проведения выборов. Когда Викери и его коллегам не удалось связаться с представителями этой компании, они сообщили о проблеме в ФБР, генпрокуратуру Калифорнии и в Internet Crime Complaint Center (IC3). Позже NationBuilder заявила, что IP, на котором была опубликована база данных, не принадлежит ни ей, ни ее клиентам, однако эксперты выразили сомнение в искренности этого заявления, поскольку, по их мнению, структура базы данных и отдельные ее поля напрямую указывают на принадлежность к NationBuilder.

В апреле 2016 г. Викери обнаружил еще одну утечку такого рода – на этот раз речь шла о 87 млн мексиканских избирателей. Состав данных был практически такой же, как в американских инцидентах: имена, адреса и т. д. Информация была также обнаружена на сервере Amazon. Немногим ранее в том же 2016 г. подобный слив был допущен на Филиппинах, он затронул 70 млн избирателей.

(вгору)

Додаток 19

20.06.2017

Обнаружена новая фишинговая атака на пользователей Facebook

Специалисты компании PhishLabs рассказали о новой фишинговой кампании, затрагивающей исключительно владельцев мобильных устройств. В основном атаки направлены на пользователей Facebook, а также сервисов Apple iCloud, Comcast, Craigslist и OfferUp (InternetUA).

Новый метод базируется на том, что мобильные браузеры не полностью отображают ссылки в адресной строке. Этой недоработкой и пользуются злоумышленники, добавляя в URL дефисы и поддомены, чтобы на мобильном

устройстве ссылка выглядела настоящей. К примеру, настоящим доменом в адресе hxxp://m.facebook.com----------validate----step1.rickytaylk[dot]com/sign_in.html является rickytaylk.com, а не m.facebook.com. Так как мобильный браузер отображает лишь часть ссылки, пользователи увидят только m.facebook.com, сопровождаемый рядом дефисов.

По словам экспертов, данная атака работает только в том случае, если пользователи невнимательны. Собранные учетные данные злоумышленники используют для отправки спам-сообщений с ссылками на фишинговые сайты друзьям пользователя. Как пояснил специалист PhishLabs Крэйн Хэссолд (Crane Hassold), в основном ссылки отправляются посредством SMS-сообщений. В то время как некоторые мобильные браузеры и мессенджеры позволяют полностью просмотреть ссылку, в большинстве SMS-приложений данная функция отсутствует.

Ранее исследователи сообщили об еще одной фишинговой кампании, в рамках которой злоумышленники использовали взломанный сайт с фиктивной страницей авторизации PayPal с целью хищения учетных данных для online-банкинга и данных банковских карт пользователей.

(вгору)

Додаток 20

21.06.2017

Разработчик опубликовал инструкцию по созданию банковских Android-троянов

В декабре минувшего года эксперты в области безопасности начали фиксировать появление новых банковских Android-троянов после того, как на подпольном форуме Exploit.in появилось руководство по разработке вредоносного ПО для Android, опубликованное русскоязычным вирусописателем, использующим псевдоним Maza-in. Помимо указаний по разработке базовых версий вредоносных программ, инструкция включала исходный код трояна BankBot, а также web-узел для связи с вредоносным ПО (InternetUA).

BankBot включает значительное количество функций, в том числе возможность перекрывать окна приложений своими окнами на различных версиях Android, перехватывать SMS-сообщения и USSD (Unstructured Supplementary Service Data) коды для обхода двухфакторной аутентификации, похищать учетные данные из различных приложений, причем не только банковских.

За последнее десятилетие в Сеть неоднократно утекали исходные коды различных вредоносных семейств, на основе которых злоумышленники впоследствии разрабатывали собственные инструменты. Так произошло в случае с исходным кодом банковского трояна ZeuS, вымогательского ПО EDA2 и HiddenTear и банковского Android-трояна GM Bot, обнародованного в начале минувшего года.

Спустя всего месяц после публикации кода BankBot, специалисты компании «Доктор Веб» обнаружили первое разработанное на его основе вредоносное ПО, предназначенное для атак на российские банки.

Maza-in не только разместил инструкцию на Exploit.in, но и продолжил дополнять ее новой информацией. Более того, к инициативе присоединились и другие участники хакерского сообщества.

В частной беседе на форуме Ripper Maza-in случайно проговорился, что является создателем банковского трояна Mazar BOT, активного в 2015 - начале 2016 года. Если его слова правдивы, именно Maza-in является тем таинственным покупателем, который приобрел исходный код GM Bot на ранних стадиях разработки и на его основе создал инструмент Mazar BOT.

Первая версия трояна GM Bot появилась в продаже на подпольных форумах в октябре 2014 года. Однако в начале февраля 2016 года один из клиентов обнародовал исходный код вредоноса. В том же месяце автор трояна GanjaMan выпустил вторую версию вредоносного ПО, написанную «с нуля». Спустя некоторое время после релиза из-за ссоры с покупателем GanjaMan стал персоной нон грата на площадках, где продавал свое вредоносное ПО. На основе исходного кода разработаны такие бановские трояны, как Bankosy, Acecard, SlemBunk и Mazar BOT.

В интервью изданию Forbes Maza-in сообщил, что публикацией руководства намеревался привлечь внимание к проблеме уязвимостей в ОС Android. Но, как отмечает ресурс BleppingComputer, если бы это было действительно так, разработчик мог бы напрямую обратиться к специалистам Google, а не выражать свою «обеспокоенность» на одном из наиболее популярных хакерских форумов.

(вгору)

Додаток 21

21.06.2017

Троян Qakbot вызывает проблемы даже после удаления с компьютеров

Банковский троян Qakbot применяет новый метод атак и использует заражённые компьютеры в качестве серверов, даже когда его устраняют антивирусы. Он представляет собой червя, который способен красть логины и пароли, создавать бэкдор и скачивать дополнительное вредоносное ПО, оставаясь незамеченным (InternetUA).

Этот троян впервые стал известен в конце прошлого десятилетия, с тех пор регулярно доставляя проблемы. Теперь он научился работать даже после устранения из поражённых сетей. Специалисты из компании McAfee Labs обнаружили новую форму трояна под названием Pinkslipbot, он использует инфицированные компьютеры как HTTPS-прокси для сокрытия настоящих управляющих серверов.

Pinkslipbot собирает банковские данные при помощи кражи паролей, кейлоггеров, чаще всего страдают пользователи финансовых учреждений в

США. Программа управляет ботнетом из более чем 500 тысяч компьютеров и крадёт по полмиллиона записей в день.

Исследователи нашли ряд связанных с приложением IP-адресов, которые состоят только из заражённых компьютеров. Используются протоколы universal plug and play (UPnP) для открытия портов, давая доступ из интернета. Пока неизвестна процедура определения, подходит инфицированный компьютер для роли прокси или нет. Роль могут играть три фактора: IP-адрес из Северной Америки, высокоскоростное подключение и способность открывать порты при помощи UPnP.

После выбора подходящего компьютера автор приложения выпускает команду для скачивания библиотеки и создания компонента прокси. При запуске создаются правила переадресации портов, которые нельзя удалить автоматически, не повредив настройки сети. Эти правила действуют и после удаления трояна; McAfee выпустила инструмент для решения этой проблемы.

(вгору)

Додаток 22

22.06.2017

Microsoft признала отключение антивирусов сторонних производителей

Действия компании Microsoft на рынке антивирусов в последнее время привлекают повышенное внимание. Это способствует майская масштабная атака приложения-вымогателя WannaCry и жалоба лаборатории Касперского в антимонопольные органы Евросоюза. Российская компания обвинила Microsoft в отключении своего антивируса на Windows-компьютерах и использовании доминирующего положения для агрессивного продвижения собственного защитника Windows (InternetUA).

По этому вопросу в блоге Microsoft появилась статья. Роб Леффертс из подразделения Windows Enterprise and Security не говорит о лаборатории Касперского напрямую, вместо этого он защищает практику установки собственного антивируса в Windows. По его словам, это требуется для того, чтобы обеспечить обещанную пользователям постоянную защиту Windows 10 от вирусов и вредоносного программного обеспечения.

Также объясняется отключение сторонних антивирусов. Microsoft заявляет, что 95 % компьютеров на Windows 10 обладают совместимыми с Windows 10 Creators Update антивирусами, но небольшому количеству требуется обновление для работы с последней версией системы. Windows 10 предлагает установить новые версии антивирусов после своего обновления, но отключает старые версии в случае их несовместимости. Речь идёт о временном отключении и Microsoft говорит о совместной работе с производителями антивирусов относительно необходимых обновлений и обеспечения совместимости.

Также лаборатория Касперского обвинила Microsoft в недостаточном количестве времени для тестирования последних версий Windows 10 для обеспечения совместимости с антивирусами. В Microsoft, естественно, так не считают и упоминают программу Microsoft Virus Initiative, в рамках которой компания работает с более чем 80 независимыми производителями антивирусных приложений. В ней партнёрам предоставляются ранние сборки Windows и необходимые технические руководства. В рамках этой программы Microsoft даёт сторонним производителям более глубокий доступ к процессу разработки Windows, чем когда-либо прежде.

Теперь представителям европейских регуляторов предстоит решить, имеется ли достаточно оснований для того, чтобы начать против Microsoft антимонопольное расследование.

(вгору)

Додаток 23

21.06.2017

Эпидемия WannaCry могла произойти из-за случайной утечки

Ошибки в коде и реализации вымогательского ПО WannaCry, в мае нынешнего года заблокировавшего сотни тысяч компьютеров по всему миру, могут служить подтверждением теории о том, что авторы шифровальщика допустили утечку вредоносной программы, и ее распространение началось до того, как она была полностью завершена. Такой точки зрения придерживается эксперт в области кибербезопасности Джейк Уиллиамс (Jake Williams) (InternetUA).

Во-первых, говорит Уиллиамс, разработчики использовали всего три Bitcoin-адреса для перевода денежных средств, тогда как обычно вымогательское ПО предусматривает свой уникальный адрес на каждый случай инфицирования для эффективного отслеживания оплат. По его словам, это аматорская ошибка, так как правоохранительные органы или ИБ-эксперты могут сравнительно легко отследить все транзакции.

Во-вторых, на пререлизную версию WannaCry указывает вшитый в код «домен-выключатель», предназначенный на тот случай, если вредонос понадобится остановить. Наличие подобного механизма вполне логично, однако удивляет отсутствие какого-либо шифрования, пояснил Уиллиамс. В прошлом другие вирусописатели шифровали канал связи с управляющим сервером, тем самым предотвращая регистрацию подобного домена правоохранителями и исследователями, что, собственно, и сделал эксперт Маркус Хатчинс (Marcus Hutchins), обнаруживший «аварийный» домен в коде WannaCry.

«Авторы вредоносного ПО, включая северокорейцев, знают об этом [шифрованиии]. Идея о том, что они реализуют домен-выключатель без этого... Это версия 0.0, которая никогда не должна была распространяться. Я на 100 % уверен в этом», – подчеркнул Уиллиамс в интервью изданию Threatpost.

(вгору)

Додаток 24

27.06.2017
Описан новый метод взлома почтовых ящиков

Израильские ученые описали новый метод атаки под названием PRMitM (Password Reset Man-in-the-Middle), позволяющей инициировать сброс пароля от электронной почты пользователя при его регистрации на другом сайте. PRMitM предполагает использование методов социальной инженерии, поскольку атакующим потребуется убедить потенциальную жертву зарегистрировать учетную запись на специально созданном сайте (InternetUA).

Когда пользователь вводит свой логин или адрес электронной почты в регистрационную форму на сайте злоумышленников, ресурс отправляет эту информацию на страницы жертвы в сервисах Google, Yandex или Yahoo! для инициализации процесса сброса пароля. В случае, если сервис запрашивает выполнение дополнительных действий, например, ввода CAPTCHA, ответа на секретные вопросы или ввода кода верификации, отправленного в SMS-сообщении, атакующий дополняет форму регистрации соответствующими пунктами.

PRMitM эффективна только против учетных записей в сервисах электронной почты. Как пояснили эксперты, большинство web-сайтов отправляют ссылки для сброса пароля в электронных письмах, тогда как сервисы электронной почты используют другие методы, такие как уже упоминавшиеся тесты CAPTCHA, ответы на секретные вопросы и коды верификации.

Успешность атаки в основном зависит от внимательности пользователей, отмечают исследователи. К примеру, в ходе тестирования нового метода многие пользователи вносили в форму регистрации все требуемые сведения даже не подозревая, что кто-то пытается взломать их учетную запись. Более того, при получении SMS-сообщений с кодом верификации большинство пользователей даже не удосужились прочитать уведомление полностью, что могло бы предотвратить взлом аккаунта. Некоторые сервисы, такие как Twitter или Facebook, указывают в SMS-сообщениях, для каких целей предназначен код (для сброса пароля, регистрации и т.д.).

Для противодействия подобным атакам в будущем исследователи рекомендуют сервисам предпринять ряд мер, в том числе отправлять ссылки для сброса паролей в SMS-сообщениях, если они не практикуют отправку таких ссылок в электронных письмах. Получив подобное сообщение при регистрации на другом сайте, пользователь поймет, что происходит нечто подозрительное, уверены исследователи.

(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.