СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(12.07–25.07)

2017 № 13

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(12.07–25.07)
№ 13

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

17.07.2017
В Skype под натиском пользователей вернули старые функции

В начале прошлого месяца компания Microsoft объявила о полном редизайне Skype. В популярный сервис обмена сообщения были добавлены функции из других мессенджеров, таких как Snapchat и Messenger.

Докладніше

***

17.07.2017
Facebook ввел возможность создания GIF-анимаций в приложении

В приложении соцсети Facebook появилась новая функция, которая дает возможность создавать GIF-анимации прямо внутри сервиса, сообщает vc.ru (Телекритика).

Для того чтобы воспользоваться нововведением, необходимо после запуска камеры в приложении свайпнуть (провести пальцем) вправо. На анимации можно накладывать те же эффекты и рамки, что и на обычные фотографии.

Созданные GIF-анимации можно опубликовать на своей странице и в «Историях», а также сохранить на устройстве, но лишь в формате видео.

Пока нововведение доступно лишь для владельцев iOS. Когда новая функция появится на Android, в компании не говорят.

***

18.07.2017
«Одноклассники» обзавелись счетчиком просмотров

Социальная сеть «Одноклассники» обзавелась счетчиком просмотров публикаций. Теперь под каждым постом различных сообществ, кроме «классов» и репостов, будут также указаны и его просмотры (HiTech-News.ru).

Счетчик будет доступен только автору публикации, сообщают разработчики функции. При этом система оборудована специальным алгоритмом, который позволяет избегать учета множественных просмотров и «накручивания». Функция доступна только для браузеров на ПК, но учитываются также все данные с мобильных устройств, в том числе и из официальных приложений. Позже функцию перенесут на все остальные платформы.

Функция будет полезна для руководителей пабликов, которым будут доступны данные по посещаемости группы, а также качеству предоставляемого контента.

В марте 2017 года подобную функцию показала социальная сеть «ВКонтакте».

***

18.07.2017

У социальной сети LinkedIn появился клиент для Windows 10

У профессиональной социальной сети LinkedIn появилось приложение для Windows 10. В нём доступны многие функции, которые присутствуют в мобильных приложениях сервиса и настольной версии сайта. Среди них – приём сообщений и приглашений от других пользователей в реальном времени.

Докладніше

***

19.07.2017

WhatsApp тестирует поддержку видео YouTube внутри приложения

Разработчики WhatsApp в настоящий момент тестируют возможность просмотра видео YouTube прямо в окне для обмена сообщениями. Другими словами, с необходимостью открывать приложение YouTube для просмотра видео может быть скоро покончено (InternetUA).

Видео воспроизводится во встроенном окне по принципу «картинка в картинке». При этом доступны функции масштабирования и перехода в полноэкранный режим. Кроме того, можно скрыть окно воспроизведения, вернувшись к общению. Воспроизведение также автоматически останавливается, если перейти к диалогу с другим собеседником.

Пока описанная функциональность доступна в iOS на смартфонах iPhone 6 и новее. Про версии для Android и Windows Phone информации нет.

***

19.07.2017

Facebook запретит менять заголовки, тексты и картинки в сниппетах ссылок

Социальная сеть запретит менять заголовки, тексты и картинки в сниппетах, которые автоматически загружаются с сайта. Функцию уже убрали в Power Editor, теперь могут отключить и в обычном интерфейсе, отмечает cossa.ru. Таким образом соцсеть борется с фейковыми новостями (Marketing Media Review).

Параллельно Facebook запускает инструмент Link Ownership в разделе «Публикации страницы». С помощью него можно кастомизировать картинки и тексты по умолчанию в сниппетах для ссылок с сайта компании. Пока новый инструмент доступен только для страниц медиа, но до 12 сентября соцсеть введёт его для всех.

Страницы, которые будут злоупотреблять изменением своих ссылок (искажать содержимое ссылки, спамить пользователей своими постами), потеряют возможность использования Link Ownership.

Соцсеть также отказывается от постов с видео и кнопкой призыва к действию. Подобные публикации Facebook обещает удалить к 26 июля 2017 года. Теперь они будут доступны только как реклама.

***

20.07.2017
Пошибайло Вадим
Amazon запустила собственную соцсеть для шопинга Spark

Пользователи приложения Amazon смогли познакомиться с новой социальной сетью для шопинга Amazon Spark. Ресурс запустили совсем недавно, но он уже набирает популярность (HiTech-News.ru).

Новая сеть помогает людям обмениваться впечатлениями о своих покупках. Каждый товар, который люди размещают в Spark, можно оценивать и оставлять под ним комментарии. Самые активные покупатели, которые публикуют много отзывов и обзоров на своем канале, получат специальный значок. Как считают разработчики, Amazon Spark призвана улучшить качество и количество отзывов и получить новые фотографии товаров лучшего качества.

После прохождения регистрации в Spark пользователю предлагается пройти опрос, в ходе которого выясняется, каковы потребности у конкретного человека. Это нужно для того, чтобы приложение показывало только необходимые и интересные товары в новостной ленте.

В данный момент приложение доступно жителям США и поддерживается на операционной системе iOS.

***

19.07.2017
Павел Красномовец
Владелец «Киевстар» запускает в Украине мессенджер с бесплатными сообщениями, звонками и новостями

Материнский холдинг «Киевстар» Veon (ранее Vimpelcom) объявил о запуске «персональной интернет-платформы» в Украине, Грузии, России и Пакистане. Приложение VEON должно стать «единой цифровой точкой входа» для абонентов. Трафик в нем для абонентов сети не будет тарифицироваться и абоненты смогут использовать его даже при нулевом балансе, утверждаютв Veon. В пресс-службе «Киевстар» подтвердили AIN.UA, что трафик для приложения уже не учитывается в счете (AIN.UA).

Докладніше

***

25.07.2017

В YouTube уберут важную функцию // Функция перестанет быть доступной в связи с низким спросом на нее

Видеохостинг YouTube откажется от функции редактирования видео, о чем сообщается в официальном пресс-релизе компании. Ожидается, что функция перестанет быть доступной с 20 сентября этого года, передает Mashable.

Сообщается, что вместе с функцией редактирования также будет закрыта функции Photo slideshows (InternetUA).

«Мы видим слабый интерес к этим функциям, поэтому решили отправить их на пенсию, чтобы сконцентрировать наши силы на более популярных продуктах», – отмечено в официальном сообщении.

Однако определенное время разработчики оставили пользователям для того, чтобы они закончили уже начатые проекта.

Известно также, что YouTube имеет собственный сервис для редактирования под названием Video Editor, в котором нет спецэффектов. Однако в нем пользователи могут смонтировать любое простое видео.

***

24.07.2017

У Telegram з'явилися фото та відео, які самознищуються

Користувачі месенджера зможуть в особистому листуванні обмінюватися повідомленнями з фото і відео, які самознищуються (Espreso.tv). Про це повідомляється на офіційному блозі сервіса.

Відправник встановлює час, протягом якого фото або відео буде доступне одержувачу, після матеріал буде безповоротно видалено. Якщо ж одержувач зробить скріншот такого контенту, то система повідомить про це відправника.

Також в месенджері з'явилася можливість додати більше особистої інформації в профіль.

Окрім того, Telegram використовуватиме CDN-мережу для кешування файлів, що передаються у публічних чатах і каналах, що істотно збільшить швидкість завантаження на пристроях. В особистих і секретних чатах ці мережі використовуватися не будуть, їх пристосують тільки для зберігання загальнодоступних файлів, оприлюднених на каналах з аудиторією понад 100 тис. осіб.

Йдеться про використання вузлів CDN, що належать сторонньої компанії, на території різних держав світу, де користується популярністю Telegram, але в яких компанія «з різних причин» не готова розміщувати свої сервери.

***

25.07.2017

На страницах в Facebook теперь можно создавать группы по интересам

Пользователям Facebook стала доступна функция Groups for Pages, которая позволяет авторам страниц создавать на них подгруппы. В них люди могут переписываться друг с другом и с владельцами страниц. Крис Кокс (Chris Cox), главный руководитель по продукту, сравнил подгруппы с фан-клубами.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

18.07.2017

#МАЮПРАВОСКАЗАТИНІ: українки розповідають про своє право на вибір

До флешмобу долучилися відомі політикині, артистки і активістки (ELLE).

Українські жінки завжди були настільки сильними, що могли навіть відмовити чоловікові, який до неї сватався. Хоча в інших країнах світу цього бути не могло. На знак відмови українська дівчина виносила парубкові гарбуза. Відтоді гарбуз став етнічним символом права на відмову, яке українки зберегли до сьогодні у різних сферах свого життя: особистому, професійному, соціальному й релігійному.

Аби нагадати про це у соцмережах стартував новий флешмоб #маюправосказатині, який закликає жінок розказати історії з власного життя про те, як вони казали НІ чоловікам, керівникам або просто відмовлялися від пропозицій, які не відповідали цінностям та цілям. Цей флешмоб ініціювала Олеся Жулинська. До неї уже долучилося багато жінок з усієї країни.

***

16.07.2017

Литовці почали флешмоб у соцмережі «Кремль, ти не перепишеш нашу історію»

Жителі Литви влаштували на сторінці МЗС РФ у Facebook флешмоб, масово залишаючи коментарі під заявою міністерства закордонних справ Росії, у якій партизан балтійських країн називають злочинцями (Високий замок).

Про це повідомляє Delfi.

Ініціатор акції журналіст Андрюс Тапінас на своїй сторінці закликав литовців залишити під інформацією про нібито злочини балтійських партизанів – «лісових братів» – запис із хештегом #Кремльнашуисториюнеперепишешь.

«Якщо МЗС РФ на своїй офіційній сторінці може поливати нас брудом, ми на це можемо відповісти», – написав журналіст.

16 липня вранці на сторінці МЗС РФ було залишено більше 10 тисяч таких повідомлень під англомовною версією посту.

«Кремль, ти не сфальсифікуєш нашу історію, незважаючи на те, скільки тролів є на твоїй фабриці», «Брехня ніколи не здолає правду», «Ви не перепишете нашу історію, розкажіть росіянам правду про радянські убивства», – пишуть користувачі у коментарях.

***

18.07.2017

NBC: половина американцев считает активность Трампа в Twitter опасной

Большинство американцев не одобряет сообщения, которые глава государства Дональд Трамп публикует на своей личной странице в Twitter, и в целом считают, что хозяин Белого дома ведет себя не по-президентски. Об этом свидетельствуют результаты опроса телеканала NBC, опубликованные 17 июля.

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

12.07.2017

Павел Красномовец

Facebook начал глобальное тестирование рекламы в Messenger

Messenger – третий по популярности продукт Facebook после самой соцсети и WhatsApp. Компания стремится монетизировать его 1,2-миллиардную аудиторию. Поэтому после «многообещающих результатов в Австралии и Тайланде», бета-тестирование рекламных объявлений расширили для брендов по всему миру, говорится в официальном блоге сервиса.

Докладніше

***

17.07.2017

Amazon может запустить собственный мессенджер

Компания Amazon готовит к запуску собственный мессенджер для мобильных устройств и ПК. Об этом сообщил ресурс AFTVnews, утверждая, что Amazon начала опрашивать пользователей относительно нового сервиса обмена сообщениями, выясняя, какие функции наиболее важны для них (InternetUA).

По данным источника, мессенджер называется Anytime, он будет доступен в версиях для ПК, iOS и Android. Среди возможностей – шифрование, голосовые и видеозвонки, стикеры и так далее. Как ожидается, одной из изюминок должна стать функция легкого входа и присоединения к групповым чатам.

***

17.07.2017
Основатель Facebook за неделю разбогател на 3,5 млрд долларов

С начала 2017 года акции Facebook выросли в цене почти на 40 % и продолжают дорожать на фоне оптимистичных прогнозов аналитиков в отношении квартальных результатов крупнейшей в мире соцсети, которые будут объявлены в конце июля. Благодаря этому подъему основатель и глава Facebook Марк Цукерберг (Mark Zuckerberg) только за последнюю неделю стал богаче на 3,5 млрд долларов, сообщает Forbes (InternetUA).

По данным издания, являясь председателем правления и генеральным директором Facebook, Цукерберг владеет примерно 17 % акций соцсети, стоимость которых на днях достигла рекордного показателя в 66,7 млрд долларов. Это больше, чем состояние главы Oracle Ларри Эллисона (Larry Ellison), которое оценивается Forbes в 61,4 млрд долларов, отмечает The Hill.

В рейтинге Forbes, включающем богатейших людей планеты, Цукерберг занимает шестое место, а в списке 50 мировых миллиардеров он единственный человек в возрасте 30 с небольшим лет, говорится в публикации.

***

20.07.2017
Українці тепер можуть здійснювати грошові перекази через Facebook

Компанія LeoGaming в партнерстві з Mastercard запустили LeoBot – платіжного бота в соціальній мережі Facebook з інтегрованою платформою цифрових гаманців Masterpass. Він дозволяє здійснювати грошові перекази між картковими рахунками українських банків з мобільного пристрою в один клік. Проект реалізований за технічної підтримки TAS Link і платформи UniBot.

Докладніше

***

21.07.2017
Олег Дмитренко
Facebook хоче зробити платним доступ до контенту ЗМІ

Соціальна мережа почала розглядати можливість введення платної підписки після скандалу з великою кількістю фейковий новин у Facebook під

час президентської передвиборної кампанії 2016 року – про це повідомила керівник Facebook з медіа-партнерств Кемпбелл Браун (Watcher).

«Це одне з тих прохань, які ми чули з боку багатьох газет та інтернет-видань, воно полягає в тому, що вони хочуть отримати платний продукт і отримати платний сервіс в межах Facebook, – сказала Браун на галузевій конференції Digital Publishing Innovation Summit. – І зараз ми це робимо. Ми запускаємо продукт за передплатою».

У минулому році Facebook і Google заробили $73 млрд на продажі реклами в інтернеті, це 70 % всього ринку реклами США. Доходи американських видавців від продажу реклами в минулому році склали лише $18 млрд. Американські видавці стурбовані, що доходи інтернет-компаній ростуть в тому числі за рахунок контенту традиційних ЗМІ.

Американський Альянс новинних медіа звернувся до конгресу США з проханням надати видавцям право вести колективні переговори з інтернет-індустрією. Антимонопольне законодавство США обмежує можливості подібних пактів.

Facebook не проти об'єднання видавців, але вважає за краще працювати з видавцями в індивідуальному порядку, сказала Браун.

***

24.07.2017

Facebook розробляє смартфон з легкозамінними елементами

Компанія Facebook працює над розробкою модульного смартфону і подала на нього патентну заявку (Espreso.tv).

Про це повідомляється у тексті заявки.

Патент стосується «модульного електромеханічного пристрою», в якому буде мікрофон, динамік, GPS, сенсорний дисплей. Пристрій зможе працювати як телефон, повідомляє видання Business Insider.

Модульна система нового пристрою дозволить користувачам заміняти його застарілі компоненти на більш нові.

Повідомляється, що спеціалісти Facebook зосереджені на технології машинного навчання та розробці модулів камери.

Раніше над схожим проектом – модульним телефоном Project Ara працювали співробітники Google. Проте в минулому році проект закрили. Повідомляється, що декілька співробітників компанії Google продовжили працювати над своїми розробками вже в Facebook.

***

25.07.2017

Цена рекламы в Facebook и Google к октябрю может увеличиться в два раза

Дарина Шварцман

Директор по развитию агентства эффективного интернет-маркетинга WebPromo Антон Воронюк детально рассказал InternetUA о том, как изменили рекламный рынок блокировки российских интернет-ресурсов.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

16.07.2017

Прокидається з відчуттям обов'язку зробити фото в Instagram

У чому причина постійної потреби людей фіксувати кожен свій крок і повідомляти про це в соцмережі, пояснює психолог Галина Синоруб.

Докладніше

***

17.07.2017

Facebook определил самый популярный эмодзи

В Международный день эмодзи Facebook определил, какие эмодзи пользователи используют чаще всего. Самым популярным стикером за последние 30 дней оказался плачущий от смеха смайлик, второе место занял эмодзи с глазами в форме сердец, на третьем месте – «поцелуй».

Докладніше

Маніпулятивні технології

13.07.2017

США підозрюють Україну у втручанні в вибори. У ФБР хочуть розслідування

У США почали підозрювати, що Україна втручалася в американські президентські вибори минулого року. Про це почали говорити 12 липня, коли кандидат на посаду керівника ФБР Крістофер Рей брав участь у слуханнях Сенату щодо призначення нового очільника Бюро.

Докладніше

***

18.07.2017

Дарина Шварцман

Правительства манипулируют общественным мнением с помощью Twitter и Facebook

Во всем мире правительства привлекают «кибервойска» для манипуляции общественным мнением в социальных сетях, в частности Twitter и Facebook. Об этом говорится в докладе Оксфордского университета, сообщает Bloomberg.

Докладніше

***

18.07.2017

Люди могут определить фейковые фото только в 60 % случаев

Лишь в 60 % случаев люди могут идентифицировать фото-подделку и только в 45 % объяснить, что именно не так с изображением. Таковы результаты исследования ученых из Университета Уорвика в Великобритании, опубликованного в журнале Cognitive Research: Principles and Implications, сообщает Indicator.ru (Телекритика).

Авторы исследования создали онлайн-тест, в котором были представлены 40 изображений. 10 из них были оригинальными, а оставшиеся 30 – изменены в разной степени. В тесте приняли участие 707 человек, каждому из них показывали по 10 случайных изображений, из которых пять никак не видоизменялись, а остальные были обработаны в программе. Участники ни разу не видели две формы одного изображения (исходную и обработанную) дважды.

Так, 60 % обработанных в фоторедакторе снимков участники идентифицировали верно. Когда экспериментаторы спрашивали у них, что именно не так с фото, лишь 45 % смогли назвать причину.

В другом эксперименте принимали участие 659 человек: они проходили онлайн-тест, в котором не сообщалось, есть ли среди фотографий видоизмененные. Как результат – 65 % респондентов выявили отредактированные снимки, но поиск изменений занял у них на 39 % времени больше, чем ожидали исследователи.

Спецслужби і технології «соціального контролю»

13.07.2017

Ольга Мінченко

Інтернет Асоціація України вважає, що в українському Інтернеті планують ввести цензуру

Впродовж тижня здійснюється уже друга спроба включити до порядку денного сесії Верховної Ради України проект Закону України щодо протидії загрозам національній безпеці в інформаційній сфері (№6676 та №6688). Ці

Законопроекти є фактично тотожними і їх розгляд відбувається з грубим порушенням Регламенту ВР – вважають в Інтернет Асоціації України (ІнАУ). А при їх підготовці були проігноровані пропозиції експертного середовища.

Докладніше

***

13.07.2017

На пользователей «ВКонтакте» и «Одноклассники» СБУ открыла 34 уголовных дела

Как сообщили в пресс-службе силового ведомства, сотрудники Службы безопасности Украины охотятся за создателями и администраторами сепаратистских и пропагандистских сообществ в российский социальных сетях «ВКонтакте» и «Одноклассники» (InternetUA).

В основном, сотрудники СБУ серьезно взялись за администраторов сообществ, которые призывают к государственному перевороту и сепаратизму. А это, как известно, в Украине незаконно и предусматривает криминальную ответственность.

По данным пресс-службы силовой структуры, с начала текущего года правоохранители и Служба безопасности Украины открыли 34 уголовных производства против таких лиц. Более того, 27 человек уже получили сообщение о подозрении.

Также сообщается, что суд вынес 27 приговоров за насильственное изменение или свержение конституционного строя и захвата государственной власти, посягательство на территориальную целостность Украины и создание террористической группы.

В ведомстве отчитались, что Служба безопасности Украины уже заблокировала деятельность около десятка пророссийский сайтов, которые якобы использовались страной-агрессором для дестабилизации ситуации в Украине.

***

17.07.2017

У Комітеті розпочала роботу місія експертів ЄС із законодавчого регулювання питань кібербезпеки

У Комітеті з питань інформатизації та зв’язку розпочала роботу експертна група ЄС із законодавчого регулювання питань кібербезпеки. Перший установчий візит експертної групи ЄС, до складу якої входять представники Естонії, Словаччини, та Польщі, відбувся 11-12 липня 2017 р., в ході якого було здійснено вивчення стану законодавчого регулювання питання кібербезпеки в Україні, готовності основних законопроектів з реформування галузі ІКТ підготовлених до розгляду у Комітеті з питань інформатизації та зв’язку (Комітет з питань інформатизації та інформаційних технологій).

Експертна група ЄС презентувала моделі законодавчого регулювання питання кібезбезпеки у Естонії, Словаччини, та Польщі для вибору найкращої моделі для імплементації в Україні.

За результатами роботи експертної групи передбачається підготовка програми технічного допомоги у 2017-2018 роках Верховній Раді Україні, зокрема Комітету з питань інформатизації та зв'язку, з метою подальшого напрацювання найкращих практик та політик з кібербезпеки на основі досвіду країн ЄС.

***

17.07.2017

На Хмельниччині чоловік для привернення уваги бойовиків створив сепаратистську групу

Співробітники СБУ затримали на Хмельниччині адміністратора сепаратистської групи «Хмельницька народна республіка» у «ВКонтакті» Як повідомила 17 липня прес-служба СБУ, затриманий пояснив, що створив групу для того, аби вийти на зв'язок із бойовиками «ДНР» (InternetUA).

«Мешканець Хмельницької області, раніше неодноразово засуджений, мав намір приєднатися до бойовиків на території ОРДЛО. Аби привернути до себе увагу ватажків незаконних збройних формувань, він створив віртуальний сепаратистський проект у соціальній мережі», – йдеться у повідомленні СБУ.

На оприлюдненому СБУ відео сам затриманий пояснює, що із ним зв'язався невідомий чоловік і представився членом хакерського угрупування «Кіберберкут».

«Я створив в інтернеті групу «Хмельницька народна республіка» для того, аби вийти на зв'язок із "ДНР". Оскільки я знайшов в інтернеті сайт їх військкомату, але не міг туди додзвонитися, то вирішив, що створю цю групу, аби на них вийти. За час існування цієї групи зі мною зв'язався чоловік під псевдонімом «Призрак Иванович» і представився працівником "Кіберберкуту". Він пояснив, що оскільки живе у Росії, то має можливість налагодити мені зв'язок із "ДНР"», – розповів затриманий.

***

19.07.2017

Домбровский Сергей

В КНР частично заблокировали WhatsApp

В КНР частично заблокировали WhatsApp. Ограничительные меры ввели 18 июня, сведения об этом сообщает New York Times. Теперь пользователи не могут передавать друг другу звуковую и видеоинформацию. Некоторые пожаловались на невозможность послать даже текстовое сообщение (HiTech-News.ru).

Жители Китая не проявляли особого интереса к мессенджеру WhatsApp. Они чаще пользуются WeChat. Однако WhatsApp является мессенджером с возможностью шифровки данных. Именно эта функция спровоцировала ограничение. Китайские чиновники попытались поднять себе рейтинг в глазах руководителей страны, принимая такое решение, – полагают эксперты.

Сейчас неизвестно коснется ограничение исключительно WhatsApp или затронет другие мессенджеры, способные шифровать информацию. Также не понятно, заблокируют WhatsApp в Китае полностью или все останется на нынешнем уровне. Чиновники КНР стараются проявить себя перед съездом Коммунистической партии, – считают некоторые пользователи.

***

18.07.2017

У Росії засудили до 3 років творця «Синього кита»

Районний суд Тобольська Тюменської області РФ ухвалив вирок адміністраторові «груп смерті» в соцмережі «ВКонтакте» Пилипу Будейкіну, відомому за псевдонімом Філіп Лис (Espreso.tv).

Про це передають російські ЗМІ.

Відзначається, що суд засудив Будейкіна до трьох років і чотирьох місяців позбавлення волі з відбуттям покарання в колонії-поселенні.

Раніше повідомлялося, що ГСУ Слідчого комітету Росії по Санкт-Петербургу завершило розслідування кримінальної справи щодо Будейкіна.

Було встановлено, що він схиляв до суїциду 15-річну мешканку Астрахані, проте правоохоронці переконали школярку відмовитися від самогубства. Також за даними слідства, зловмисник довів до самогубства школярку 2000 року народження з Тюменської області. Її життя вдалося врятувати.

***

18.07.2017

Студентів КПІ зобов'язали видалити групи в «Одноклассниках» і «ВКонтакте»

Деканат Національного технічного університету «Київський політехнічний інститут імені Ігоря Сікорського» розіслав студентам листи, в яких рекомендує їм видалити групи в російських соціальних мережах «ВКонтакте» і «Одноклассники». Про це повідомляє Hromadske.UA (InternetUA).

Як наголошується у документі, відповідне рішення ухвалили на вимогу кіберполіції.

«Згідно з листом із Департаменту кіберполіції Національної поліції України звертаємося до вас з проханням видалити офіційні сторінки груп на

ресурсах “Вконтакте” і “Одноклассники”. У разі неможливості видалення надішліть логін і пароль», – йдеться в повідомленні.

***

20.07.2017

WikiLeaks сообщил о секретных документах ЦРУ с анализом хакерских атак

Известный сайт WikiLeaks опубликовал новые данные о секретных документах ЦРУ. Теперь пользователи могут ознакомиться, каким образом разведка США изучает кибератаки (HiTech-News.ru).

Ранее подрядная компания Raytheon Blackbird Technologies предоставила агентам ЦРУ ряд отчетов о деятельности хакеров. Организация составила для работников управления рекомендации по разработке личных вирусных приложений, а также по изучению имеющихся.

Как сообщается, документы содержат доказательства механизмов работы и оценки нападения вредоносных программ. WikiLeaks провело свое расследование частично на платформе общедоступных данных. Все бумаги говорят о том, что отдельные специалисты занимались проведением мониторинга Сети и искали новые вирусы. Обнаружив полезные, они определяли, какие могут быть полезными, позже применяв их в своих целях. WikiLeaks собирается вскоре обнародовать дополнительную партию секретных документов, но тема их пока не называется.

***

24.07.2017

У російських військових забирають документи перед поїздкою на Донбас, – розвідка // Зокрема їх змушують видаляти сторінки в соцмережах

Російське командування продовжує вживати заходів для приховування участі громадян РФ в бойових діях на окупованій території сходу України (iPress.ua).

«У з’єднаннях та частинах 1, 2 АК триває реалізація заходів з приховування участі громадян РФ в бойових діях на окупованій території сходу України шляхом вилучення у них особистих документів (паспортів і військових квитків). Встановлено, що ці заходи проводяться відповідно до розпорядження Генерального штабу ВС РФ і контролюються співробітниками ФСБ РФ. Крім того, російських військовослужбовців змушують видаляти особисті сторінки в соціальних мережах», – йдеться у зведенні ГУР (станом на 24 липня) в понеділок на сторінці у Facebook.

Розвідка також інформує, що серед особового складу російських окупаційних військ зафіксовано чергові випадки небойових втрат і суїцидів через знущання російських офіцерів і доведення підлеглих до самогубства. Так, 23 липня військовослужбовець одного з підрозділів 7-ої окремої мотострілкової

бригади (Брянка) 2 АК (Луганськ) ЗС РФ наклав на себе руки з особистої зброї. У той же час командування подає подібні небойові втрати як загибель на передовій позиції під час виконання бойових завдань.

Проблема захисту даних. DDOS та вірусні атаки

12.07.2017

В Android обнаружили скрытый «режим паники» для борьбы с вирусами

Пользователи Android регулярно оказываются в опасности из-за разных вредоносных приложений. Совершенно неожиданно разработчики с популярного сайта XDA выяснили, что в последних версиях Android компания Google добавила скрытый «режим паники» для борьбы с вредоносными приложениями.

Докладніше

***

12.07.2017

Twitter и WhatsApp плохо защищают данные пользователей: EFF

Компании Adobe, Dropbox, Pinterest, Uber и WordPress являются самыми надежными digital-игроками. Об этом говорится в ежегодном отчете о защите приватности пользователей интернет-компаний некоммерческой правозащитной организации Electronic Frontier Foundation (EFF), созданной для защиты прав людей в цифровом пространстве,сообщает Cossa (Телекритика).

Эксперты оценивали открытые данные 26 крупных интернет-компаний по пяти направлениям: прописанные правила взаимодействия компании с государством; публикация отчетов о запросах госорганов; запрет на передачу личных данных третьим лицам; проверка секретных запросов правительства США на легальность; борьба за изменения в законе о негласном наблюдении в целях внешней разведки.

За соблюдение каждого критерия компания получала одну звезду.

По четыре звезды заработали Facebook, Google, LinkedIn и Microsoft, которые «посыпались» на пункте о проверке секретных правительственных запросов. Apple же не получила высший балл из-за того, что публично не борется против закона о негласном наблюдении.

По три звезды получили Airbnb, Twitter, Tumblr, а WhatsApp заработала лишь две. По одной – у американских мобильных операторов T-Mobile и Verizon.

***

12.07.2017

Новый троян напал на WhatsApp, Skype, Viber и Telegram. Под угрозой полмиллиарда смартфонов

Программа SpyDealer способна перехватывать SMS, звонки, делать снимки со встроенных камер и собирает личные данные о пользователях зараженных устройств. Судя по всему, это шпионский инструмент узконаправленного действия.

Докладніше

***

12.07.2017

Эксперты раскрыли подробности о кибератаках на электростанции в США

В СМИ появилась информация о расследовании кибератак на энергетический и ядерный секторы США, в осуществлении которых подозревается Россия. Ажиотаж возник после того, как Министерство внутренней безопасности США и ФБР разослали энергетическим компаниям предупреждения об активизировавшейся хакерской активности. Главным подозреваемым в атаках является группировка Energetic Bear, также известная под названиями Dragonfly и Crouching Yeti.

Докладніше

***

12.07.2017

Белый дом ограничил закупку продуктов «Лаборатории Касперского» для госструктур

Администрация президента США убрала «Лабораторию Касперского» из двух списков разрешенных поставщиков программного обеспечения для правительственных агентств. Об этом сообщает Reuters со ссылкой на Администрацию общих служб США (InternetUA).

Продукты российской компании удалены из списков, разрешенных для осуществления контрактов, касающихся информационных технологий и цифрового фотооборудования. По словам представителя американского ведомства, решение принято после «тщательного рассмотрения» вопроса.

Американские власти опасаются, что «Лаборатория Касперского» может быть тесно связанно с российскими разведывательными службами.

Однако отмечается, что другие подразделения, не связанные с работой Администрации общих служб, смогут продолжить использовать ПО российской компании.

***

12.07.2017

Новая версия банковского трояна для Windows атакует пользователей Mac

Специалисты компании Trend Micro обнаружили новое вредоносное ПО, ориентированное на пользователей компьютеров Apple. Вредонос, получивший название OSX_DOK, представляет собой модифицированную версию банковского трояна Werdlod, разработанного для систем на базе Windows. Преимущественно OSX_DOK атакует клиентов швейцарских банков.

Докладніше

***

12.07.2017

Adwind атакует предприятия аэрокосмической промышленности

Исследователи компании Trend Micro рассказали о новой спам-кампании по распространению кроссплатформенного вредоносного ПО Adwind. Программа представляет собой написанный на Java троян для удаленного доступа (RAT). Вредонос находится в разработке с 2013 года и недавно снова напомнил о себе. На этот раз Adwind атакует предприятия аэрокосмической отрасли преимущественно в Швейцарии, Австрии, Украине и США (InternetUA).

Другие названия трояна – AlienSpy, Frutas, Unrecom, Sockrat, JSocket и jRat. Adwind атакует устройства, работающие под управлением Windows, Mac, дистрибутивов Linux и мобильной ОС Android. Вредонос способен похищать учетные данные, записывать нажатия клавиш на клавиатуре, делать скриншоты, а также собирать данные. Кроме того, троян способен сделать зараженную систему частью ботнета для осуществления DDoS-атак.

Исследователи Trend Micro зафиксировали всплеск числа атак с использованием Adwind в июне текущего года – 117 649 заражений (на 107 % больше, чем в мае). В частности были зафиксированы две отдельные кампании – 7 и 14 июня.

***

12.07.2017

Хакеры использовали серверы итальянского банка для майнинга криптовалюты

Серверы одного из итальянских банков использовались хакерами для добычи криптовалюты. Об этом рассказал директор компании Darktrace Дэйв Палмер (Dave Palmer) в рамках выступления на прошедшей в Лондоне конференции Research and Applied AI Summit.

Докладніше

***

12.07.2017

«Хакерский» сканер для поиска уязвимостей доступен в даркнете за $500

На одном из хакерских форумов продается полностью автоматизированный сканер для поиска уязвимостей, позволяющих внедрить SQL-код. Инструмент Katyusha Scanner стоимостью $500 может осуществлять массовое сканирование на предмет наличия уязвимостей и управляется посредством смартфона через мессенджер Telegram (InternetUA).

Сканер, созданный русскоязычным разработчиком, был обнаружен исследователями из компании Recorded Future. Katyusha Scanner представляет собой гибрид классического сканера для поиска SQLi (SQL injection)-уязвимостей и открытого инструмента для проведения тестов на проникновение Anarchi Scanner.

Предложение о продаже Katyusha Scanner появилось на форуме в апреле нынешнего года. Инструмент приобрел настолько высокую популярность, что месяц спустя разработчик «Катюши» выпустил «бюджетную» версию ПО стоимостью $250 для тех, кто не может заплатить $500 за полный пакет. В июне автор запустил сервис, предлагающий доступ к Katyusha Scanner всего за $200 в месяц.

По словам эксперта Recorded Future Андрея Барисевича, Katyusha Scanner обладает широким набором функциональных возможностей. К примеру, злоумышленники могут загрузить список с интересующими их web-сайтами и провести параллельные атаки на несколько объектов, управляя операцией через мессенджер Telegram. При обнаружении уязвимости на сайте инструмент способен проэксплуатировать проблему, внедрить вредоносный скрипт, загрузить различные типы файлов, автоматически сделать дамп базы данных и пр.

***

12.07.2017

Ольга Карпенко

Новый вирус на Android угрожает разослать по контактам фото и переписку со смартфона

Специалисты по безопасности из компании McAfee обнаружили новый тип вируса, который угрожает мобильным устройствам на базе операционной системы Android. Это – вирус-вымогатель (ransomware), но он работает не совсем традиционными методами. Вместо того, чтобы зашифровывать пользовательские файлы и требовать выкуп за ключ разблокировки, он угрожает разослать личные данные со смартфона по всему контакт-списку пользователя (AIN.UA).

Вирус обнаружили в Google Play, он называется LeakerLocker. На данный момент эту угрозу содержат два приложения – Wallpapers Blur HD и Booster &

Cleaner Pro, их уже успели скачать тысячи пользователей. Если смартфон им заражен, экран будет заблокирован, а пользователю покажут такое сообщение:

В нем авторы вируса сообщают, что у пользователя 72 часа, чтобы заплатить выкуп. Если требование не будет выполнено, история браузера, фото, переписка в Facebook, история звонков, SMS и полные тексты почтовой переписки будут разосланы по всем контактам. То, что вирус получает доступ к таким чувствительным данным, можно заметить в перечне скриптов, который приводят в пример эксперты из McAfee:

Если пользователь платит выкуп, ему сообщают, что его данные были удалены с сервера.

В компании уже сообщили о проблеме в Google, там ответили, что исследуют вопрос.

***

12.07.2017

Google прорекламировал лучшие сайты для просмотра пиратских фильмов

Американская версия поисковой системы Google по ошибке прорекламировала лучшие торрент-трекеры для скачивания пиратских фильмов и телешоу. Об этом сообщает TorrentFreak (InternetUA).

Если набрать в поисковой строке запрос «лучшие торрент-сайты», Google выдаст список с логотипами и ссылками на пять самых популярных пиратских стриминговых сервисов, в том числе The Pirate Bay и Torrent Project. На них можно не только загрузить популярные фильмы, сериалы и ТВ-шоу, но и посмотреть их онлайн.

***

12.07.2017

Поліція відкрила 909 карних справ після кібератак на державні та приватні установи України

Правоохоронні органи отримали 1415 заяв та повідомлень щодо блокування роботи комп'ютерної техніки за допомогою вірусу-шифрувальника (InternetUA).

Національна поліція України відкрила 909 карних справ за фактами кібератак, внісши відомості до Єдиного реєстру досудових розслідувань.

Як повідомили «Главкому» у департаменті інформаційної підтримки та координації поліції, провадження порушені за статтею 361 Кримінального кодексу України («Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»). Санкція статті передбачає штраф від 600 до 1000 неоподаткових мінімумів доходів громадян або обмеження волі на строк від двох до п'яти років, або позбавлення волі терміном до трьох років.

Загалом, протягом 27 червня – 11 липня до поліції надійшло 1415 заяв та повідомлень про вчинені кримінальні правопорушення та інші події щодо блокування роботи комп'ютерної техніки за допомогою вірусу-шифрувальника.

***

17.07.2017
Придуман новый способ обмана пользователей iOS-устройств

Компания ESET предупредила пользователей iPhone и iPad о новой афере (Український телекомунікаційний портал).

Злоумышленники рассылают письма о несуществующей покупке в iTunes и собирают данные банковских карт и другую личную информацию.

Потенциальной жертве приходит письмо от лица онлайн-магазина, в котором говорится, что Apple ID использовался на неизвестном устройстве для покупки альбома Рианны.

Пользователю предлагается игнорировать сообщение, подтвердив тем самым покупку, или отменить транзакцию, перейдя по ссылке.

Пользователь, часто не обращая внимания на грамматические ошибки в письме и факт того, что адрес отправителя не имеет отношения к Apple, верит мошенникам и переходит на фишинговый сайт.

Там ему предлагается ввести Apple ID и пароль, а также заполнить анкету «для подтверждения личности» (ФИО, телефон, почтовый адрес, дату рождения, данные банковских карт). После ввода данных на странице появится сообщение о том, что учетная запись успешно прошла проверку.

Затем пользователя направляют на главную страницу настоящего iTunes Store, а его персональные данные оказываются у мошенников.

Эксперты рекомендуют игнорировать спам-рассылки и использовать комплексные антивирусные продукты с функциями антиспама и антифишинга.

***

17.07.2017
Киберполиция посоветовала не верить разработчикам M.E.Doc

Правоохранители не рекомендуют вносить M.E.Doc в список исключений антивируса (IGate).

После атак вируса Petya.A/NotPetya департамент Киберполиции Украины советует компания не верить заявлениям разработчика бухгалтерского ПО M.E.Doc о его «полной безопасности». Правоохранители рекомендуют не вносить ПО в список исключений антивирусных программ и фаерволов, что по утверждению компании-разработчика необходимо для его нормального функционирования.

«В случае выполнения этих рекомендаций пользователи неосознанно запретят системам защиты компьютера правильно и своевременно реагировать на вредоносную деятельность ПО, внесенного в «список исключений», –

говорится в пресс-релизе Киберполиции. Такой подход мотивируется тем, что ни один из бухгалтерских программных продуктов не проходит аудит международными компаниями по информационной безопасности.

Правоохранители также не рекомендуют:

– запускать такие программы от имени администратора;

– отключать автоматические обновления ПО и проводить их в ручном режиме, перед установкой проверяя файлы обновления на порталах virustotal.com, malwr.com, reverse.it;

– в случае срабатывания антивируса – следовать его указаниям (блокировать, удалять или вносить в карантин).

***

17.07.2017

Washington Post назвало ОАЭ организатором кибератак на катарские СМИ

Взлом агентства правительственных новостей Катара и сайтов социальных сетей, где в конце мая были опубликованы ложные цитаты скандального характера, приписываемые эмиру Катара шейху Тамиму бин Хамаду аль-Тани и послужившие поводом для конфликта с соседями, организовали ОАЭ. Об этом пишет The Washington Post со ссылкой на источники в разведывательном сообществе США (InternetUA).

Как сообщается, после анализа информации, собранной американскими спецслужбами, подтвердилось, что 23 мая высокопоставленные представители правительства ОАЭ обсудили план спецоперации и его реализацию. При этом осталось неясным, сами ли ОАЭ осуществили хакерские атаки либо наняли иную сторону для их выполнения.

В ложных сообщениях говорилось, что эмир, в частности, назвал Иран «исламской силой» и похвалил ХАМАС. Ссылаясь на эти комментарии, Саудовская Аравия, ОАЭ, Бахрейн и Египет немедленно запретили все катарские СМИ. Затем они разорвали отношения с Катаром и объявили торговый и дипломатический бойкот.

ОАЭ в лице посла в Вашингтоне Юсефа аль-Отайбы отвергли свою причастность к этим действиям и подтвердили ранее высказанные обвинения в адрес Катара.

***

18.07.2017

Как защититься от вирусов-вымогателей и вирусов-разрушителей

27 июня 2017 в Украине была зафиксирована масштабная кибератака, которая одновременно поразила и блокировала деятельность десятков, а впоследствии и тысяч государственных и коммерческих структур страны. Хакерская атака осуществлялась с использованием злоумышленниками

вредоносной программы-разрушителя под названием Diskcoder.C (ExPetr, PetrWrap, Petya, NotPetya).

Докладніше

***

19.07.2017

З’явився стартап, що ловить інтернет піратів за допомогою Bitcoin

Південноафриканський стартап Custos допомагає видавцям та кінокомпаніям знаходити джерела витоку піратських копій та ловити порушників (Espreso.tv).

Про це повідомляє Hightech.

Custos вставляє секретний ключ в кожен примірник фільму чи електронної книги. Секретний ключ – це, по суті, пароль, який дозволяє заявити права на Bitcoin, з якими зазвичай мають справу інтернет пірати. Далі як тільки, порушники поширюють вкрадену продукцію за допомогою Bitcoin, компанія отримує повідомлення з повною інформацією про користувача – де він знаходиться, на який рахунок та звідки переводив кошти.

За словами розробників, як тільки піратська копія потрапляє в мережу, за Bitcoin звертаються, як правило, протягом 5 хвилин. В соціальних мережах – за 42 секунди. Якщо фільм скопійований на DVD або USB, то за 28 хвилин.

Повна анонімність криптовалюти дозволяє піратам відчувати себе абсолютно спокійно та продовжувати свої незаконні операції саме в Bitcoin, адже жодні інші види цифрових платежів не давали б такого ефекту.

***

19.07.2017

Новый вирус превращает Android-смартфоны в шпионские устройства

Специалисты компании Trend Micro обнаружили на Android вирус, который получил название GhostCtrl. Он распространяется на пиратских сайтах с помощью APK-файлов, выдаваемых за популярные приложения и игры (Pokemon GO, WhatsApp и т.п.).

Докладніше

***

19.07.2017

Глобальная кибератака может привести к убыткам, как от природных катастроф

По оценкам аналитиков Lloyd’s of London, масштабная глобальная кибератака способна привести к экономическим потерям на сумму в 53 млрд

долларов, что сопоставимо с ущербом от таких природных катастроф, как суперштorм «Сэнди», который поразил США в 2012 году.

Докладніше

***

18.07.2017
Евгения Подгайная
Рада предлагает штрафовать за «пробелы» в киберзащите

В Верховной Раде зарегистрирован законопроект №6711 «О внесении изменений в КоАП относительно невыполнения требований законодательства по организации и обеспечению защиты информации» (InternetUA).

Нормами документа предлагается накладывать штраф от 50 до 100 необлагаемых минимумов доходов граждан (850 – 1700 грн) на должностных лиц органов госвласти, местного самоуправления, военного управления, предприятий, учреждений и организаций независимо от формы собственности за следующие нарушения:

– Невиконання вимог законодавства щодо організації та забезпечення технічного та/або криптографічного захисту державних інформаційних ресурсів та/або інформації, вимога щодо захисту якої встановлена законом, що циркулюють на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, внаслідок чого створюється реальна загроза порушення цілісності і доступності державних інформаційних ресурсів та/або конфіденційності, цілісності і доступності інформації, вимога щодо захисту якої встановлена законом.

За повторные нарушения, совершенные в течение года после наложения административного взыскания, – штраф от 100 до 150 НМДГ (1700 – 2550 грн).

Законопроект разрабатывала Госспецсвязи.

В пояснительной записке, подписанной главой этого ведомства Леонидом Евдоченко, подчеркнуто, что цель принятия закона – повышение уровня ответственности должностных лиц, по вине которых не обеспечивается выполнение требований законодательства Украины в сфере защиты информации.

***

18.07.2017
Расширение Particle для Chrome сменило владельца и тут же стало вредоносным

Специалисты сайта Bleeping Computer и пользователи популярного расширения Particle для Chrome обратили внимание на странное поведение некогда удобного инструмента. Как выяснилось, в новой версии Particle появилась директория algoad, и расширение «научилось» осуществлять

инжекты в код таких сайтов, как Google, Yahoo, Bing, Amazon, eBay, Booking.com и так далее.

Докладніше

***

18.07.2017

Apple позволит нам защитить паролем любое приложение или файл

Компания Apple работает над продвинутой системой защиты данных на устройствах под управлением iOS. Это подтверждается материалами патента, с которыми ознакомился AppleInsider.ru. Новый интерфейс предусматривает возможность индивидуальной установки паролей для доступа к приложениям и содержащимся в них файлам (InternetUA).

Разработка позволит пользователям оградить свои персональные данные от несанкционированного доступа третьих лиц. Работа функции блокировки описывается на примере приложения, содержащего информацию медицинского характера, однако при должном интересе клиентов ничто не мешает Apple расширить сферу ее применения.

В качестве дополнительного метода защиты приложений Apple планирует задействовать функцию двухфакторной проверки, которая сможет подтвердить личность пользователя, отсканировав его лицо. Соответствующая технология также присутствует в распоряжении компании и, вероятно, будет реализована в iPhone 8.

На данный момент функция защиты приложений паролем не имеет широкого распространения в среде iOS. Такая возможность, как правило, предусматривается только банковскими программами, а также некоторыми текстовыми редакторами. Единственным штатным приложение для iOS, позволяющим установить пароль, остаются «Заметки».

***

18.07.2017

Форма для восстановления пароля MySpace позволяет похитить чужой аккаунт

Исследователь безопасности Ли-Энн Гэллоуэй (Leigh-Anne Galloway) обнаружила простой способ, позволяющий получить доступ к любой учетной записи MySpace. Как оказалось, для похищения чужого аккаунта достаточно лишь знать имя, на которое он зарегистрирован, имя пользователя и его дату рождения. Исследователь уведомила MySpace о проблеме еще в апреле текущего года. Поскольку администрация соцсети не ответила на сообщение, Гэллоуэй решила предать уязвимость огласке (InternetUA).

Проблема заключается в том, что форма для восстановления пароля учетной записи MySpace запрашивает слишком мало данных для подтверждения личности владельца аккаунта. Для изменения пароля

достаточно лишь указать имя и фамилию нужного человека, имя пользователя и дату рождения. Первые два пункта и так видны всем, и злоумышленнику остается лишь узнать дату рождения жертвы. Другие поля в форме рекомендуются к заполнению, но на практике достоверность указанной них информации не проверяется.

17 июля администрация MySpace перенаправила URL-адрес для восстановления пароля, и теперь он больше не ведет на уязвимую форму. Решение администрации соцсети закрыть доступ к уязвимой форме свидетельствует о том, что ей известно о проблеме.

***

18.07.2017

Google упростит двухэтапную аутентификацию для приверженцев SMS

В феврале этого года Google обновила подсказки для двухэтапной аутентификации, обеспечивающей лучший способ защиты учётных записей пользователей. Помимо подтверждения личности по зашифрованному соединению новая функция также позволяет блокировать несанкционированный доступ к своей учётной записи в режиме реального времени при попытке входа посторонним человеком в систему. Начиная с этой недели Google будет предлагать перейти на новую систему защиты всем, кто использует подтверждение личности по SMS (InternetUA).

Каждому, кто использует двухэтапную аутентификацию с помощью SMS, при очередном входе в систему придёт уведомление с предложением перейти на новую систему авторизации с помощью уведомлений вместо обычных текстовых сообщений. Если им этот способ не понравится, то они смогут вернуться к старому методу.

Google рекомендует переходить на новую систему, так как проверки личности с помощью SMS и одноразовых кодов более восприимчивы к фишинговым атакам. Благодаря уведомлениям администраторы могут быть уверены в защите своих систем, так как аутентификация происходит через зашифрованное соединение.

Предложение протестировать новый способ двухэтапной аутентификации получат только те, кто сейчас использует технологию проверки личности по SMS. Владельцам iOS-устройств придётся загрузить приложение Google Search. При этом если человек решит не отказываться от SMS, через полгода ему повторно будет предложено перейти на новый способ аутентификации.

***

18.07.2017

Личные данные 4 миллионов клиентов Dow Jones утекли в Сеть

Американская аналитическая компания Dow Jones ненамеренно опубликовала в открытом доступе данные 4 миллионов своих клиентов. Утечка была обнаружена в июне текущего года исследователем безопасности Крисом Викери (Chris Vickery) (InternetUA).

В открытом доступе оказались личные данные подписчиков аналитической компании Dow Jones, включая имена, внутренние идентификаторы, адреса, платежные реквизиты и 4 последние цифры пластиковых карт.

Компания Dow Jones подтвердила утечку данных, однако не считает инцидент чем-то серьёзным. По мнению аналитиков Dow Jones, попавшие в открытый доступ данные не являются конфиденциальными, поскольку не содержат пароли в открытом виде. Поэтому компания не будет уведомлять своих клиентов об утечке.

Утечка произошла из-за некорректно настроенных политик безопасности AWS S3.

***

19.07.2017

ФБР предупредило родителей об опасности IoT-игрушек

17 июля ФБР опубликовало уведомление для родителей, чьи дети играют с «умными» игрушками. Бюро рекомендовало внимательно проверить подключенных к интернету кукол, медведей и пр. на предмет угрозы конфиденциальности персональных данных (InternetUA).

Согласно уведомлению, многие игрушки с функционалом, базирующимся на облачных технологиях (например, распознавание речи), «могут представлять угрозу конфиденциальности и безопасности детей в связи с большим объемом персональной информации, которая может быть непреднамеренно раскрыта». Безопасности таких игрушек уделяется недостаточно внимания, поскольку производители прежде всего стремятся сделать их как можно более удобными в использовании и привлекательным для покупателей, считают специалисты ФБР.

«Потребители должны найти в интернете информацию обо всех известных проблемах в этих игрушках, обнаруженных исследователями или упомянутых в отзывах покупателей», – говорится в уведомлении. Кроме того, бюро рекомендовало родителям внимательно ознакомиться с положениями о защите конфиденциальных данных, которыми руководствуется производитель.

***

19.07.2017

В сети выследили крупнейшую сеть порноботов

Исследователи в области интернет-безопасности вычислили порноботнет SIREN, распространявший ссылки на эротические видео в Twitter. Об этом сообщается в отчете компании ZeroFOX (InternetUA).

По словам специалистов, ботнет контролировал более 90 тысяч аккаунтов и сгенерировал 8,5 миллионов постов, что делает его крупнейшей сетью фейковых аккаунтов в соцсетях. С февраля 2017 года по размещенным SIREN ссылкам перешли более 30 миллионов человек.

Аккаунты-боты притворялись молодыми девушками и связывались с пользователями через ответы на их твиты, предлагая перейти по прикрепленным к их записям ссылкам. Жертвы попадали на сайты с порнороликами и эротическими чатами, где им под видом оформления платной премиум-подписки предлагали оставить свои платежные данные.

В июне журналисты Motherboard получили доступ к серверу, с помощью которого работал порнобот в Twitter. Там размещались сотни имен, тысячи эротических фотографий и подписей к ним, с помощью которых фейковый аккаунт распространял ссылки на сайты для взрослых.

***

19.07.2017

Исследователь нашел необычный способ «угона» учетных записей Facebook

Исследователь Джеймс Мартиндейл (James Martindale) нашел способ перехвата управления над чужой учетной записью Facebook. Сделать это можно посредством функции восстановления аккаунта и старого телефонного номера владельца.

Докладніше

***

20.07.2017

«Дьявольская» уязвимость ставит под угрозу тысячи IoT-устройств

Исследователи компании Senrio обнаружили уязвимость в библиотеке gSOAP, ставящую под угрозу тысячи устройств «Интернета вещей» (IoT). Уязвимость CVE-2017-9765, получившая название Devil’s Ivy, позволяет вызвать переполнение буфера, однако экспертам удалось с ее помощью выполнить код на уязвимой камере безопасности (InternetUA).

Проблема была обнаружена во время анализа прошивки камер безопасности Axis M3004. Когда исследователи уведомили о ней производителя, представители Axis сообщили, что уязвимость затрагивает 249 из 252 выпускаемых компанией моделей камер безопасности. Производитель уже выпустил обновления для своих продуктов. Разработчик библиотеки Genivia исправил уязвимость в версии gSOAP 2.8.48, вышедшей 21 июня текущего года.

По данным, указанным на сайте gSOAP, библиотека была загружена более 1 млн раз. Согласно подсчетам Senrio, Devil’s Ivy затрагивает тысячи устройств.

gSOAP – библиотека с двойным лицензированием (бесплатная и коммерческая), широко используемая в разработке прошивки для встроенных устройств. Библиотека разработана компанией Genivia и позволяет производить продукты в соответствии с новейшими промышленными стандартами XML, XML Web services, WSDL и SOAP, REST, JSON, WS-Security, WS-Trust с SAML, WS-ReliableMessaging, WS-Discovery, TR-069, ONVIF, AWS, WCF и пр.

***

20.07.2017

Опасный банковский троян получает контроль над Android-устройствами

«Доктор Веб» предупреждает о появлении опасной вредоносной программы, атакующей владельцев мобильных устройств на базе операционных систем семейства Android (InternetUA).

Зловред Android.BankBot.211.origin – это банковский троян, угрожающий пользователям десятков стран по всему миру. Программа распространяется под видом безобидных приложений, например, проигрывателя Adobe Flash Player. После проникновения на устройство жертвы зловред пытается получить доступ к специальным возможностям (Accessibility Service). Для этого троян показывает окно с запросом, которое при каждом его закрытии появляется вновь и не даёт работать с устройством.

Режим специальных возможностей упрощает работу со смартфонами и планшетами на базе Android. Он применяется в том числе для помощи пользователям с ограниченными возможностями: этот режим позволяет программам самостоятельно нажимать на различные элементы интерфейса, такие как кнопки в диалоговых окнах и системных меню.

В случае Android.BankBot.211.origin режим специальных возможностей эксплуатируется для выполнения вредоносных действий. Так, троян добавляет себя в список администраторов устройства, устанавливает менеджером сообщений по умолчанию и получает доступ к функциям захвата изображения с экрана.

Зловред крадёт конфиденциальную информацию клиентов кредитно-финансовых организаций. Так, троян способен показывать поддельные формы ввода логина и пароля поверх запускаемых банковских программ, а также отображать фишинговое окно настроек платёжного сервиса с запросом ввода информации. Свои действия вредоносная программа согласует с управляющим сервером.

***

20.07.2017

Британцы не сертифицировали продукты «Лаборатории Касперского»

В Национальном центре кибербезопасности Великобритании (National Cyber Security Centre, NCSC) заявили, что организация никогда не сертифицировала продукцию российского производителя антивирусных решений «Лаборатория Касперского» (InternetUA).

«NCSC сертифицирует продукты по ряду инициатив и поставщики подают заявки на сертификацию через наших аккредитованных партнеров лаборатории, но у нас никогда не было продуктов “Лаборатори Касперского”», – приводит информагентство Reuters заявление центра.

Ранее власти США исключили «Лабораторию Касперского» из списка поставщиков, чьи разработки разрешено приобретать госструктурам страны. В ответ на это, представители российского производителя заявили, что компания оказалась жертвой геополитического противостояния России и США.

***

21.07.2017

AVPass – инструмент для обхода антивируса на Android AVPass – инструмент для обхода антивируса на Android

Команда исследователей из Технологического института штата Джорджия (США) разработала хакерский инструмент под названием AVPass, который может изучать и обходить защиту антивирусных решений для смартфонов и планшетов под управлением Android.

Докладніше

***

25.07.2017

Опасный вирус поразил смартфоны на Android в десятках стран

Специалисты антивирусной компании «Доктор Веб» предупредили о распространении банковской троянской программы BankBot. Она управляет зараженными смартфонами и похищает конфиденциальную информацию (InternetUA).

В настоящее время угроза реальна для пользователей из десятков стран мира, утверждают эксперты.

BankBot распространяется под видом безобидных приложений – например, Adobe Flash Player. После заражения троян открывает окно с требованием предоставить ему доступ к специальным возможностям (Accessibility Service). В этом режиме, предназначенном для пользователей с ограниченными возможностями, программы могут самостоятельно нажимать на виртуальные кнопки в диалоговых окнах и системных меню. Для мобильных вредоносных приложений это необычная функциональность.

После того как пользователь вынужденно разрешает BankBot доступ к специальным возможностям, троян самостоятельно получает права администратора («нажимая» на нужные кнопки в настройках). Пользователь может даже не заметить этого, потому что процесс происходит очень быстро. Впоследствии, если владелец смартфона попытается ограничить вирусу доступ к расширенным функциям, BankBot вернет их обратно.

В ходе своей деятельности BankBot собирает информацию о запускаемых приложениях и действиях пользователей в них, а также похищает все логины и пароли, которые пользователь вводит на любых сайтах и в приложениях. Кроме того, вирус может демонстрировать фальшивые окна для входа в системы интернет-банкинга, платежные системы и магазин Google Play.

***

24.07.2017

Павел Красномовец

ESET обнаружил adware-кампанию, поразившую более 100 000 устройств в Украине

Исследователи словацкой антивирусной компании ESET обнаружили adware-кампанию Stantinko, успешно действующую с 2012 года. С 2015 года злоумышленникам удалось заразить более 500 000 устройств. Больше всего пострадавших в Украине (33 %) и России (46 %).

Докладніше

***

24.07.2017

Швеция допустила утечку личных данных практически всех своих граждан

Утечка личных данных практически всех граждан Швеции произошла по вине Транспортного ведомства Швеции во время передачи компании IBM личных данных всех владельцев транспортных средств. Утечка затронула не только частный сектор, но и транспортные средства, принадлежащие полиции и армии (InternetUA).

В ходе утечки стали доступными имена, фотографии и адреса проживания миллионов граждан Швеции, среди которых пилоты ВВС Швеции, сотрудники секретных подразделений, люди, пребывающие в розыске, граждане, находящиеся в программе защиты свидетелей, а также пропускная способность всех дорог, постов и много всего другого.

В 2015 году Транспортное ведомство Швеции заключила с компанией IBM контракт на обслуживание IT-инфраструктуры ведомства, включая обслуживание баз данных и телекоммуникационные сети.

После заключения контракта сотрудники ведомства загрузили базы данных на серверы IBM в облако, а затем осуществили email-рассылку всего

содержимого базы своим подписчикам. Кроме того, все сотрудники IBM заполучили полный доступ ко всей базе ведомства.

Утечка была обнаружена лишь в 2016 году, по факту которой было открыто служебное расследование. В 2017 году глава ведомства Мария Агрен (Maria Ågren) была уволена со своего поста. В качестве наказания ей был назначен штраф в размере 70 тыс. шведских крон (примерно $8,5 тыс.).

***

25.07.2017
Андрей Щербаков
Как обезопасить данные с мобильных гаджетов и быть уверенным в защите устройства

Блокировка телефона сложным паролем, хранение в труднодоступных карманах, шифрование мессенджеров и файлов зачастую не помогает избежать неприятного инцидента с кражей или потерей телефона. Продумать надежные способы защиты с использованием современных технологий и полезных лайфхаков лучше сразу после покупки нового устройства.

Докладніше

ДОДАТКИ

Додаток 1

17.07.2017
В Skype под натиском пользователей вернули старые функции

В начале прошлого месяца компания Microsoft объявила о полном редизайне Skype. В популярный сервис обмена сообщения были добавлены функции из других мессенджеров, таких как Snapchat и Messenger. Разработчики добавили интеграцию с популярными сервисами, вроде YouTube, Giphy и Weather, аналог историй из Snapchat, редактор фотографий и прочее. Многие пользователи встретили такие кардинальные изменения не совсем радостно. Некоторые перешли на другие сервисы, а другие потребовали вернуть всё обратно. Microsoft всё же пошла на уступки и решила вернуть некоторые старые функции (InternetUA).

С последним обновлением в Skype вернули значок состояния. Он позволяет другим пользователям видеть ваш статус из списка контактов. Также Microsoft вернула в клиент на Android и iOS функцию обмена контентом с другими сервисами и мобильными приложениями.

Не обошлось и без новых функций. Microsoft расширила возможность настройки внешнего вида приложения с помощью новых тем и цветов. Были также внесены некоторые исправления, связанные с возможностью удалять контакты и переписки, с уведомлениями и проблемами многозадачности.

Также Microsoft выпустила обновление для Windows 10. В Skype переработали пользовательский интерфейс. Доступ к профилю, новым разговорам, панели набора номера и прочему теперь стал гораздо проще и быстрее.

В меню Share появилась возможность обмениваться видео, фотографиями и другими файлами. Также к каждому сообщению в переписке можно добавить эмоцию, показав собеседнику, как вы относитесь к сказанному.

Все изменения уже доступны в новых версиях Skype.

(вгору)

Додаток 2

18.07.2017

У социальной сети LinkedIn появился клиент для Windows 10

У профессиональной социальной сети LinkedIn появилось приложение для Windows 10. В нём доступны многие функции, которые присутствуют в мобильных приложениях сервиса и настольной версии сайта. Среди них – приём сообщений и приглашений от других пользователей в реальном времени (InternetUA).

Новое приложение – это более гибкий способ всегда оставаться в курсе последних событий, рассказал старший директор по разработке Крис Прюэ (Chris Pruett). Именно он обновил сайт и мобильные приложения LinkedIn.

«Я вижу приложение для Windows 10 как очередную главу нашей развивающейся истории, – сказал Прюэ. – Весь упор в нём сделан на том, чтобы вы могли оставаться на связи».

Приложение для Windows 10 поддерживает анимированную плитку в меню «Пуск». На ней отображаются новые сообщения и другая актуальная информация.

По словам менеджера по продукту Хермеса Альвареса (Hermes Alvarez), новое приложение LinkedIn избавит от необходимости переключаться между мобильной и настольной версией платформы. Он сравнил программу с популярным корпоративным мессенджером Slack.

Новым клиентом уже могут пользоваться жители США. К концу июля он станет доступен по всему миру.

В социальной сети зарегистрировано примерно 500 миллионов человек. Около 40 % из них пользуются ей с компьютеров: ищут работу и новости, а также устанавливают деловые связи. Остальные 60 % – мобильные пользователи.

Чуть больше года назад Microsoft купила LinkedIn за $26,2 миллиарда. С тех пор для удержания пользователей компания добавила в социальную сеть интеллектуальную систему сообщений, новые возможности для поиска работы и раздел с деловыми новостями.

(вгору)

Додаток 3

19.07.2017

Павел Красномовец

Владелец «Киевстар» запускает в Украине мессенджер с бесплатными сообщениями, звонками и новостями

Материнский холдинг «Киевстар» Veon (ранее Vimpelcom) объявил о запуске «персональной интернет-платформы» в Украине, Грузии, России и Пакистане. Приложение VEON должно стать «единой цифровой точкой входа» для абонентов. Трафик в нем для абонентов сети не будет тарифицироваться и абоненты смогут использовать его даже при нулевом балансе, утверждаютв Veon. В пресс-службе «Киевстар» подтвердили AIN.UA, что трафик для приложения уже не учитывается в счете (AIN.UA).

Для Android приложение VEON уже доступно для скачивания, а для iOS пока еще находится в разработке. Оно включает в себя мессенджер со всеми функциями, к которым уже привыкли пользователи на других платформах: звонки, аудиосообщения, групповые чаты, возможность делиться своим местоположением и другие функции.

Приложение также позволяет управлять своим счетом: следить за состоянием баланса, трафиком, управлять тарифами. Помимо этого, VEON с помощью «аналитики данных и искусственного интеллекта позволяет открывать новый контент каждый день: персонализированные новости, музыку и видео». Абоненту также будут доступны спецпредложения от кафе, кинотеатров и других заведений.

Из этих функций абонентам «Киевстар» пока доступны звонки и тексовые сообщения, новостной канал и управление мобильным счетом. Но в пресс-службе заверили, что обновление приложения происходит постоянно и украинские пользователи постепенно будут получать новую функциональность.

В дальнейшем в Veon обещают расширять возможности платформы и добавлять новые сервисы совместно с партнерами. Предложения будут базироваться на «контекстуальной информации, полученной от давших согласие пользователей».

Напомним, о ребрендинге VimpelCom в Veon и новой цифровой стратегии холдинг объявил в финансовом отчете за прошлый год. Тогда же компания заключила глобальное партнерство с видеосервисом STUDIO+, музыкальным стриминговым сервисом Deezer и Mastercard. Каждая из компаний должна была интегрировать новые сервисы в платформу VEON.

Цифровая платформа – опытка телеком-холдинга перейти от модели продажи доступа к инфраструктуре (связи и мобильному интернету) к цифровым услугам. В ближайшем будущем компания планирует зарабатывать до 40% от мобильно-финансового бизнеса, а не связи. Монетизация VEON, который не приносит денег с трафика, будет идти за счет кооперации с другими бизнесами (комиссия за привод клиента) и таргетированной рекламы.

(вгору)

Додаток 4

25.07.2017

На страницах в Facebook теперь можно создавать группы по интересам

Пользователям Facebook стала доступна функция Groups for Pages, которая позволяет авторам страниц создавать на них подгруппы. В них люди могут переписываться друг с другом и с владельцами страниц. Крис Кокс (Chris Cox), главный руководитель по продукту, сравнил подгруппы с фан-клубами (InternetUA).

«Если вы художник или представляете компанию, бренд или газету, то теперь можете создавать фан-клубы и группы для своих суперфанатов», – заявил Кокс.

Он рассказал, что идея ввести новую функцию пришла, когда сотрудники газеты Washington Post создали в Facebook группу PostThis – from The Washington Post. В ней репортёры могут напрямую общаться с читателями. Кокс сравнил это с «цифровой версией писем редактору, но с постоянными обсуждениями в реальном времени».

Нововведение позволяет брендам создавать собственные группы, не используя личные аккаунты сотрудников. Это помогает защитить их конфиденциальность.

В отдельной публикации генеральный директор Facebook Марк Цукерберг (Mark Zuckerberg) сказал, что новая функция должна помочь большему числу людей вступить в значимые сообщества. В качестве примера он привёл группу сайта по борьбе с зависимостями Addiction Unscripted, в которую вступило уже более 47 тысяч человек.

«В современном мире все мы получаем поддержку из нескольких источников: наших семей и друзей, наших сообществ и нашей системы социальной защиты, – написал Цукерберг. – В рамках гражданской дискуссии мы больше всего концентрируемся на системе социальной защиты, но я выяснил, что сообщества зачастую не менее важны в заботе о нас, и нам нужно уделить столько же времени их созданию».

Facebook рассказала, что в социальной сети 70 миллионов страниц художников, компаний, брендов и газет.

(вгору)

Додаток 5

18.07.2017

NBC: половина американцев считает активность Трампа в Twitter опасной

Большинство американцев не одобряет сообщения, которые глава государства Дональд Трамп публикует на своей личной странице в Twitter, и в

целом считают, что хозяин Белого дома ведет себя не по-президентски. Об этом свидетельствуют результаты опроса телеканала NBC, опубликованные 17 июля (MResearcher).

Согласно данным проведенного исследования, 68 % опрошенных считают, что Трамп своим поведением демонстрирует негативный пример, 70 % полагают, что он ведет себя не так, как положено президенту. 57 % респондентов заявили, что чем больше они слышат о Трампе, тем меньше он им нравится. 56 % при этом отметили, что поведение главы государства «наносит ущерб его президентству» отмечает NBC.

Критике со стороны участников данного опроса, проведенного совместно с газетой The Washington Post, подверглись сообщения, которые Трамп публикует в своем Twitter. 68 % респондентов считают большинство «твитов» президента неуместными, 65 % – оскорбительными, 52 % – опасными, следует из результатов опроса, участие в котором приняли более 1 тыс. случайно выбранных жителей США. В целом 67 % респондентов не одобряют тот факт, что американский лидер пользуется Twitter.

Трамп после инаугурации начал пользоваться официальным президентским аккаунтом в Twitter, однако при этом продолжил публиковать сообщения на своей личной странице в этом сервисе. Республиканец уделяет повышенное внимание социальным сетям в качестве средства информации и общения со своими сторонниками. Он ранее заявлял, что без возможности доводить с помощью соцсетей свои мысли до общественности он никогда, по его мнению, не стал бы президентом США. Многие публикуемые Трампом в Twitter сообщения часто подвергаются критике со стороны противников президента.

(вгору)

Додаток 6

12.07.2017
Павел Красномовец
Facebook начал глобальное тестирование рекламы в Messenger

Messenger – третий по популярности продукт Facebook после самой соцсети и WhatsApp. Компания стремится монетизировать его 1,2-миллиардную аудиторию. Поэтому после «многообещающих результатов в Австралии и Тайланде», бета-тестирование рекламных объявлений расширили для брендов по всему миру, говорится в официальном блоге сервиса (AIN.UA).

В июле небольшой процент пользователей начнет видеть рекламу в основной вкладке Messenger. В течение ближайших месяцев аудитория объявлений будет расширяться. Размещение рекламы будет зависеть от «количества разговоров пользователя, физического размера экрана смартфона и плотности пикселей дисплея», – сообщили в компании TechCrunch. Отключить рекламу в мессенджере пользователи не смогут. Единственный вариант –

нажимать на стрелку в каждом объявлении, чтобы пожаловаться на него и спрятать.

Процент рекламодателей, которым доступно размещение в Messenger, также будет увеличиваться в ближайшее время. Создать кампанию можно в Ads Manager или Power Editor. Messenger станет одним из автоматических плейсментов наряду с основным приложением Facebook, Instagram и Audience Network.

Таргетинг объявлений происходит не по тому, что пользователи пишут в сообщениях. В размещениях в Messenger используется стандартный таргетинг соцсети и инструменты измерения. Просмотренным считается объявление, 50 % пикселей которого находилось в поле зрения пользователя.

При нажатии на объявление, во внутреннем браузере Messenger может открыться веб-сайт рекламодателя. Еще один вариант – интеграция с другими рекламными форматами, доступными в мессенджере Facebook. Баннер также может работать как объявления Click To Messege, которые начинают разговор пользователя с брендом в мессенджере. Благодаря ему в дальнейшем рекламодатель сможет отправлять Sponsored Messeges, чтобы продолжить общение.

(вгору)

Додаток 7

20.07.2017

Українці тепер можуть здійснювати грошові перекази через Facebook

Компанія LeoGaming в партнерстві з Mastercard запустили LeoBot – платіжного бота в соціальній мережі Facebook з інтегрованою платформою цифрових гаманців Masterpass. Він дозволяє здійснювати грошові перекази між картковими рахунками українських банків з мобільного пристрою в один клік. Проект реалізований за технічної підтримки TAS Link і платформи UniBot (Finance.ua).

Скористатися ботом LeoBot можуть всі користувачі програми Messenger. Додаткова реєстрація не потрібна, всі функції платіжного бота доступні для нових клієнтів.

Навігація між функціями бота відбувається за допомогою команд, які можна вибрати в переліку або ж прописати вручну. Завдяки інтеграції з Masterpass здійснити грошовий переказ з використанням робота можна навіть не тримаючи платіжну картку в руках. Для цього необхідно лише один раз ввести дані банківської картки або авторизувати раніше створений гаманець Masterpass, в якому можна зберігати дані карток різних платіжних систем. Під час подальшого використання LeoBot можна буде швидко вибрати шаблон платежу на основі попередніх транзакцій і здійснити грошовий переказ в один клік. Гарантом безпеки переказів з Masterpass є Mastercard.

(вгору)

Додаток 8

25.07.2017

Цена рекламы в Facebook и Google к октябрю может увеличиться в два раза

Дарина Шварцман

Директор по развитию агентства эффективного интернет-маркетинга WebPromo Антон Воронюк детально рассказал InternetUA о том, как изменили рекламный рынок блокировки российских интернет-ресурсов (internetua).

– Ваш коллега Александр Колб заявил, что блокировки российских ресурсов отбросили его бизнес на 6-8 месяцев назад…

– Не называя цифры, скажу, что и на нас они негативно отразились. Если говорить в целом, то за полтора месяца ставка в Google увеличилась на 10-30 %, в Facebook – в полтора раза. И это еще не предел. Не нужно забывать о том, что сейчас лето, соответственно бизнес-активность низкая. В октябре-декабре, когда начнут вливаться основные бюджеты, ставки будут расти. Может произойти и двукратный рост, по сравнению с июнем.

Механика предельно простая – растет конкуренция и повышается цена клика. Поэтому из-за того, что рекламодатели одновременно перебросили свои деньги с «Яндекса», «ВКонтакте» и «Одноклассников» на Google и Facebook произошел ощутимый рост стоимости клика.

– Но будет ли реклама, скажем, в Facebook также эффективна как в «ВКонтакте», ведь там разные аудитории?

– С точки зрения рекламных инструментов, таргетинга Facebook изначально был довольно сильным. И не стоит забывать, что Facebook – это еще плюс одна площадка Instagram. С одного кабинета вы запускаете рекламу в двух социальных сетях. Instagram – это непаханое поле, там еще многие не представлены. Поэтому если вести правильную рекламную политику на этой площадке можно получить хорошие результаты и заменить, условно говоря, «ВКонтакте». На Facebook при текущей стоимости реклама будет нерентабельной.

– Какой бизнес больше всего пострадал от Указа Президента?

– Досталось электронной коммерции, которая и так балансирует на грани нерентабельности. Если же говорить о нишах, то практически всем придется затянуть пояса – и fashion-сегменту, и игрушкам.

– На данный момент бизнес все еще ведет активную деятельность на запрещенных ресурсах и продолжает размешать там рекламу. Есть ли в этом смысл?

– Большинству нужна украинская аудитория. В сложившейся ситуации географический таргетинг отсутствует. Поэтому это как стрелять из пушки по воробьям. Мы проводили семинар в Одессе. И ради интереса посмотрели, какой процент горожан заходят через VPN: 15-20% были с Румынии, Нидерландов, Германии и т.д.

– Как вы лично относитесь к блокировкам?

– Я не затрагиваю политический аспект, говорю только с точки зрения бизнеса. Блокировка «Яндекса» и российских социальных сетей сформировала монополию. А монополия – это плохо как для бизнеса, так и для людей. Всегда хорошо, когда есть выбор. Но вся Европа замечательно живет с 98 % Google и 100 % Facebook. Мы же работали по-другому. И нас резко заставили изменить правила игры.

– Какая была реакция рекламодателей?

– Они потеряли свои деньги на аккаунтах. Какая в таком случае может быть реакция? Все возмущались. Ведь нормально ничего не дали закрыть. Был просто бардак.

– Насколько придется увеличить рекламные бюджеты?

– Я бы не говорил об увеличении. Нужно полностью менять маркетинговую стратегию. И к этому сейчас многие приходят. В Украине интернет-маркетинг всегда был сконцентрирован на Performance. А это только одна колонка из всех возможных источников трафика. То есть вы отвечаете на сформированный спрос: у человека есть потребность купить ноутбук, вы ему его показываете. Но дальнейшее существование бизнеса напрямую зависит от того, сможете ли вы этой аудитории, которой один раз продали ноутбук, продать его же через два-три года только нового поколения и сделать кросс-продажи. Данный процесс построения бренда в интернете – лояльности и коммуникации – основывется уже на других инструментах: контент-маркетинге, e-mail рассылках, smm-коммуникациях. Это те инструменты, которые, в первую очередь, отталкиваются от инвестиций в контент. Но пока у нас на рынке отсутствует качественный e-mail маркетинг. Сложно встретить хорошую рассылку, которую приятно читать, порекомендовать знакомым, перейти из нее в интернет-магазин и сделать покупку. Все только начинает развиваться.

– То есть балом будет править качественный контент?

– Сейчас многие зациклены только на краткосрочной стратегии: вложил-получил. Но на данный момент тем компаниям, которые хотят выстоять на рынке, постоянно расти, нужно будет научиться играть в долгую.

В США в большинстве нишах реклама нерентабельная: вкладываешь больше, чем получаешь. Все коммуникации, которые происходят, направлены на сбор сообщества и его удержание.

Есть три классические точки приземления. Первая, по которой сейчас все играют, – это коммерческое предложение, иными словами «купи ноутбук». Все хотят, чтобы человек зашел на сайт, увидел предложение «купить ноутбук» и купил. Но среднестатистическая конверсия в электронной коммерции 1% и она уменьшается. На сто человек, которые зашли на сайт, покупает только один. Платят же за сто.

Вторая точка приземления – это так называемая широкая воронка, то есть акции. Их логика проста: используя инфоповоды, акционные предложения заставляют человека быстрее решиться на покупку. Такой прием хорошо работает в медийной рекламе, почтовых рассылках и т.д.

Третья точка – лидогенерация, когда человеку предлагается какая-либо «плюшка» в обмен на регистрацию. В итоге компания получает e-mail, номер телефона. Формируется большая база контактов, которые можно использовать в e-mail-маркетинге, смс-рассылках. Можно также делать ремаркетинг в Facebook и Google.

Сейчас идет перераспределение рекламных бюджетов между этими тремя точками приземления. Больше всего уходит в третий канал. Постепенно до трети рекламного бюджета уйдет в лидогенерацию.

– Если сравнивать 2017 год и ситуацию несколько лет назад, изменился ли рекламный рынок, стало ли легче завлекать клиентов?

– Стоимость привлечения стала дороже. Но у большинства игроков отточились процессы – появились интернет-маркетологи, логика взаимодействия с подрядчиком, система отслеживания результатов, нормальная веб-аналитика. То есть с точки зрения дикого рынка, который был еще три года назад, рынок стал лучше, идут осмысленные инвестиции.

Также за это время увеличилось проникновение интернета, значительно вырост мобайл и дальше будет только расти. Как результат, в онлайн начали заходить ниши, которые раньше не были представлены в интернете – крупные продуктовые компании, фарма, аграрный сектор. Это показывает, что интернет стал серьезным и эффективным каналом коммуникации.

– Что нового может появиться на рынке интернет-рекламы в ближайшие несколько лет?

– Делать прогнозы не очень благодарное дело. Ведь кроме субъективных веяний на рынок, существуют непредсказуемые вещи – запреты, различные видоизменения. Может Google захочет купить «Яндекс»?

Если и посмотреть на существующие тренды, то Performance-маркетинг будет постепенно смещаться к каналам удержания, соответственно, будут увеличиваться инвестиции в качественный контент.

В соцсетях сейчас популярная тема чат-ботов. Пока они используются как коммуникационные инструменты. Смогут ли они продавать, остается еще под вопросом.

Facebook и Google все больше используют искусственный интеллект – системы автоматизации, которые позволяют запускать рекламу даже не особо подкованным. Тенденция в будущем станет только усиливаться. Все большую популярность будет набирать Programmatic.

(вгору)

Додаток 9

16.07.2017

Прокидається з відчуттям обов’язку зробити фото в Instagram

19-річна студентка ТНПУ Христина Луцик прокидається вранці не з відчуттям голоду, а з відчуттям обов`язку – зробити нове фото для Instagram.

Дівчина доєдналася до інстаграмерів рік тому. І відтоді «пішло-поїхало» (20 хвилин).

– Я стала активніше користуватися Instagram після того, як закрили ВКонтакті, – розповідає Христина. – Так би мовити, перекочувала з однієї мережі в іншу. Всі друзі і знайомі там зареєстровані, тому не хотіла залишатися білою вороною. Дівчина розповідає, що фотографії робить кожного дня, коли трапляється якийсь гарний кадр. – Можна сказати, що я роблю світлини з плином життя, – пояснює дівчина. – Сиджу в кафе, бачу гарну локацію – фотографуюся. Тільки завжди підходжу до цього творчо. Христина каже, що стежить в мережі за життям своїх фоловерів і показує їм своє життя.

– Я люблю ділитися хорошими моментами із друзями – розповідає інстаграмер. – А також люблю, коли бачу схвальні відгуки – лайки і коментарі. Дівчина розуміє актуальність проблеми людей, залежних від соціальних мереж. – Втуплених в екрани своїх телефонів тернополян можна зустріти на кожному кроці, – каже Христина. – Вони і в парку, і в кафе, і в магазинах. Люди перестали цінувати живе спілкування. Я розумію, що сама можу стати однією із тих залежних, які уже не уявляють свого життя без Instagram або іншої соціальної мережі. Ще дівчина зазначає «фальшивість» багатьох профілів в Instagram. Мовляв, кожен прагне показати своє ідеальне життя. Тому часто вдається до обману своїх фоловерів. – Маю одну знайому, яка в Instagram пропагує здоровий спосіб життя, – розповідає Христина. – Але після того, як вона відкладає телефон, щойно сфотографувавши низькокалорійний салат, береться за жирнючий гамбургер.

У чому ж причина постійної потреби людей фіксувати кожен свій крок і повідомляти про це в соцмережі, пояснює психолог Галина Синоруб.

– Це все самовираження, самоствердження, – розповідає психолог. – Люди хочуть, щоб на них звернули увагу. До того ж зараз активізувалася така собі «лайко манія». Саме лайки дарують людям відчуття самовизнання, у них підвищується настрій та самооцінка. Психолог вважає, що залежність від соціальних мереж частіше «діагностують» у невпевнених у собі людей. До того ж зараз людство переходить на вищий рівень комунікації. Тепер не потрібно зустрічатися, щоб вирішити якісь питання, варто лише написати в Messenger. – Не можна сказати, що людина, яка постійно «тусується» в соцмережах, – самотня, – вважає психолог. – Вона може бути самодостатньою і мати багато реальних друзів, але їй просто легше самовиразитися в онлайні.

Галина Синоруб дає основну пораду, що допоможе не потрапити в тенета соцмереж, – контролювати час. Не втрачати відчуття часу і простору. Зараз такий темп і спосіб життя, що цілком обірвати всі зв`язки з соціальними мережами ми не можемо. Але можемо контролювати час перебування в них. За словами психолога, ми повинні жити в реальності і час від часу доєднуватися до «напівреальності», а не навпаки.

(вгору)

Додаток 10

17.07.2017

Facebook определил самый популярный эмодзи

В Международный день эмодзи представители корпорации представили статистику по использованию смайликов в социальной сети и Messenger (InternetUA).

В Международный день эмодзи Facebook определил, какие эмодзи пользователи используют чаще всего. Самым популярным стикером за последние 30 дней оказался плачущий от смеха смайлик, второе место занял эмодзи с глазами в форме сердец, на третьем месте – «поцелуй».

Аудитория Facebook, по данным корпорации на конец июня, составляет 2 млрд человек. Ежедневно пользователи отправляют друг другу более 60 млрд эмодзи в социальной сети и более 5 млрд через Messenger.

Самым популярным эмодзи в США оказался «плачущий от смеха», а в Messenger американцы чаще всего пересылают поцелуй. В Германии популярнее всех обычный улыбающийся смайлик, а французы любят подмигивать в социальных сетях. Причем в Messenger во Франции лидирует сердце, пронзенное стрелой. В Италии и Испании также часто шлют поцелуи. Британцы чаще всего шлют в Facebook смеющиеся стикеры со слезами, а через Messenger – сердце.

Кроме того, в преддверии выхода в прокат The Emoji Movie представители социальной сети решили добавить набор из 16 новых наклеек с персонажами эмодзи. В фильме рассказывается о жителях города Текстополис, который есть внутри каждого смартфона.

Международный день эмодзи отмечают 17 июля и не имеет официального статуса. Эта дата была выбрана в связи с тем, что она нарисована на иконке с календарем в iOS.

(вгору)

Додаток 11

13.07.2017

США підозрюють Україну у втручанні в вибори. У ФБР хочуть розслідування

У США почали підозрювати, що Україна втручалася в американські президентські вибори минулого року (Espreso.tv).

Про це повідомляє видання «Голос Америки».

Про це почали говорити 12 липня, коли кандидат на посаду керівника ФБР Крістофер Рей брав участь у слуханнях Сенату щодо призначення нового очільника Бюро. Тоді сенатор-республіканець Ліндсі Грем попросив його дати оцінку закидів про втручання України у перебіг виборчої кампанії 2016 у США. Відповідну інформацію ще на початку цього року почало поширювати видання Politico у статті «Спроби України саботувати Трампа нашкодили їй самій».

У ній йшлося про те, що колишній співробітник посольства України у США Андрій Теліженко заявив, що посольство, буцімто, тісно співпрацювало з Александрою Чалупою. Ця жінка є американкою українського походження та тісно пов'язана із Демократичною партією США та наче допомагала партії збирати викривальні матеріали щодо члена виборчого штабу Трампа Пола Манафорта.

«Розслідування видання Politico виявило, що американка українського походження, яка консультувала DNC, зустрічалась із високопосадовцями посольства України в Вашингтоні з метою викрити зв'язки співробітника виборчого штабу Трампа, Пола Манафорта, з Росією, відповідно до повідомлень людей безпосередньо обізнаних з ситуацією. Вам відомо про ці звинувачення?», – запитав Грем у Рея.

На це Рей відповів, що про цю ситуацію йому нічого не відомо, однак він готовий взятися за цю проблему.

Пізніше того ж дня речниця Білого дому Сара Сандерс знову порушила цю тему, коли відповідала на запитання щодо втручань Кремля у вибори 2016 року та спробу російської влади допомогти перемогти Трампу. Тоді вона заявила, що змова Демократичної партії з українською владою у цьому контексті була б більш ймовірною та має більше доказів.

«Якщо і є якісь докази змови під час минулих президентських виборів у США, то це – докази змови між Демократичною партією США та урядом України», – наголосила Сандерс.

(вгору)

Додаток 12

18.07.2017

Дарина Шварцман

Правительства манипулируют общественным мнением с помощью Twitter и Facebook

Во всем мире правительства привлекают «кибервойска» для манипуляции общественным мнением в социальных сетях, в частности Twitter и Facebook. Об этом говорится в докладе Оксфордского университета, сообщает Bloomberg (InternetUA).

Отмечается, что исследователи обнаружили 29 стран, которые используют социальные сети для формирования общественного мнения не только внутри страны, но и за ее пределами. В список попали Великобритания, США, Израиль, Австралия, Мексика, Аргентина, Филиппины, Россия, Турция, Венесуэла.

«В социальных медиа пропагандистские кампании получаются намного сильнее. Они стали потенциально более эффективными, чем в ранее, – говорит автор доклада Исследовательского проекта Oxford's Computational Propaganda Саманта Брэдшоу. – Я не думаю, что люди понимают, когда именно правительства используют эти инструменты. Все очень скрыто».

Задания «кибервойск», поддерживаемых правительством, варьируются от написания комментариев к постам и сообщениям в Facebook и Twitter, до индивидуального подхода к человеку. Для распространения информации правительства часто используют фейковые аккаунты и ботов.

В докладе говорится, что в Мексике и России политические силы используют как ботов, так и настоящих пользователей для нападения на журналистов и распространения дезинформации в социальных сетях. В британской пропагандистской кампании публикуются фальшивые видеоролики на YouTube, чтобы помешать мусульманам радикализоваться и присоединиться к войне в Сирии.

По словам Брэдшоу, правительства издавна использовали пропаганду, но цифровые инструменты сделали ее более сложной и эффективной. За последние несколько лет правительства переняли опыт активистов по использованию социальных сетей для распространения информации. И теперь частично применяют их методы. А интерактивные инструменты, такие как ПО для анализа данных, позволяют более эффективно адаптировать сообщения для определенных групп людей, максимизируя его влияние.

Twitter и Facebook отказались комментировать отчет.

(вгору)

Додаток 13

13.07.2017

Ольга Мінченко

Інтернет Асоціація України вважає, що в українському Інтернеті планують ввести цензуру

Впродовж поточного тижня здійснюється уже друга спроба включити до порядку денного сесії Верховної Ради України проект Закону України щодо протидії загрозам національній безпеці в інформаційній сфері (№6676 та №6688) (Watcher).

Ці Законопроекти є фактично тотожними і їх розгляд відбувається з грубим порушенням Регламенту ВР – вважають в Інтернет Асоціації України (ІнАУ). А при їх підготовці були проігноровані пропозиції експертного середовища.

У ІнаУ стверджують, що законопроекти містять «кращий досвід» КНДР, Ірану та РФ, а також повністю ігнорують досвід демократичних країн, в тому числі тих, які перебувають в стані війни (наприклад, Ізраїлю), або постійних терористичних атак:

– Законопроектами встановлюється, що СБУ може де-факто вводити воєнний стан в мережі Інтернет та телекомунікаціях та може здійснювати цензуру будь-яких ресурсів в мережі Інтернет поза судовою процедурою. Надання права СБУ забезпечувати тимчасове блокування (обмеження) та блокування доступу до визначеного (ідентифікованого) інформаційного

ресурсу (сервісу) дорівнюють заходам правового режиму воєнного стану, що визначені статтею 8 Закону України «Про правовий режим воєнного стану».

– Оголошується можливість введення санкцій в частині блокування доступу до інформаційних ресурсів відносно інформаційно-телекомунікаційних мереж (систем), які можуть належати приватним особам, громадським і політичним організаціям, бізнесовим структурам, банкам тощо.

– Введення в предмет регулювання Закону України «Про телекомунікації» суспільних відносин, пов'язаних з інформаційними ресурсами, інформаційними сервісами грубо порушує положення Статуту Міжнародного союзу електрозв'язку, ратифікованого Законом України «Про ратифікацію Статуту і Конвенції Міжнародного союзу електрозв'язку» № 116/94-ВР від 15.07.94 р.

– Законопроект фактично легалізує діяльність на ринку телекомунікацій нелегальних суб'єктів поза межами державного регулювання та контролю.

– Законопроект покладає повноваження, непритаманні для сфери телекомунікацій, на Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації, в частині ведення Єдиного реєстру виконання судових рішень. При цьому створюється негативний прецедент виконання судових рішень, нехтуються положення статті 129-1 Конституції України.

– Законопроект юридично прирівнює повноваження звичайного слідчого районного рівня або прокурора до рішення Ради національної безпеки і оборони України в частині застосування санкцій щодо блокування інформаційних ресурсів (сервісів).

– Законопроект містить численні грубі помилки технологічного характеру, наприклад: «доменні імена», «лінії доступу або вузли мережі Інтернет, які містять інформацію, поширення якої в Україні заборонене», «покажчики сторінок сайтів у мережі Інтернет» тощо, що свідчить про вкрай низку обізнаність авторів щодо сутності сфери телекомунікацій,

– Законопроект прирівнює рішення звичайного слідчого районного рівня або прокурора до рішення суду в частині блокування (обмеження) доступу до інформаційних ресурсів (сервісів).

– Положення законопроекту грубо порушують положення Регламенту міжнародного електрозв'язку від 9 листопада 1988 р., яким керуються 192 держави-члени Міжнародного союзу електрозв'язку, щодо вимог припинення пропуску всіх видів трафіка до/від телекомунікаційних мереж суб'єктів господарювання, до яких застосовано відповідні санкції.

– Законопроект вимагає покласти безпрецедентний фінансовий тягар на понад 6000 операторів, провайдерів телекомунікацій, а також на ВСІХ суб'єктів господарювання в Україні, які використовують міжнародні канали електрозв'язку (мережу Інтернет сьогодні використовують всі!!!) в частині зобов'язань за власні кошти закуповувати та встановлювати технічні засоби, які відповідають технічним вимогам, визначеним Адміністрацією Державної служби спеціального зв'язку та захисту інформації України за погодженням зі

Службою безпеки України, необхідні для блокування доступу до інформаційних ресурсів (сервісів).

– Автори законопроекту пропонують запровадити положення щодо обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування, що прямо порушує Конституцію України.

– Автори законопроекту пропонують вкрай незбалансовані, «драконівські» адміністративно-господарські санкції, наприклад, за ненадання операторами, провайдерами телекомунікацій документів, інформації щодо предмета перевірки на письмову вимогу посадових осіб Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, – штраф у розмірі 1 відсотка від доходу, отриманого суб'єктом господарювання від надання телекомунікаційних послуг за попередній календарний рік.

– Законопроектом пропонується прирівняти виключні підстави, які визначені частиною другою статті 34 Конституції України щодо обмеження права на вільне використання та поширення інформації, до випадків будь-якого кримінального провадження. Це беззаперечно перетворює незалежну і демократичну України на поліцейську державу у самому поганому сенсі.

При цьому в ІнАу стверджують, що в разі прийняття законопроекту, користь від цього отримає низка гравців ринку. Зокрема:

– представники тих політичних сил, які бояться політичної конкуренції і роблять ставку на інтернет-цензуру;

– спецслужби, які отримають надзвичайні повноваження, які перевищують повноваження, що проваджуються під час воєнного стану;

– нечесні чиновники, які неодмінно скористаються закладеними в Законопроектах новими можливостями корупційного тиску на бізнес;

– кілька крупних операторів, значна частина котрих контролюється російським капіталом, які отримають нагоду монополізувати український ринок телекомунікацій, витіснивши з нього інших гравців;

– кілька закордонних виробників обладнання з аналізу трафіку, яке, незважаючи на високу вартість, не гарантує повного блокування і залишає масу можливостей для його обходу;

– зовнішній агресор, якому вдається нав'язати України свої «підходи до забезпечення інформаційної безпеки», і який неодмінно скористається плодами невдоволення українських громадян.

Хто програє:

– українські абоненти, які отримають нові платіжки за доступ в Інтернет, де будуть закладені не тільки всі кошти на закупівлю додаткового обладнання, але й багаторазово збільшені апетити створених владою монополістів;

– український бюджет, який не отримає податкових відрахувань від кількох тисяч сумлінних вітчизняних провайдерів і десятків тисяч їх працівників, котрі замість сплати податків підуть за виплатами по безробіттю;

– галузь ІКТ – одна з небагатьох надій вітчизняної економіки на вихід з перманентної кризи, значна частина якої вже знищена і змушена емігрувати за

кордон через багаторазові випадки вилучення серверного обладнання силовиками з переважно корупційною метою;

– чесні політики і громадськість, яким надбання Революції гідності підміняють диктаторськими законами в стилі Януковича;

Інтернет Асоціація України стверджують, що закладені у Законопроектах новації не зменшать агресивний вплив РФ на інформаційний простір України.

(вгору)

Додаток 14

12.07.2017

В Android обнаружили скрытый «режим паники» для борьбы с вирусами

Пользователи Android регулярно оказываются в опасности из-за разных вредоносных приложений. Существует несколько типов вирусов: одни крадут личные данные, включая информацию о банковских карточках, другие отправляют платные SMS, третьи скачивают в фоновом режиме другие приложения для накрутки рейтингов и т.д. Совершенно неожиданно разработчики с популярного сайта XDA выяснили, что в последних версиях Android компания Google добавила скрытый «режим паники» для борьбы с вредоносными приложениями (InternetUA).

Новая функция получила название «Обнаружение паники». Интересно, что сама компания никогда её официально не представляла и нигде не упоминала о ней. Данная опция отслеживает то, как пользователь нажимает на системную кнопку «Назад». Режим «паники» активируется, если нажать эту кнопку как минимум четыре раза подряд с задержкой не более 300 мс. Дело в том, что в коде Android прописано, что система резервирует период задержки в 300 мс после нажатия кнопки «Назад» для принятия решения о том, хочет ли пользователь вернуться к предыдущей странице или же это сигнал для запуска «режима паники».

Если пользователь запустил этот «режим паники» многократными быстрыми нажатиями кнопки «Назад», то система понимает это и определяет, какое приложение было запущено в данный момент, блокирует его и возвращает пользователя на главный экран, чтобы тот мог удалить вредоносную программу.

Важно отметить, что данная функция работает только с Android 7.1 и более поздними версиями. При этом даже наличие нужной прошивки не гарантирует, что опция включена на устройстве. Проверить это можно в файле config.xml в SystemUI APK.

(вгору)

Додаток 15

12.07.2017

Новый троян напал на WhatsApp, Skype, Viber и Telegram. Под угрозой полмиллиарда смартфонов

Программа SpyDealer способна перехватывать SMS, звонки, делать снимки со встроенных камер и собирает личные данные о пользователях зараженных устройств. Судя по всему, это шпионский инструмент узконаправленного действия (InternetUA).

«Хочу все знать»

Эксперты Palo Alto Networks выявили новую троянскую программу для Android, способную воровать личные данные из коммуникационных приложений и телефонных звонков.

Троянец способен обеспечивать для зараженных им приложений административные привилегии с помощью эксплойтов из коммерческого приложения Baidu Easy Root, и этим обеспечивает себе возможность сбора данных и защищает себя от попыток удаления.

После установки вредонос регистрирует в системе два приемника, которые, в свою очередь, регистрируют загрузки устройства и статус беспроводного соединения. При первом запуске троянец считывает данные настроек из локального файла readme.txt – это IP-адрес командных серверов, а также функции, которые разрешено выполнять при подключении к сотовым сетям и/или к Wi-Fi.

Поскольку принимающая функция имеет более высокий приоритет, нежели используемое по умолчанию коммуникационное приложение, SpyDealer может получать команды от командного сервера прямо с помощью SMS-сообщений. Он также создает TCP-сервер на скомпрометированном устройстве и «слушает» порт 39568. В определенных условиях он может устанавливать активные соединения через UDP или TCP.

Всего троянец может выполнять более полусотни различных команд. В частности, как отмечают исследователи, троянец способен красть данные из популярных мессенджеров WeChat, WhatsApp, Skype, Line, Viber, QQ, Tango, Telegram, Sina Weibo, Tencent Weibo, из приложения, Facebook, предустановленного браузера Android, браузеров Firefox и Oupeng, почтовых клиентов QQ Mail, NetEase Mail, Taobao и Baidu Net Disk.

Для перехвата отдельных сообщений вредонос использует штатную функцию Android AccessibilityService.

Джентльменский набор шпиона

Проникнув на устройство, он собирает и переправляет на контролирующие серверы все доступные личные данные, в том числе номер телефона, данные IMEI, IMSI, сообщения SMS и MMS, список контактов, историю телефонных звонков, географическое местоположение и информацию о текущих соединениях Wi-Fi.

В некоторых случаях он может принимать телефонные звонки с определенного номера, записывать разговоры, делать скриншоты и снимки с помощью передней и тыловой камер.

– Все вместе это выглядит как «джентльменский набор» шпионских инструментов, причем, скорее всего, разрабатывавшийся для весьма избирательного применения, вплоть до слежки за конкретными лицами, – считает Ксения Шилак, директор по продажам компании SEC Consult. – На это, в частности, может указывать то, что часть жертв могла заразиться через скомпрометированные беспроводные сети.

Действительно, эксперты Palo Alto отмечают, что вредонос не распространяется через приложения в официальном магазине Google Play Store (но ничего не говорят об альтернативных источниках приложений) и что как минимум некоторые пользователи в Китае были заражены через скомпрометированные Wi-Fi-соединения, которые могут встречаться как в публичных кафе, так и в отелях любой «звездочности».

То, что создатели троянца более всего заинтересованы именно пользователями, располагающимися на территории Китая, указывает и то, что он атакует коммуникационные приложения, наиболее распространенные в КНР, и то, что большинство его контрольных серверов располагаются имеют китайские IP-адреса (несколько штук, правда, располагаются на территории США).

Есть и еще один значимый фактор: в то время как первый перехваченный сэмпл SpyDealer датирован 2015 г., по-настоящему эффективен он только на устройствах под управлением Android 2.2.x-4.4.x, а последнее обновление к версиям 4.4.x датировано 2013 г. В 2015 г. актуальной была пятая версия Android, вышедшая в конце 2014 г.

С другой стороны, распространение новых операционных систем среди пользователей происходит ощутимо медленнее, чем их выпуск, и по состоянию на июнь 2017 г. доля версий до 4.4.x включительно весьма высока - около 25%. Версия 5.0 обогнала 4.4 по популярности только весной 2016 г., так что на момент своего предполагаемого запуска SpyDealer атаковал наиболее распространенные версии мобильной ОС.

Таким образом, из примерно 2 млрд работающих в мире Android-устройств, под ударом SpyDealer находятся около 500 млн.

SpyDealer может собирать довольно значительное количество данных и на версиях от пятой и выше, но реализованные в них защитные механизмы препятствуют выполнению функций, требующих повышенных привилегий.

Разработка троянца, судя по всему, активно продолжается, так что нельзя исключать, что пользователи коммуникационных приложений под более новыми версиями Android скоро также могут оказаться под угрозой.

(вгору)

Додаток 16

12.07.2017

Эксперты раскрыли подробности о кибератаках на электростанции в США

На прошлой неделе в СМИ появилась информация о расследовании кибератак на энергетический и ядерный секторы США, в осуществлении которых подозревается Россия. Ажиотаж возник после того, как Министерство внутренней безопасности США и ФБР разослали энергетическим компаниям предупреждения об активизировавшейся хакерской активности (InternetUA).

Главным подозреваемым в атаках является группировка Energetic Bear, также известная под названиями Dragonfly и Crouching Yeti. Группировка активна с 2010 года и осуществляет атаки на предприятия электроэнергетического сектора по крайней мере с 2014 года. Многие решили, что атаки, о которых предупредили американские власти, аналогичны атакам на электроэнергетические компании Украины, ставшим причиной обесточивания целых районов городов в 2015-2016 годах. В ходе атак использовалось специальное вредоносное ПО BlackEnergy (2015 год) и Industroyer (2016 год).

О том, какую опасность на самом деле представляют атаки на американские компании, сообщили эксперты Cisco Talos в пятницу, 7 июля. По словам специалистов, речь идет о фишинговых рассылках, с помощью которых хакеры пытались похитить учетные данные для авторизации в локальных сетях.

С мая 2017 года Energetic Bear стала рассылать сотрудникам электроэнергетических компаний вредоносные электронные письма с файлами DOCX, замаскированными под резюме от соискателей работы. Как показал первоначальный анализ, вложенные файлы были безвредными, так как не содержали ни макросов, ни эксплоитов. Однако по чистой случайности исследователи вдруг обнаружили нечто подозрительное. Эксперты обратили внимание на интересное сообщение о статусе при загрузке Microsoft Office. Благодаря ему исследователи увидели, что DOCX-файл незаметно загружал с удаленного сервера шаблон Word.

Как показало дальнейшее исследование, DOCX-файл пытался установить соединение с удаленным SMB-сервером. С помощью подключения локального хоста к удаленному SMB-серверу злоумышленники пытались обманным образом выманить у компьютера учетные данные для локальной сети. Этот фокус отнюдь не является новым и уже давно используется хакерами.

По словам экспертов, на момент проведения исследования большая часть задействованных в атаках серверов и инфраструктуры уже были отключены, а значит, хакеры постарались как можно скорее замести свои следы.

(вгору)

Додаток 17

12.07.2017

Новая версия банковского трояна для Windows атакует пользователей Mac

Специалисты компании Trend Micro обнаружили новое вредоносное ПО, ориентированное на пользователей компьютеров Apple. Вредонос, получивший название OSX_DOK, представляет собой модифицированную версию

банковского трояна Werdlod, разработанного для систем на базе Windows. Преимущественно OSX_DOK атакует клиентов швейцарских банков (InternetUA).

Как считают исследователи, вредоносная кампания OSX_DOK является частью операции Emmental, о которой впервые стало известно в 2012 году. В рамках Emmental злоумышленники пытались получить полный контроль над банковскими счетами пользователей в Швейцарии, Швеции, Австрии и Японии с помощью различных инструментов и техник, таких как фишинговые атаки, вредоносное ПО и мошеннические DNS-серверы.

Распространение трояна OSX_DOK осуществляется с помощью фишинговых писем, содержащих вредоносные фалы с расширениями .zip и .docx. Файл .zip представляет собой фальшивое приложение для macOS, а второй файл содержит троян Werdlod и используется для атак на системы под управлением Windows. Обе программы работают как банковские трояны и обладают схожим функционалом.

Оказавшись на системе, вредоносная программа удаляет стандартное приложение App Store и запускает поддельное окно обновления macOS, запрашивающее пароль администратора. Получив учетные данные, вредонос инициирует загрузку других приложений и генерирует фальшивые сертификаты для атаки «человек посередине».

Вредонос автоматически закрывает браузеры, чтобы установить сертификат. Каждый раз, когда пользователь пытается подключиться к сайту швейцарского банка, домен которого содержится во вшитом в код трояна списке, на экране отображается фишинговая страница для кражи учетных данных.

(вгору)

Додаток 18

12.07.2017

Хакеры использовали серверы итальянского банка для майнинга криптовалюты

Серверы одного из итальянских банков использовались хакерами для добычи криптовалюты. Об этом рассказал директор компании Darktrace Дэйв Палмер (Dave Palmer) в рамках выступления на прошедшей в Лондоне конференции Research and Applied AI Summit, пишет издание Quartz (InternetUA).

Инцидент произошел в 2015 году. Тогда экспертов компании пригласили расследовать возможное вмешательство в системы одного из итальянских банков. Специалисты выявили потоки данных, которые отправлялись с серверов финорганизации на ботнет, управляемый европейским преступным синдикатом. По словам Палмера, под видом клиентских данных скрывалась довольно «дырявая» реализация программного обеспечения для майнинга криптовалюты биткойн. Скомпрометированный банковский сервер был быстро

обнаружен и отключен. Как пояснил Палмер, он проработал под управлением синдиката не больше часа после старта добычи биткойн. «Не думаю, что им удалось много заработать», – отметил он.

По его словам, 2014 год стал периодом расцвета криминальной добычи криптовалюты. «Это было модно заниматься майнингом монет наряду с рассылкой спама», – говорит Палмер. Случаи, когда для подобной деятельности использовались банковские серверы, были довольно редкими, поскольку в основном хакеры ориентировались на ПО для майнинга криптовалют, работающее на ноутбуках и стационарных компьютерах.

Эксперт не смог привести точную статистику за минувшие годы, но отметил, что сейчас число подобных инцидентов снизилось в разы. Если раньше специалисты сталкивались со случаями майнинга криптовалюты чуть ли не ежедневно, то за последние шесть месяцев компания выявила только 24 таких случая.

В 2014 году добыча криптовалюты была распространенным явлением, причем вычислительную мощь организаций «заимствовали» не только киберпреступники, но и сотрудники компаний, которые для этих целей использовали рабочие ноутбуки. Некоторые служащие даже покупали собственные серверы и прятали их в корпоративных дата-центрах, таким образом обеспечивая круглосуточную добычу монет.

Однако дни подобного майнинга уже позади, отметил Палмер. Сейчас для получения прибыли требуется слишком много вычислительной мощности. В экосистеме биткойн доминируют профессиональные организации с тысячами серверов, размещенных в гигантских складах специального назначения. С 2014 года необходимая мощность для майнинга возросла в 770 раз, что исключает возможность заработка на обычных ноутбуках.

(вгору)

Додаток 19

18.07.2017

Как защититься от вирусов-вымогателей и вирусов-разрушителей

27 июня 2017 в Украине была зафиксирована масштабная кибератака, которая одновременно поразила и блокировала деятельность десятков, а впоследствии и тысяч государственных и коммерческих структур страны (ITnews).

За первые трое суток в Национальную полицию Украины обратилось более 2 тысяч юридических и физических лиц с сообщениями о блокировании работы компьютерной техники в результате распространения вируса. С официальными заявлениями, по состоянию на 30 июня, в полицию обратились 309 организаций частного сектора и 111 организаций государственного сектора страны. Хакерская атака осуществлялась с использованием злоумышленниками вредоносной программы-разрушителя под названием Diskcoder.C (ExPetr, PetrWrap, Petya, NotPetya). Особенность действия вируса заключается в

поражении компьютеров и серверов под управлением ОС Microsoft Windows и предусматривает перезапись информации на жестких дисках.

В результате заражения компьютерного оборудования вирусом появлялось сообщение от кибермошенникам с предложением выплаты «выкупа» за разблокировку пораженных данных (приобретение ключа дешифрования) в размере 300 долларов в цифровой валюте – биткоины. Однако эксперты отмечают, что вредоносное программное обеспечение (ПО) Diskcoder.C не является «шифровальщиком» и не относится к категории «ransomware» (программ-вымогателей). Таким образом, поврежденные данные невозможно «расшифровать» и восстановить. Есть только возможность восстановить другие файлы, которые не попали под действие Diskcoder.C. Ключевая цель программы-уничтожителя заключалась в выведении компьютерного оборудования из строя и блокировании работы компаний. Поэтому, Diskcoder.C является наглядным примером того, что платить выкуп преступникам ни в коем случае нельзя. Попадание к кибермошенникам «на крючок» может обернуться не только потерей файлов, но и потерей средств.

Экспертами установлено, что поражение информационных систем украинских компаний преимущественно происходило через обновление программного обеспечения «M.E.Doc», предназначенного для отчетности и документооборота. По полученным киберполицией данным, которые подтверждены правоохранительными органами иностранных государств и международными компаниями, осуществляющими деятельность в сфере информационной безопасности, злоумышленники осуществили несанкционированное вмешательство в работу одного из персональных компьютеров компании-разработчика указанного программного обеспечения.

Специалисты отмечают, что атака Diskcoder.C, начатая 27 июня, имела предшественников. Начало системных нападений на «украинские компьютеры» – это первые атаки, которые были осуществлены в марте-апреле 2017 года (когда происходило как заражение компьютеров вирусом-шифровальщиком с помощью писем, якобы, от Государственной налоговой службы, или от банка). Специалисты отмечают ряд схожих признаков, которые связывают весенние атаки, атаку Diskcoder.C, а также кибернападения на объекты критической инфраструктуры в Украине, совершенные за последние несколько лет.

С каждым годом вопрос безопасности данных становится все более весомым как для организаций различных масштабов и отраслей, так и для каждого отдельного пользователя. Эксперты Украинской межбанковской Ассоциации членов платежных систем ЕМА подчеркивают важность донесения информации о необходимости принятия превентивных мер и последствиях уплаты «выкупа» киберпреступникам, принимая во внимание опыт последних массовых кибератак в Украине и мире, связанных с применением злоумышленниками вирусов-разрушителей и вирусов-вымогателей.

Для защиты компьютерного оборудования от программ-уничтожителей (в частности вредоносного ПО Diskcoder.C) специалисты советуют:

Все то, что может быть причастно к фазе инициации атаки вирусом (как правило это: сервер/ПК, «M.E.Doc», контроллер домена), необходимо отключить, сделать копии жестких дисков, переустановить. Перед этим подключаться к Интернету и локальной сети нельзя.

Изменить свои пароли к административным учетным записям на компьютерах и файерволах (при формировании пароля используйте как минимум 10 символов – 2 большие буквы, 2 маленькие буквы, 2 цифры, 2 символа. Не следует использовать обычные слова из словаря).

Изменить пароли к электронной почте и электронные цифровые подписи в связи с тем, что эти данные могли быть скомпрометированы.

Воспользуйтесь рекомендациями по восстановлению доступа к пораженной вирусом операционной системе, которые приведены на сайте Департамента киберполиции Национальной полиции Украины.

Сегодня вирусы-разрушители и программы-вымогатели являются проблемой международного масштаба, которая требует безотлагательного разрешения. По результатам первого квартала 2017 года, 6 из 10 вредоносных ПО составляли именно вирусы-вымогатели, По данным специалистов «Лаборатории Касперского», каждые 40 секунд коммерческие и государственные учреждения по всему миру подвергаются атакам вирусами-вымогателями, при этом индивидуальные атаки происходят каждые 10 секунд. Согласно прогнозам исследовательской компании Cybersecurity Ventures, ожидается, что в 2017 году глобальные потери в результате действий кибервымогателей будут превышать 5 млрд. долларов, по сравнению с суммой убытков в размере 325 млн. долларов в 2015 году.

(вгору)

Додаток 20

19.07.2017

Новый вирус превращает Android-смартфоны в шпионские устройства

Специалисты компании Trend Micro обнаружили на Android вирус, который получил название GhostCtrl. Он распространяется на пиратских сайтах с помощью APK-файлов, выдаваемых за популярные приложения и игры (Pokemon GO, WhatsApp и т.п.) (InternetUA).

После установки приложения вирус попадает в оперативную память, работает в фоновом режиме и полностью перехватывает управление устройством. Список возможностей GhostCtrl обширен:

– Контроль состояния Wi-Fi

– Управление Bluetooth и ИК-датчиком

– Мониторинг сенсоров устройства

– Активация различных режимов работы (экономия энергии, ночной режим, автомобильный режим)

– Управление вибромотором
– Скачивание файлов
– Установка новых обоев
– Переименование и удаление файлов и папок
– Передача файлов на удалённый сервер
– Удаление истории браузера
– Отправка SMS и MMS на любой номер
– Звонок на любой номер
– Распознавание речи и перевод её в письменный текст
– Выполнение команд, заданных удалённо и отправка отчётов на управляющий сервер
– Воспроизведение любых звуков
– Сброс паролей
– Запись видео и отправка записей хакерам

По всей видимости, вирус GhostCtrl создавался для прицельной слежки за конкретными пользователями, но может использоваться для массового сбора информации, интересной хакерам. Trend Micro советует пользователям обновить устройства до новейшей версии Android, а также воздержаться от установки приложений, скачанных из сомнительных источников.

(вгору)

Додаток 21

19.07.2017

Глобальная кибератака может привести к убыткам, как от природных катастроф

По оценкам аналитиков Lloyd’s of London, масштабная глобальная кибератака способна привести к экономическим потерям на сумму в 53 млрд долларов, что сопоставимо с ущербом от таких природных катастроф, как суперштorм «Сэнди», который поразил США в 2012 году (InternetUA).

В исследовании, проведенном совместно с компанией Cyence, специализирующейся на оценке рисков, были рассмотрены потенциальные экономические потери от гипотетического взлома провайдеров облачных сервисов и кибератак на компьютерные системы, управляющие предприятиями по всему миру, сообщает «Рейтер».

Экономические последствия от гипотетической атаки на облачного провайдера превосходят ущерб от недавней атаки вируса-шифровальщика WannaCry, поразившей более 100 стран по всему миру. Ущерб от последней в Cyence оценивают в 8 млрд долларов. При подсчете ущерба, как правило, учитываются убытки из-за простоя бизнеса и затраты на восстановление компьютеров.

Специалисты также упомянули вирус-вымогатель Petya, который в конце июня атаковал десятки компаний и организаций в Азии, Европе, Латинской

Америке, России и в Украине. Позднее «Лаборатория Касперского» нашла отличия от уже известного семейства вирусов Petya и назвала эту разновидность вредоносного ПО ExPetr. Экономический вред, причиненный данным вирусом, специалисты оценивают в 850 млн долларов.

В рассмотренном аналитиками сценарии атаки на облачный сервис хакерам удается внедрить в программное обеспечение облачного провайдера вредоносный код, который спустя год после заражения начнет вызывать системные сбои на компьютерах пользователей. За это время вредоносное ПО сможет распространиться и поразить большое число клиентов провайдера, от компаний, предоставляющих финансовые услуги, до отелей. В результате все они потеряют доход и понесут другие издержки, говорят специалисты.

В случае такого сценария экономические убытки от компьютерных сбоев могут варьироваться от 4,6 до 53 млрд долларов в зависимости от масштабов происшествий, однако фактические потери от подобного рода атаки могут достигнуть 121 млрд долларов, следует из доклада.

Аналитики предупреждают, что до 45 млрд долларов из предполагаемой суммы убытков могут быть не покрыты страховками из-за неполного страхования компаний на подобные случаи.

Также специалисты рассчитали, что масштабный взлом компьютерных систем, управляющих предприятиями по всему миру, может привести к потерям от 9,7 до 28,7 млрд долларов.

(вгору)

Додаток 22

18.07.2017

Расширение Particle для Chrome сменило владельца и тут же стало вредоносным

Специалисты сайта Bleeping Computer и пользователи популярного расширения Particle для Chrome обратили внимание на странное поведение некогда удобного инструмента (InternetUA).

Расширение Particle (ранее известное как YouTube+) представляло собой простой инструмент для смены UI и оптимизации работы с некоторыми стандартными функциями YouTube. Но, как это часто случается, со временем приоритеты разработчика поменялись, и в мае 2017 года он сообщил, что грядущие изменения YouTube UI представляют слишком большую проблему, поэтому он собирается оставить развитие Particle ради нового проекта Iridium.

Где-то между маем и серединой июля 2017 года у расширения сменился владелец, так как к оригинальному создателю Particle обратились представители некой компании, приложившие выкупить у него заброшенный инструмент. Автор расширения признается, что не смог отказаться от щедрого предложения. Теперь он пишет, что перед совершением сделки проверил будущего покупателя и убедился, что никаких «тревожных сигналов» не обнаружено. К сожалению, он также подписал соглашение о неразглашении

информации, которое теперь запрещает ему раскрывать имя компании, купившей Particle.

11 июля 2017 года в Chrome Web Store появилась обновленная версия Particle, и пользователи сразу заметили, что теперь расширение запрашивает новые, крайне подозрительные права: чтение и изменение информации на любых сайтах, а также управление другими приложениями, расширениями и темами. Лишь после этого автор оригинального Particle признался, что расширение сменило хозяев.

Изучая странное поведение обновленной версии, пользователи, исследователи Bleeping Computer и специалисты Emsisoft, которых попросили посмотреть, в чем дело, пришли к одинаковым выводам. Как выяснилось, в новой версии Particle появилась директория algoad, и расширение «научилось» осуществлять инжекты в код таких сайтов, как Google, Yahoo, Bing, Amazon, eBay, Booking.com и так далее.

После смены владельца, расширение Particle числилось в официальном каталоге, как принадлежащее пользователю roberthawkinsg. У него было еще два продукта, расширения Typewriter Sounds и Twitch Mini Player. Изучив отзывы о них, исследователи поняли, что эти расширения, по сути, являются adware и демонстрируют аналогичное вредоносное поведение.

У Particle насчитывалось более 31 000 пользователей, у Typewriter Sounds почти 40 000 пользователей, а Twitch Mini Player набрал почти 20 000 установок. В настоящее время все три расширения удалены из Chrome Web Store.

Разработчик оригинальной версии Particle извинился перед пользователями. Теперь он советует пострадавшим загружать Userscript-версию инструмента или дождаться релиза расширения Iridium.

(вгору)

Додаток 23

19.07.2017

Исследователь нашел необычный способ «угона» учетных записей Facebook

Исследователь Джеймс Мартиндейл (James Martindale) опубликовал в своем блоге интересный материал, озаглавленный: «Я вроде бы взломал пару аккаунтов Facebook, используя уязвимость, которую они не собираются исправлять». Мартиндейл действительно нашел способ перехвата управления над чужой учетной записью Facebook. Сделать это можно посредством функции восстановления аккаунта и старого телефонного номера владельца (internetua).

Проблема заключается в том, что старые телефонные номера, более не принадлежащие владельцам учетных записей, все равно остаются привязаны к аккаунтам Facebook. По сути, новый владелец телефонного номера может без каких-либо проблем войти в чужой аккаунт, без использования пароля, а при

желании может и вовсе сменить пароль на новый. Конечно, проблема не позволяет устраивать направленные атаки на конкретные учетные записи, однако даже это не умаляет ее критичности.

Исследователь связался с разработчиками Facebook, но ему ответили, что эта проблема не является багом. После этого ситуацией заинтересовались журналисты издания The Register, которые тоже связались с представителями Facebook и попросили их разъяснить, почему компания допускает подобное. Представители социальной сети сообщили, что «многие онлайновые сервисы позволяют людям использовать телефонные номера для восстановления [доступа] к аккаунтам. Мы призываем пользователей добавлять в список только актуальные телефонные номера, и если мы замечаем «подозрительную» попытку восстановления пароля, то можем запросить больше информации о пользователе».

Мартиндейл, в свою очередь, пишет, что представители Facebook не понимают или намеренно игнорируют самую суть проблемы. Дело в том, что, в отличие от других сетевых сервисов, Facebook позволяет пользователям привязывать к аккаунту сразу несколько телефонных номеров.

Сам исследователь обнаружил эту особенность совершенно случайно, когда оказалось, что новый номер его мобильного телефона ранее уже был связан с чьей-то учетной записью Facebook. Причем предыдущего владельца номера «скомпрометировала» сама социальная сеть. Facebook прислала на номер исследователя текстовое сообщение, в котором неактивному пользователю Facebook предлагали вернуться к использованию сервиса. Хуже того, вскоре Мартиндейл выяснил, что к той же учетной записи были привязаны еще пять других телефонных номеров.

Проблема состоит в том, что Facebook позволяет добавить к аккаунту новый телефонный номер, при этом не удаляя предыдущий, поэтому многие пользователи даже не догадываются о том, что старый номер вообще нужно удалять.

«Когда я начал свой эксперимент, я рассчитывал, что дойду до того момента, когда заставляю Facebook осуществить принудительный сброс пароля, а затем остановлюсь. Facebook удивил меня, позволив мне залогиниться, ничего не меняя. Я не знаю ни одного другого сайта, кроме Facebook, который позволил бы мне восстановить аккаунт при помощи телефонного номера, но без смены пароля», – рассказывает исследователь.

Мартиндейл пишет, что он проверил на «привязку к Facebook» множество телефонных номеров и часто ему везло, он обнаруживал и другие уязвимые аккаунты. При этом исследователь отмечает, что ни разу не сталкивался со срабатыванием защитного механизма, который призван замечать «подозрительные» попытки входа.

Исследователь резюмирует, что Facebook определенно нужно поработать над безопасностью. Как минимум, стоит сразу же уведомлять пользователей о необходимости удаления старого телефонного номера, в случае его смены. Также Мартиндейл отмечает, что «нельзя позволять людям восстанавливать

аккаунты, без принудительного сброса пароля и отправки уведомлений на все привязанные к учетной записи email-адреса и номера телефонов. Владельцы аккаунтов должны знать, что их пароли поменялись, чтобы они понимали, что кто-то без их ведома получил доступ к их профилям».

(вгору)

Додаток 24

21.07.2017

AVPass – инструмент для обхода антивируса на Android AVPass – инструмент для обхода антивируса на Android

Команда исследователей из Технологического института штата Джорджия (США) разработала хакерский инструмент под названием AVPass, который может изучать и обходить защиту антивирусных решений для смартфонов и планшетов под управлением Android. Проект разработан в рамках исследовательской инициативы по выявлению уязвимостей в алгоритмах машинного обучения, направленной на изучение того, как злоумышленники могут манипулировать данными технологиями в своих целях. AVPass включает три компонента: модуль для изучения возможностей обнаружения антивирусного решения, генератор вредоносного ПО, который генерирует несколько вариантов вредоносного кода и анализатор данных, обрабатывающий информацию и использующий ее для обхода защиты антивируса. По сути, инструмент препятствует обнаружению вредоносного ПО антивирусом, пояснил один из авторов проекта Макс Волоцки (Max Wolotsky) в интервью изданию DarkReading. AVPass отправляет фрагменты фальшивого вредоносного кода для проверки возможностей антивируса и на основе полученных данных модифицирует вредоносное ПО. «Мы выяснили, что большинство антивирусов обычно используют фиксированное число правил детектирования. К примеру, для обхода слабого антивируса достаточно обфусцировать только одну функцию», – заявил Волоцки. В процессе тестирования инструмент смог обойти почти все 56 антивирусов для Android на VirusTotal, за исключением решений AhnLab и WhiteArmour. По словам исследователей, разработанное ими решение работает не только на Android, но и на других платформах. В дальнейшем ученые планируют протестировать инструмент на компьютерах под управлением Windows (IT новости).

(вгору)

Додаток 25

24.07.2017

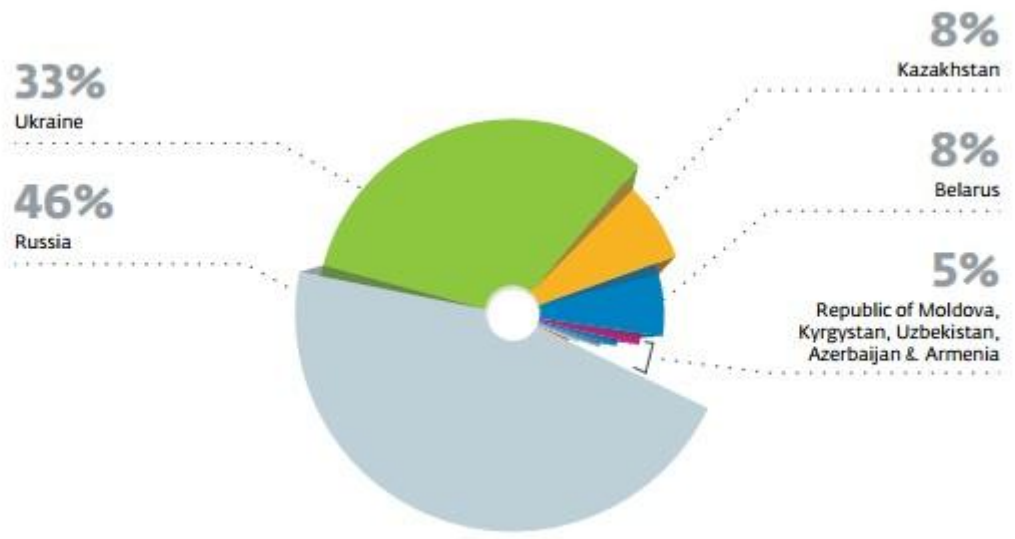
Павел Красномовец

ESET обнаружил adware-кампанию, поразившую более 100 000 устройств в Украине

Исследователи словацкой антивирусной компании ESET обнаружили adware-кампанию Stantinko, успешно действующую с 2012 года. С 2015 года злоумышленникам удалось заразить более 500 000 устройств. Больше всего пострадавших в Украине (33 %) и России (46 %) (AIN.UA).

Разработчики Stantinko монетизируют ботнет через установку расширений для браузера Chrome, которые вставляют рекламу и занимаются кликфродом (кликанием на рекламные объявления без ведома зараженного пользователя).

Однако вредоносный сервис Windows, который устанавливается на компьютер жертвы, позволяет хакерам выполнять любые действия. Исследователи отмечали случаи установки бота, проводившего массовый поиск в Google; инструмента для брутфорс-атак на панели администраторов Joomla и WordPress, с целью их взлома и продажи; полноценного бэкдора для управления зараженной системой.



Распределение заражения с 2015 года по странам. Изображение: ESET

Обнаруженная кампания также примечательна тем, что злоумышленникам удалось скрывать активность вредоносного ПО в течение пяти лет. Исследователи отметили старательную обфускацию (запутывание) и шифрования вредоносного кода и структуру вредоносного ПО, которое позволяло избежать обнаружения антивирусами долгие годы.

Один из сайтов, распространяющих пиратское ПО. При попытке скачать продукцию Microsoft загружается вредоносное приложение FileTour.

Загрузка Stantinko (вместе с сервисами Mail.Ru вроде браузера Amigo) на компьютер жертвы происходит через еще одно вредоносной ПО – FileTour. Оно, в свою очередь, распространяется через сайты с пиратским ПО вроде Microsoft Office или играми вроде Grand Theft Auto V иногда под видами торрент-файлов. FileTour устанавливает множество программ, отвлекая

внимание пользователя от загрузки компонентов Stantinko, которая происходит в фоновом режиме.

Главная функциональность Stantinko – установить два браузерных расширения для Chrome: The Safe Surfing и Teddy Protection. На момент проведения исследования ESET оба были доступны в магазине Chrome, однако сейчас уже удалены. На первый взгляд они выглядят как легитимные расширения, блокирующие нежелательные ссылки. Но во время установки они получают специальную конфигурацию, позволяющую заниматься кликфродом и встраиванием рекламы.

На видео видно, как с установленным The Safe Surfing при клике на ссылку в Rambler пользователь перенаправляется на другой сайт:

Перенаправление пользователя или встраивание рекламы позволяет операторам Stantinko зарабатывать на трафике, который они предоставляют рекламодателям. Кликфрод – одно из наиболее прибыльных занятий для киберпреступников. Согласно исследованию компании White Ops и Ассоциации национальных рекламодателей общий объем рынка кликфрода в 2017 году составит $6,5 млрд.

У Stantinko также есть специальный модуль для Facebook, который позволяет создавать через зараженные компьютеры аккаунты в соцсети, лайкать страницы и добавлять в друзья. Махинации с Facebook действительно выгодны, поскольку 1 000 лайков могут стоить около $15, хотя они и генерируются ботами.

Еще один способ заработка злоумышленников – использование ботнета из зараженных компьютеров для взлома панелей администраторов сайтов на базе Joomla или WordPress. С помощью специального модуля, устанавливаемого на компьютер жертвы, хакеры проводили брутфорс-атаки, пытаясь методом перебора найти пароль учетной записи администратора. При успешном взломе, данные могли перепродаваться в дарквебе.

В полном тексте исследования ESET (PDF) содержится список из взломанных сайтов, среди которых есть несколько украинских. К примеру, сайт Первомайского политехнического института, использующий Joomla.

В конце текста также имеется список файлов, ассоциирующихся с Stantinko. Но главным индикатором заражения является наличие расширений Teddy Protection и The Safe Surfing в браузере Chrome. Список установленных расширений можно увидеть здесь: chrome://extensions/.

Напомним, ранее мы публиковали инфографику с пошаговой инструкцией, показывающую как избавиться от тулбаров Mail.ru и «Яндекса».

(вгору)

Додаток 26

25.07.2017
Андрей Щербаков

Как обезопасить данные с мобильных гаджетов и быть уверенным в защите устройства

Мобильные гаджеты с каждым годом все больше проникают во все сферы человеческой жизни. Персональная информация и личная переписка, фото и видео файлы, доступ к финансам и почте – все это хранится в современных смартфонах. Вместе с ростом их популярности увеличивается и число заинтересованных грабителей. По статистическим данным, в 2016 году в Украине зарегистрировано около 105 тысяч заявлений о краже мобильных телефонов, из которых в суд попало менее 10 тысяч. Потерпевшие далеко не всегда обращаются в полицию, поэтому фактическое количество таких преступлений в разы больше. Например, почти 300 тысяч обращений абонентов с просьбой восстановления SIM-карты получил в прошлом году только один «Киевстар» (IGate).

Блокировка телефона сложным паролем, хранение в труднодоступных карманах, шифрование мессенджеров и файлов зачастую не помогает избежать неприятного инцидента с кражей или потерей телефона. Продумать надежные способы защиты с использованием современных технологий и полезных лайфхаков лучше сразу после покупки нового устройства.

Приложения «антивор»

Благодаря разработчикам и прогрессивным антивирусам специальных приложений для безопасности гаджетов становится все больше. Их обширный функционал предлагает большое количество вариантов защиты. Среди самых популярных:

– полная блокировка при удаленном включении статуса утерянного телефона;

– геолокация и дистанционное удаление и восстановление данных;

– сигнал сирены даже при выключенном звуке и вывод сообщения на экран;

– отправка письма с gps-данными и письма с фотографией при неверном вводе пин-кода.

Некоторые приложения могут при включении телефона проверить SIM-карту и в случае обнаружения нового номера — отправить сообщение, а также заблокировать кнопку питания телефона. Среди самых известных приложений-антиворов – Prey, AndroidLost, Cerbeus, Comodo Anti Theft и много других.

Программа защиты со страховкой

Кроме информации и файлов, большую ценность для пользователя представляет и сам смартфон. Вернуть его в случае кражи гораздо сложнее, чем удаленно восстановить данные.

В этом контексте в последнее время набирает популярность платная услуга украинских операторов, с помощью которой можно не только заблокировать телефон, но и вернуть его или же получить компенсацию. У "Киевстара", lifecell и Vodafone принцип услуги одинаковый: абоненту необходимо установить мобильное приложение с уникальным

идентификатором, разработанное международной компанией mySafety. Это дает возможность дистанционно управлять гаджетом, включая блокировку информации, получение gps-данных, размещение сообщений на экран и автоматическое получение данных о новой SIM-карте в телефоне. Выполнение всех команд приложения доступно в личном кабинете на веб-ресурсе и работает даже без включенного мобильного интернета.

Персональная заставка e-Sticker и специальная наклейка на телефон – ID Sticker содержат информацию о вознаграждении для человека, вернувшего телефон. При этом всю коммуникацию берет на себя оператор и компания mySafety, а телефон лично в руки владельцу передает курьер.

С таким приложением и мерами со стороны мобильного оператора возможность вернуть устройство увеличивается во много раз. Если же телефон безнадежно утерян и в течении 14 дней вернуть его не удалось, владелец получит компенсацию стоимости устройства от страховой компании на банковский счет.

Кроме функционального мобильного приложения, в ближайшее время разработчики планируют внедрить во все наклейки и брелоки чип NFC. В случае потери телефона, нашедший сможет получать всю необходимую информацию о вариантах возврата и получении вознаграждения, просто приложив свой смартфон к девайсу с наклейкой mySafety.

Функционал от производителя

В большинстве современных смартфонов есть встроенная функция защиты и поиска устройства, которая работает при условии включенного мобильного интернета. Владельцам Apple доступна служба Find My iPhone, которая определяет местоположение девайса, может воспроизвести звуковой сигнал, показать на экране сообщение с номером телефона, заблокировать гаджет и стереть с него все данные. Аналогично работают подобные сервисы и для других систем: Android Device Manager для поклонников Android и Find my phone для пользователей Windows Phone.

Не лишним будет также записать IMEI-код телефона и сфотографировать заводскую коробку с его изображением – это облегчит обращение в правоохранительные органы, если телефон все же украдут. Правда, в последнее время все чаще преступникам удается обойти встроенную защиту и получить доступ к содержимому устройства, поэтому ограничиваться только защитой от производителя не стоит.

Эффективнее всего работает комплекс из технических и тактических мер защиты телефона и информации в нем. Чем больше сложностей будет на пути потенциального вора – тем меньше вероятность того, что гаджет украдут.

(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.