СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(11.04–24.04)

2018 № 8

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(11.04–24.04)
№ 8

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 2018

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

11.04.2018

Instagram упростит поиск популярных страниц путем сканирования тегов

Разработчики социальной сети Instagram тестируют возможность перехода к страницам пользователей путем сканирования персональных тегов. Нововведение должно значительно упростить поиск популярных аккаунтов, в значительной степени повысив эффективность их продвижения (InternetUA).

Персональные теги представляют собой небольшие баннеры наподобие QR-кодов, используемых Snapchat для быстрого перехода к выбранным страницам. Правда, в отличие от конкурентов, Instagram позволит своим пользователям оформлять баннер со ссылкой более креативно, размещая на нем, помимо никнейма, эмодзи и стикеры.

Предполагается, что возможность создания персональных тегов в первую очередь заинтересует корпоративных пользователей. Они смогут размещать баннеры со ссылками на свои страницы в Instagram в местах максимального скопления людей и на фирменной продукции. Например, рестораторы дополнят тегом свои меню, а продавцы одежды напечатают их на этикетках.

На данный момент функция создания персональных тегов находится в стадии предварительного тестирования и недоступна подавляющему большинству пользователей. Instagram никак не комментирует данное нововведение, оставляя в секрете сроки его повсеместного релиза.

***

11.04.2018

Олег Дмитренко

Українська аудиторія «ВКонтакте» в березні знову зросла

Facebook та Instagram стали лідерами за приростом української аудиторії в березні. Місячне охоплення обох соцмереж в березні зросло на 2 %. Теж виросла, але не так різко, російська соцмережа «Вконтакте». Третій місяць поспіль падають «Одноклассники». Про це свідчать дані щомісячного дослідження аудиторії українського інтернету дослідницької компанії Фактум Груп (Watcher).

Загалом, серед найпопулярніших сайтів в Україні суттєвих змін не відбулось. Лідерами залишаються Google, YouTube та Facebook.

***

16.04.2018

Telegram снова работает без прокси и VPN. Дуров обошёл блокировку?

После непродолжительной блокировки у большинства российских провайдеров и операторов сотовой связи Telegram снова начал работать без использования прокси-серверов и VPN-сервисов. С чем это связано и как долго мессенджер продержится незаблокированным, пока непонятно. Веб-версия Telegram по-прежнему остаётся недоступной (InternetUA).

Операторы и провайдеры получили от Роскомнадзора поручение блокировать Telegram утром 16 апреля. 13 апреля Таганский суд Москвы разрешил Роскомнадзору запретить работу мессенджера в России из-за того, что тот не передал ФСБ ключи для расшифровки сообщений пользователей.

Павел Дуров обещал, что в Telegram будет встроен инструмент для обхода блокировок без прокси и VPN. Возможно, этот инструмент появился в приложениях заранее и был активирован. Об этом косвенно свидетельствует тот факт, что официальные клиенты Telegram не обновлялись на Android и iOS уже несколько недель.

***

16.04.2018

Социальная сеть Orkut 2.0 дебютирует в Индии как Hello.com

Шумиха вокруг скандала с передачей сведений о подписчиках крупнейшей соцсети фирме Cambridge Analytica и набирающее в этой связи силу движение «снеси Facebook», заставили зашевелиться когда-то главного конкурента Цукерберга на пути к мировому господству – Оркута Бьюккоктена (Orkut Büyükkökten) (Компьютерное Обозрение).

Этот бывший сотрудник Google в далёком 2004 г. создал соцсеть, скромно названную Orkut. Она была предшественницей родившегося в том же году проекта гарвардского студента «the Facebook» и стала одной из наиболее популярных соцсетей с 300 млн пользователей по всему миру.

Google закрыла Orkut в 2014 г., но теперь, как считает Бьюккоктен, его творение получило шанс на возрождение как «правильная соцсеть» под новым именем – Hello.

«Люди потеряли доверие к социальным сетям, и главная причина в том, что сегодня социальные медиа-сервисы не ставят пользователей во главу угла. Они отводят ему последнее место вслед за рекламодателями, брендами, третьими сторонами и акционерами. Их действиям не хватает прозрачности. Политика конфиденциальности и условия обслуживания больше похожи на черные ящики. Сколько пользователей на самом деле их читают?», – вопрошает Бьюккоктен.

***

17.04.2018

В WhatsApp появилась новая возможность

Разработчики WhatsApp добавили в мессенджер новую функцию, которая позволяет повторно загружать удаленные файлы. Об этом пишет ресурс Gadgets Now (InternetUA).

В данный момент если пользователь удаляет фотографию, видео или GIF-изображение из WhatsApp, то спустя 30 дней восстановить данные уже не получится. Благодаря новой функции удаленные файлы можно будет вновь загрузить. Пока эта возможность доступна только в бета-версии приложения для Android.

Контент, который пользователи загружают через WhatsApp, сохраняется в отдельной папке на устройстве. Теперь файлы будут храниться еще и на серверах мессенджера даже после удаления со смартфонов и планшетов. При этом данные владельцев аккаунтов будут защищены сквозным шифрованием.

***

22.04.2018

Facebook начал предлагать европейским пользователям включить технологию распознавания лиц

Сразу несколько пользователей Facebook из Европы рассказали о том, что социальная сеть начала предлагать им включить функцию распознавания лиц. Об этом, к примеру, можно прочитать в материале автора издания Metro Джимми Нсубуга. Ранее о планах перезапустить систему оповещений о публикации материалов с данными пользователей рассказал и заместитель директора по конфиденциальности компании Роб Шерман (InternetUA).

В оповещении говорится о том, что компания «работает над тем, чтобы сделать Facebook лучше, поэтому добавляет больше способов контролировать распознавание лиц, а не просто предлагать теги к фотографиям». В тексте также отмечается, что функция может быть отключена в любое время.

Раньше в настройках аккаунта не было отдельной опции, которая бы позволяла запретить социальной сети автоматически определять шаблоны лица пользователя. Однако в Facebook разъясняли, что эта функция и не требовалось – если пользователь удалял метку с фотографии, то эти данные не могли использоваться системой. Также если пользователь удалит метки со всех фото на Facebook, то у соцсети не будет сводной информации о нем, соответственно, системе не удастся создать шаблон его лица, который может использоваться при распознавании.

Решение предложить технологию пользователям было принято параллельно с судебным разбирательством об использовании данных лица без разрешения в США. В коллективный иск пользователей Facebook легла претензия о том, что социальная сеть собирает и сохраняет биометрические данные пользователей как часть «шаблона лица» без предварительного уведомления или согласия.

***

23.04.2018
Ирина Фоменко
Ключевые моменты новой политики данных Facebook

Пользователи Facebook уже давно жаловались, что настройки конфиденциальности и информация о сборе данных службы слишком сложны и их трудно найти. Стремясь уменьшить эту путаницу, компания опубликовала новое руководство, чтобы ознакомить пользователей с обновленной политикой сбора данных.

Докладніше

***

24.04.2018
Дмитрий Демченко
Facebook опубликовала свои секретные правила по работе с контентом

Facebook опубликовала ранее неизвестные общественности правила, по которым в компании работают с контентом. Таким образом, соцсеть предоставила намного больше деталей о запрещенных темах на своих платформах, чем когда-либо. Также компания разрешила подавать апелляции по решениям, принятым по конкретным постам.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

11.04.2018
Показания счетчиков воды передают через Viber в 160 городах и селах Украины

По данным Viber, на начало марта 2018 года этот мессенджер использовался в более чем 160 населенных пунктах Украины для сбора показателей квартирных счетчиков холодной и горячей воды (Компьютерное Обозрение).

С 2017 года мессенджер используют для сбора информации 15 водопроводных предприятий в Киевской, Николаевской, Днепропетровской, Житомирской, Харьковской, Полтавской, Черкасской, Херсонской, Львовской,

Черновицкой и Сумской областях. Выбор платформы не случаен: на сегодняшний день Viber установлен практически у каждого второго украинца.

Для подачи информации через Viber пользователю необходимо сохранить указанный на официальном сайте предприятия номер в списке контактов Viber и отправить в соответствующий чат номер лицевого счета или адрес пользователя (улица, дом, квартира), фамилию владельца дома или квартиры и текущие показатели. Эти данные необходимы для составления корректной квитанции на оплату.

***

11.04.2018

Возмущенные пользователи Facebook в знак протеста установили у Капитолия клонов Цукерберга

Возле здания Конгресса США в Вашингтоне, расположенного на Капитолийском холме, прошла акция Fix Facebook, что в перводе означает «Почини Facebook» (InternetUA).

Как сообщает Reuters, активисты Avaaz.org установили на зеленой лужайке возле Капитолия картонные копии основателя Facebook Марка Цукерберга.

Акция протеста вязана со скандалом в связи с тем, что британская аналитическая фирма Cambridge Analytica злоупотребляла большими объемами личных данных пользователей, полученных через Facebook. Эксперты полагают, что эта информация повлияли на результаты президентских выборов в США.

***

12.04.2018

У соцмережі відреагували на послання Трампа Путіну

Користувачі соціальних мереж припустили, що у президента США Дональда Трампа біполярні розлади або ж синдром роздвоєння особистості.

Приводом для цього стали нещодавні повідомлення глави Білого дому в Twitter, – передає Сегодня (zik).

У своєму першому повідомленні президент США закликає Росію гарненько підготуватися до удару «нових славних і розумних» американських ракет. Всього через 20 хвилин Трамп опублікував нове послання, в якому пропонує Москві дружбу, співробітництво і економічну допомогу.

Користувачі соціальних мереж реагували по різному. Дехто пропонував лідеру Кремля прислухатися до слів Трампа.

Інші – корелювали твіти американського президента з курсом рубля.

В основному ж користувачів цікавила причина такої різкої зміни тематики постів Трампа.

***

17.04.2018

«Самозаблокувалися»: У соцмережах продовжують знущатися над Роскомнадзором

Користувачі російського сегмента соцмереж продовжують висміювати Роскомнадзор, який безуспішно намагається заблокувати роботу месенджера Telegram (Інфотаб).

Особливою дошкульністю відрізняються жарти користувачів соцмереж щодо професійності дій відомства, адже, результатом блокування мільйонів IP-адрес стало те, що мешканцям РФ відкрився вільний доступ до деяких раніше заборонених сайтів, однак перестала працювати сторінка самого Роскомнадзора.

Як відзначає переважна більшість дописувачів, дії російської влади, у черговий раз наносять найбільшу шкоду самим росіянам.

Здобула популярність і фотографія глави Роскомнадзора Жарова, з «раритетними» телефонами за спиною.

Зазначимо, на сьогодні, за даними з реєстру заборонених сайтів Роскомнадзора, заблокованими є понад 16 мільйонів IP-адрес.

Варто зазначити, що на провальне блокування месенджера витратили вісім мільярдів рублів.

***

23.04.2018

У РФ пройшла акція на підтримку Telegram

У Росії 22 квітня користувачі Telegram провели акцію проти блокування месенджера Роскомнадзором (Українська правда).

Користувачі, які підтримали пропозицію від офіційного сервісного аккаунта месенджера, о сьомій годині вечора почали запускати з вікон паперові літачки.

Зазначається, що акція пройшла на підтримку вільного інтернету, приурочена до сьомого дня блокування Telegram в Росії.

Раніше біля будівлі ФСБ РФ паперові літачки запускали учасниця арт-гурту Pussy Riot Марія Альохіна і активіст Дмитро Ентео. Суд в Москві призначив їм за це по 100 годин громадських робіт.

***

23.04.2018

Павел Дуров назвал новую дату проведения акции протеста

Дуров оценил старания пользователей мессенджера и предложил повторить акцию протеста 29 апреля (InternetUA).

Об этом он рассказал на своей странице «ВКонтакте».

Кроме того, чтобы все смогли поддержать акцию правильно, создатель Telegram попросил ставить у каждой подобной публикации хэштег #sundaypaperplane. Кажется, скоро это станет еженедельной традицией по всей России.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

21.04.2018

Сколько придется заплатить за Facebook без рекламы?

11-14 долларов ежемесячно пришлось бы заплатить пользователям Facebook за использование социальной сети без рекламы, подсчитал TechCrunch. Переход сервиса на подписную модель является одним из возможных направлений его развития после скандала с утечкой персональных данных (InternetUA).

«Сегодня мы не предлагаем возможности отказаться от просмотра рекламы за плату, – говорит Марк Цукерберг, основатель социальной сети. – В целом, я полагаю, это было правильным решением, потому что далеко не все могут позволить себе платить реальные деньги за доступ к социальной сети».

Реклама является одной из основных статей дохода Facebook, поэтому отказ от ее размещения может сильно ударить по сложившейся за долгие годы модели монетизации социальной сети. Даже с учетом огромной аудитории Facebook компенсационная плата может оказаться непосильной для многих пользователей.

Идея переведения Facebook на подписную модель распространения возникла в результате утечки огромного массива пользовательских данных. Cambridge Analytica удалось завладеть личной информацией около 90 миллионов пользователей социальной сети, которые впоследствии были использованы для манипуляции общественным мнением.

***

20.04.2018

Facebook займётся разработкой собственных процессоров

Социальная сеть Facebook набирает команду специалистов для разработки собственных микрочипов. Об этом сообщает Bloomberg, ссылаясь на информацию, полученную от осведомлённых лиц, а также на перечень вакансий Facebook (InternetUA).

Отмечается, что инженерам предстоит заняться созданием «систем на чипе» (SoC) и «интегральных схем специального назначения» (ASIC). Кроме

того, в задачи войдёт работа с сопутствующим программным обеспечением и драйверами.

Наблюдатели полагают, что процессоры собственной разработки компания Facebook сможет применять в мобильных гаджетах, «умных» динамиках, а также в серверах для центров обработки данных. Использование специализированных чипов позволит улучшить совместимость программного и аппаратного обеспечения, а также снизить зависимость от сторонних поставщиков процессоров.

О сроках появления чипов Facebook ничего не сообщается. Социальная сеть обнародованную интернет-источниками информацию предпочитает не комментировать.

Нужно добавить, что разработкой фирменных чипов занимаются многие компании. В их число входят Apple, Google, Huawei, Samsung и другие.

***

22.04.2018

Twitter запретил рекламу «Лаборатории Касперского»

Сервис микроблогов Twitter запретил официальным аккаунтам «Лаборатории Касперского» публиковать рекламу в социальной сети, следует из открытого письма главы и основателя компании Евгения Касперского руководству американской компании (InternetUA).

«В конце января Twitter неожиданно уведомил нас о запрете на рекламу с наших официальных аккаунтов, где мы анонсируем посты с наших блогов по кибербезопасности (в том числе Securelist и Kaspersky Daily) и рассказываем пользователям о новых киберугрозах и методах борьбы с ними», – написал Касперский.

По его словам, сервис прислал письмо «Лаборатории», где утверждалось, что компания «работает по бизнес-модели, которая не соответствует стандартам приемлемой рекламы».

По словам Касперского, антивирусная компания направила официальное обращение в Twitter, однако более чем через два месяца американская компания прислала ответ «с тем же текстом».

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

18.04.2018

Как бороться со смартфонозависимостью: версия создателя iPod

Производителям смартфонов следует лучше осведомлять потребителей о рисках, связанных с чрезмерным увлечением гаджетами. Об этом в колонке для журнала Wired написал Тони Фаделл – бывший инженер Apple, один из авторов медиаплеера iPod.

Докладніше

***

21.04.2018

Чи заважають соцмережі складати іспити?

Невже багатозадачність підлітків сягнула такого рівня, що вони безболісно можуть відповідати на повідомлення в Snapchat, WhatsApp та Instagram, дивитися кумедні відео про тваринок у YouTube, та ще й вчитися?

Наближається гаряча пора підготовки до іспитів у школах та університетах. Батьки намагатимуться виховувати, прекрасно розуміючи – хоч би що вони сказали, суперечка, мабуть, неминуча.

Докладніше

***

23.04.2018

Разработчик придумал, как бороться с зависимостью от смартфона

Лучший способ преодолеть зависимость от смартфона – это принудительная блокировка, решили разработчики студии TeqTic и выпустили приложение LockMeOut. Разработка способна самостоятельно отключать большую часть функций устройства, сохраняя за пользователем только возможность принимать и совершать звонки (InternetUA).

В основе приложения, безусловно, лежит самосознание пользователя, который в курсе своей зависимости от смартфона, но не может с легкостью побороть ее. LockMeOut позволяет задать время дозволенной активности, по истечении которого аппарат просто заблокирует выбранные заранее функции и приложения на определенный срок.

Сколь бы странными ни казались методы борьбы с зависимостью, предложенные TeqTic, они могут быть достаточно действенными, особенно если установить LockMeOut на устройство ребенка. Тогда родители, предварительно защитив приложение паролем, смогут ограничивать время, которое их чадо проводит, глядя в экран.

Как вы уже, вероятно, догадались, приложение LockMeOut доступно только пользователям Android, поскольку Apple ни за что бы не позволила сторонней программе ограничивать функциональность iPhone. Владельцам же яблочной техники не остается ничего другого, как контролировать себя и своих детей самостоятельно.

Маніпулятивні технології

11.04.2018

Цукерберг отказался гарантировать невмешательство России в выборы в США

Во время выступления в сенате США глава Facebook Марк Цукерберг заявил о невозможности гарантировать, что Россия не сможет использовать социальную сеть для вмешательства в американские выборы (InternetUA).

«Сенатор, нет, я не могу гарантировать это [невмешательство России], поскольку у нас идет гонка вооружений. Пока будут существовать люди в России, работа которых вмешиваться в выборы, – будет продолжающийся конфликт», — сказал Цукерберг.

Ранее Цукерберг прокомментировал информацию о хранении в России данных, похищенных из Facebook.

***

14.04.2018

Пентагон: активність російських тролів зросла на 2000 %

Прес-секретар Пентагону Дана Уайт заявила, що активність російських інтернет-тролів за останні 24 години зросла на 2000 % (Українська правда).

Про це вона сказала на брифінгу 12 квітня, повідомляє CNN.

На брифінгу було представлено інформацію, пов'язану з повітряними ударами по об`єктах у Сирії США, Великобританії та Франції в на ніч на суботу.

«Російська кампанія з дезінформації вже почалася. За останні 24 години активність російських тролів збільшились на 2000 %, тому ми будемо тримати вас у курсі подій», – сказала Уайт.

Як відомо, в ніч на 14 квітня США, Велика Британія та Франція завдали авіаударів по військових об’єктах в Сирії, які пов’язують із зберіганням та виготовленням хімічної зброї.

***

20.04.2018

В Twitter фейки распространяются быстрее настоящих новостей

Исследователи Соруш Восау, Деб Рой и Синан Арал из Массачусетского технологического института проанализировали более 126000 фейковых новостей, которые были опубликованы в Twitter за все время его существования – с 2006 по 2017 годы, – чтобы оценить масштаб проблемы.

Докладніше

***

20.04.2018

Власник «фабрики тролів» відправляє політтехнологів до Африки

Вони працюють у країнах, де незабаром мають бути вибори.

На Мадагаскарі, в ПАР, Кенії і декількох інших країнах Африки, де найближчим роком або двома мають відбутися вибори, російські політтехнологи проводять моніторинг соціально-політичної ситуації і соціологічні дослідження (ТСН).

Про це повідомляє «Комерсант».

За інформацією видання, організовує їхню роботу Євген Пригожин, пов'язаний з російською «фабрикою тролів». На думку експертів, політтехнологи можуть заробити на експорті російських політтехнологій, але навряд мають намір вплинути на результат африканських виборів на користь РФ.

Як зазначається, у дослідженнях беруть участь в основному фахівці з Санкт-Петербурга. Учасники проекту не уповноважені давати коментарі ЗМІ і намагаються не афішувати свою роботу.

***

23.04.2018

В России распространяют фейк о сайте «Миротворец»

В российских СМИ появилась информация, что Госдепартамент начал использовать базу «Миротворца» для отказа россиянам во въезде на территорию Соединенных Штатов (InternetUA).

Об этом сообщается на странице сайта в Facebook.

В качестве примера приводится ситуация с примой-балериной Большого театра Ольгой Смирновой, которая находится в разделе «Чистилище» базы «Миротворца» из-за посещения Крыма. По этой причине, теперь ее не пустили в США, из-за чего гастроли Большого театра были сорваны.

В центре «Миротворец», в свою очередь, отмечают, что сведениями о нарушении Ольгой Смирновой государственной границы Украины или поддержки ею российской агрессии против Украины не располагают.

В центре «Миротворец» отмечают, что российская пропаганда пользуется тем, что сайт, на котором находится база всех, кто незаконно посещает Крым и поддерживает аннексию полуострова, запрещен в России и граждане РФ самостоятельно не могут проверить достоверность информации, которая появляется в росСМИ.

***

24.04.2018

В Facebook впервые раскрыли правила удаления постов

Руководство социальной сети Facebook впервые опубликовало внутренние правила, касающиеся правил, которыми должны руководствоваться сотрудники при удалении постов или блокировке пользователей (InternetUA).

Документ содержит в себе шесть глав: «Насилие и преступное поведение», «Безопасность», «Спорный контент», «Целостность и подлинность», «Соблюдение прав на интеллектуальную собственность» и «Запросы относительно контента». Среди причин, которые могут привести к удалению сообщения, относятся «правдоподобные угрозы», поддержка терроризма, признание в совершении пользователем или его сообщниками преступлений, размещение изображений обнаженного детского тела и явных изображений полового акта, призывы к травле и публикация личной информации других лиц.

В руководстве социальной сети отметили, что жесткость правил зависит от степени серьезности нарушения и персональной истории пользования Facebook.

Спецслужби і технології «соціального контролю»

14.04.2018

Еврокомиссия заинтересовалась конфиденциальностью в социальных сетях

Еврокомиссия намерена разобраться со сбором личных данных пользователей социальных сетей для использования в экономических или политических целях. Соответствующее решение было принято на фоне скандала с компанией Facebook, передавшей данные почти 87 миллионов пользователей британскому политическому консалтинговому агентству Cambridge Analytica (InternetUA).

«Когда платформа многомиллиардной социальной сети просто извиняется, этого недостаточно», – приводит источник слова председателя группы по защите данных ЕС Андреа Елинек (Andrea Jelinek).

Уже создается специальная рабочая группа. Ей предстоит изучить широко распространенную практику сбора персональных данных в социальных сетях. Группа должна сформулировать долгосрочную стратегию ЕС по этому вопросу.

25 мая в ЕС вступит в силу закон о конфиденциальности данных, который даст каждому европейцу право знать, какие данные о нем хранятся, и требовать удаления этих данных. Согласно новому закону, компаниям потребуется прямое согласие пользователя перед использованием его данных. Кроме того, объяснение, как будут использоваться данные, должно быть конкретнее, чем сейчас. Нарушителя может ждать штраф в размере до 4 % годового оборота (во все мире, не только в Европе).

***

16.04.2018

У Росії заблокували понад 2 млн IP-адрес Amazon та Google через месенджер Telegram

Роскомнагляд почав блокувати IP-адреси компаній Amazon та Google, хостинг яких використовує нещодавно заборонений в Росії месенджер Telegram (InternetUA).

Блокування з боку Роскомнагляду підтвердив російським пропагандистським ЗМІ глава відомства Олександр Жаров.

Станом на 21:00 16 квітня, за даними «Дождя», російська влада заблокувала понад два мільйони адрес.

«У нас на вивантаження надійшла підмережа Amazon, на яку перейшов Telegram. Річ у тім, що третій пункт рішення суду (про заборону Telegram- ред.) передбачає для Роскомнагляду не створювати умови для технічного доступу до заблокованого месенджеру. Ми виконуємо рішення», – заявив Жаров.

Про те, що Роскомнагляд додав у реєстр заборонених сайтів підмережі Amazon, першим повідомляв активіст Фонду боротьби з корупцією Владислав Здольник. На момент його публікації о 18:00 за Києвом було відомо про 800 тисяч заборонених IP-адрес.

IP-адреси Amazon та Google у Роскомнагляді блокують, адже їхні адреси використовує Telegram, аби обійти блокування.

За даними «Интерфаксу», Роскомнагляд також почав надсилати сповіщення про майбутні блокування власникам проксі-серверів, які дозволяють обходити заборону Telegram.

***

16.04.2018

Услід за Telegram у Росії можуть заблокувати Viber та WhatsApp – експерт // *Усі ці месенджери не передали ключі від шифрування державним регуляторам*

Услід за Telegram на території Російської Федерації в країні можуть також заблокувати не менш популярні месенджери, такі як Viber та WhatsApp. Про це заявив заступник керівника лабораторії комп'ютерної криміналістики Group-IB Сергій Нікітін, передає «Русскій Монітор» (mind).

Експерт вважає, що після рішення суду щодо блокування Telegram користувачі масово та невідкладно почали шукати шляхи вирішення питання у разі, якщо месенджер буде заблоковано раптово.

Нікітін дивується ажіотажу навколо Telegram, оскільки аналогічними месенджерами є Viber та WhatsApp, які, до речі, так само не передали ключі шифрування. Міністр зв'язку та масових комунікацій РФ Микола Нікіфоров

зазначив, що відомство має навіть більше претензій до Messenger від Facebook, Viber та WhatsApp, а тому є імовірність, що їх теж буде заблоковано.

Як зазначається, у Росії усі сервіси, які дають можливість обмінюватись повідомленнями, повинні бути внесені до Реєстру організаторів розповсюдження інформації. У разі ігнорування власниками цієї вимоги регулятори блокуватимуть до них доступ. Втім, якщо месенджери та соцмережі внесуть до відповідного реєстру дані про себе, вони будуть зобов'язані виконати ряд додаткових зобов'язань перед державою.

Соціальна мережа Facebook та WhatsApp, яким вона володіє, на даний момент не просто відсутні в реєстрі, а до того ж зберігають персональні дані громадян Росії в країні їх проживання. Таким чином, з формальної точки зору російського законодавства, вони порушують цілих 2 закони.

***

18.04.2018

«Роскомнадзор» перевірятиме Facebook, існує імовірність блокування соцмережі в РФ

«Роскомнадзор» анонсував проведення перевірки соціальної мережі Facebook, і, якщо до кінця 2018 року ключові вимоги російського регулятору не будуть виконані, постане питання про її закриття на території РФ. Про це заявив голова «Роскомнадзору» Олександр Жаров, передають «Ізвєстія» (mind).

«До кінця 2018 року ми проведемо перевірку компанії, і є кілька пунктів, які мають бути виконані: локалізація баз даних російських громадян на території Росії, видалення всієї забороненої інформації – а вони вже значно запізнюються за термінами – і дотримання інших законів», – сказав він.

Якщо вищезазначені пункти керівництвом Facebook виконані не будуть, постане питання щодо блокування програми в Росії.

Жаров також повідомив, що регулярно, раз на півроку, зустрічається з представниками Facebook.

«При цьому постійно чую: Жаров усе спускає з рук Facebook, тому що там є якісь особливі відносини. Немає жодних особливих відносин, під час останньої зустрічі з її представниками в лютому ми ще раз проговорили нашу позицію», – додав він.

***

18.04.2018

Microsoft, Facebook та ще 30 компаній підписали декларацію про відмову від участі в кібератаках *// Google, Apple та Amazon поки що до угоди не долучилися*

Більше 30 високотехнологічних компаній на чолі з Microsoft та Facebook підписали угоду про відмову від участі в кібератаках, які можуть бути організовані урядом будь-якої країни.

Докладніше

***

17.04.2018

Facebook грозит коллективный иск из-за технологии распознавания лиц

Федеральный суд в Калифорнии постановил в понедельник, что Facebook можно предъявить коллективный иск за использование технологии распознавания лиц без согласия пользователей (InternetUA).

Об этом пишет AFP.

Средство распознавания лиц, запущенное в 2010 году, предлагает имена людей, которых оно идентифицирует на фотографиях, загружаемых пользователями.

Истцы утверждают, что данная технология противоречит закону штата Иллинойс о защите биометрической информации.

Судья постановил, что для подачи иска есть достаточно оснований.

Пресс-секретарь Facebook сообщила, что компания изучает решение, при этом добавив: «Мы по-прежнему считаем, что дело не имеет перспектив и будем защищаться».

Facebook также утверждает, что с момента своего создания он был очень открытым, и позволял пользователям не допускать, чтобы их имена предлагали в тегах с фотографиями.

Эта технология была приостановлена для пользователей в Европе в 2012 году из-за опасений по поводу конфиденциальности.

***

18.04.2018

Российские санкции против соцсети Linkedin ударили по Газпрому

Запрет Роскомнадзором сети Linkedin в России осложнил Газпрому задачу поиска квалифицированных специалистов мирового класса, сократив источники поиска кандидатов (InternetUA).

Также осложняет ситуацию секвестирование количества кадровых агентств, привлекаемых для закрытия сложных вакансий, добавили собеседники агентства.

К примеру, формируемое в Санкт-Петербурге подразделение по трейдингу газа за год с момента начала своего формирования смогло укомплектовать штат (около 30 человек) примерно на десятую часть.

При работе над этими вакансиями кадровики Газпрома столкнулись также с несоответствием зарплатных ожиданий кандидатов из Европы финансовым лимитам, установленным в компании, а также дефицитом русскоговорящих кандидатов на рынке труда в России и Европе.

Linkedin была заблокирована в РФ еще в 2016 году, поскольку Роскомнадзор не получил от компании информации о локализации соцсетью персональных данных россиян на территории РФ.

***

18.04.2018

Французские власти разработали свою альтернативу WhatsApp и Telegram

Французское правительство приступило к тестированию собственного защищенного мессенджера, который будет хранить все данные официальных лиц внутри страны. Новый мессенджер призван обеспечить защиту от шпионажа за частными разговорами высокопоставленных чиновников правительства, сообщает информагентство Reuters (InternetUA).

Власти обеспокоены возможными утечками данных в случае, если информация шифруется в США или России. В настоящее время в тестировании нового мессенджера принимают участие только 20 чиновников, однако к лету использование сервиса станет обязательным для всех сотрудников правительства. Государственный мессенджер создан на основе открытого кода, доступного в сети, и в будущем его смогут использовать и рядовые граждане, рассказал источник. Собеседник агентства не уточнил, о каком коде идет речь, или как называется мессенджер.

Как отмечается, желание разработать собственный мессенджер может быть связано с приверженностью президента Франции Эммануэля Макрона сервису Telegram, который он и его соратники использовали для обсуждения рабочих вопросов в ходе предвыборной кампании. Однако ранее в этом году в связи с соображениями безопасности на рабочих смартфонах чиновников французского правительства были установлены инструменты, блокирующие доступ в WhatsApp и Telegram.

***

18.04.2018

Роскомнадзор в ярости: всё валится, а Telegram стоит, – правозащитник

Из-за действий Роскомнадзора многие россияне утратили доступ к банковским и торговым сервисам.

Попытка российских властей заблокировать мессенджер Telegram связана с желанием контролировать распространение информации в стране, заявил российский политик и правозащитник Лев Шлосберг.

Докладніше

***

18.04.2018

Павел Дуров объявил о старте движения «Цифровое сопротивление» и пообещал гранты держателям прокси и VPN

Основатель Telegram Павел Дуров подвёл итоги первых суток с начала блокировки мессенджера в России и пообещал наградить держателей прокси и VPN-сервисов. На выплаты в рамках движения «Цифровое сопротивление» он собирается потратить «миллионы долларов» в 2018 году.

Докладніше

***

23.04.2018
Владимир Кондрашов
ФБР ищет в Украине своего «контрагента»

Прокуратура США по Восточному округу штата Висконсин, Федеральное бюро расследований и Налоговая служба США проводят расследование относительно пользователя под псевдонимом «parkerproo». Хакера из Украины подозревают в нарушении уголовного законодательства США, а именно – в незаконном получении через компьютер персональных данных 1 тысячи человек, которые «parkerproo» рекламировал и продавал другим.

Докладніше

***

23.04.2018
Путин подписал закон о блокировке сайтов с порочащей честь информацией

Президент Российской Федерации Владимир Путин подписал закон о блокировке в интернете сведений, «порочащих честь и достоинство» гражданина или юридического лица. Соответствующий документ опубликован на официальном интернет-портале правовой информации РФ (InternetUA).

Таким образом, решение о блокировке вступает в силу в том случае, если владелец сайта не удалил «порочащие» данные в заданный судом срок.

Так, если портал не отреагирует на требование суда и откажется ограничить доступ к «порочащей» информации, судебный пристав на правовых основаниях сможет требовать блокировку интернет-ресурса.

В таком случае будет направлено письмо в Роскомнадзор, который в течение суток должен будет заблокировать сайт.

Как считают авторы законопроекта из «Единой России», он поможет «защите прав и законных интересов лиц, чьи честь, достоинство и доброе имя потерпели ущерб в результате распространения не соответствующей действительности негативной информации».

***

23.04.2018
У Великобританії посилять тиск на соцмережі

Міністр охорони здоров'я Британії Джеремі Хант заявив про можливість введення нових правил для соціальних мереж, якщо вони не вжиють необхідних заходів для захисту дітей онлайн. Про це повідомляє Reuters. За його словами, соцмережі не реагують на те, що порушуються правила щодо мінімального віку, допустимого для реєстрації нового користувача.

«Боюся, що ви колективно закриваєте очі на проблему того, що ціле покоління дітей передчасно піддається шкідливим ефектам соціальних мереж», – заявив він. У свою чергу, він не уточнив, які нові правила можуть бути введені відносно соцмереж. Міністр дав компаніям час до кінця квітня, щоб вони запропонувати способи скоротити час, проведений дітьми в соцмережі (Експрес).

Проблема захисту даних. DDOS та вірусні атаки

11.04.2018
7 млн пользователей загрузили фальшивые антивирусы из Google Play

Компания ESET сообщила, что ее специалисты обнаружили в Google Play 35 рекламных приложений, замаскированных под антивирусы. Подделки скачали в общей сложности до 7 миллионов пользователей.

Докладніше

***

11.04.2018
В файлы Word пробрался новый опасный вирус

Эксперты компании Menlo Security зафиксировали волну кибератак на финансовые и IT-организации. Нападение ведется новым многоступенчатым методом, использующим уязвимость Microsoft Word. Об этом сообщает издание TreatPost (InternetUA).

Вредоносные документы пересылаются на электронные адреса сотрудникам крупных корпораций в фишинговых письмах. Как правило, это файлы в формате docx, которые содержат специальные теги HTML с зараженными элементами. При попадании на устройство они активизируются и, в свою очередь, загружают новую ступень инфицирования машины – программное обеспечение FormBook.

FormBook является вредоносным алгоритмом, который может передать под контроль хакеров большую часть функционала компьютера: загрузку файлов, захват паролей, запуск различных программ и так далее.

Особенность новой волны атак в том, что для активации вредного вложения не требуется макрос. Уязвимость удаленного выполнения кода, которую используют злоумышленники, называется CVE-2017-8570, она связана с механизмом обработки объектов в памяти компьютера.

Кибератака нацелена на американские компании и фирмы, расположенные в ближневосточном секторе. Специалисты подозревают, что новый многоступенчатый механизм – продукт работы хакерской группировки Cobalt (также известна как Carbanak и Anunak), так как метод атаки на финансовые компании с помощью фишинговых писем является для них основным способом совершения киберпреступлений.

***

11.04.2018

Как проверить APK-файлы приложений для Android на вирусы

Популярный онлайн-сканер вредоносных программ и ссылок VirusTotal представил виртуальную песочницу Droidy для проверки приложений для Android на вирусную активность. Она позволяет еще до установки APK-файла выявить его способности к совершению звонков, отправке SMS, активации служб геолокации и майнингу (InternetUA).

Droidy работает в составе стандартного онлайн-сканера, который позволяет производить вирусную проверку файлов до 128 МБ включительно. Как правило, большинство установочных файлов не превышают максимальный объем, установленный разработчиками сервиса. При проверке URL-адресов это ограничение и вовсе не имеет значения.

Скрытые майнеры

VirusTotal придется весьма кстати пользователям, предпочитающим бесплатно скачивать платные приложения в виде APK-файлов из сторонних источников. Установка ПО, найденного вне официального каталога, сопряжена с риском заражения устройства. Известны случаи, когда создатели таких приложений использовали мощности гаджетов своих жертв для майнинга криптовалют, истощая тем самым их ресурс.

***

11.04.2018

Уязвимость в системах аварийного оповещения позволяет хакерам запускать ложные сигналы тревоги

Исследователи безопасности из компании Bastille обнаружили в системах аварийного оповещения серьезную уязвимость, позволяющую хакерам дистанционно активировать все сирены с помощью радиочастот (Центр информационной безопасности).

Сирены аварийного предупреждения используются во всем мире для уведомления граждан о стихийных бедствиях, техногенных катастрофах и

чрезвычайных ситуациях, таких как опасные погодные условия, сильные штормы, торнадо и теракты.

Атака, получившая название SirenJack Attack может быть осуществлена на сирены производства ATI Systems, которые используются в крупных городах, а также в университетах, военных и промышленных объектах США.

По словам исследователей, поскольку в радиопротоколе, используемом для управления уязвимыми сиренами, отсутствует какое-либо шифрование, злоумышленники могут проэксплуатировать данную уязвимость для активации сирен.

«Нужна лишь ручная радиостанция стоимостью $30 и компьютер», – отметили специалисты.

Для успешной эксплуатации проблемы хакер должен находиться в зоне досягаемости и идентифицировать радиочастоту, используемую целевой сиреной для отправки специально сформированного сообщения.

«Как только мы нашли нужную частоту, анализ радиопротокола быстро показал, что команды не были зашифрованы, а следовательно, уязвимы», – добавили специалисты.

***

11.04.2018

Странный вирус-вымогатель требует играть в PUBG

В сети появилась новая программа-вымогатель, которая, попадая на компьютер пользователя, зашифровывает всего его файлы, сообщается на сайте Bleeping Computer. Создатель вируса не требует от пострадавших денег: расшифровать файлы можно, поиграв несколько часов в онлайн-игру PlayerUnknown’s Battlegrounds (Центр информационной безопасности).

Программы-вымогатели часто распространяются благодаря уязвимостям в браузерах или маскируются под другие приложения, чтобы пользователь запустил установщик. Попадая на компьютер пользователя, такая программа обычно шифрует файлы или блокирует нормальную загрузку устройства.

Чтобы снять блокировку или расшифровать данные, пользователю обычно предлагается заплатить выкуп автору вируса, но новая программа-вымогатель вместо этого требует от пользователя поиграть в онлайн-игру. Вирус PUBG Ransomware блокирует файлы на зараженном компьютере, добавляя к ним расширение .PUBG. После окончания шифрования на экране появляется окно с предупреждением о том, что компьютер заражен, файлы на нем зашифрованы.

Программа также предоставляет код для восстановления: после окончания шифрования файлов его можно использовать – и дешифровать файлы обратно. Кроме того, редакторы Bleeping Computer, изучив исходный код программы, заметили, что на самом деле вирус не обращает внимание на то, сколько пользователь играл в игру, – он запускает дешифровку после того, как на зараженном компьютере был запущен файл TslGame.exe.

***

11.04.2018

Windows-ПК можно взломать, просто заставив жертву посетить сайт

10 апреля компания Microsoft выпустила плановые ежемесячные обновления безопасности для своих продуктов. Помимо прочего, патчи исправляют ряд критических уязвимостей, пять из которых позволяют злоумышленнику получить контроль над компьютером жертвы, лишь заставив ее посетить вредоносный сайт (Центр информационной безопасности).

Пять вышеупомянутых уязвимостей были исправлены в Windows Graphics Component. Проблемы связаны с некорректной обработкой встроенных шрифтов библиотекой шрифтов Windows и затрагивают все актуальные версии ОС от Microsoft, в том числе Windows 10 / 8.1 / RT 8.1 / 7 и Windows Server 2008 / 2012 / 2016. Все пять уязвимостей (CVE-2018-1010, CVE-2018-1012, CVE-2018-1013, CVE-2018-1015 и CVE-2018-1016) были обнаружены исследователем безопасности из Flexera Software Хоссейном Лотфи (Hossein Lotfi).

Злоумышленник может проэксплуатировать уязвимости, просто заставив жертву открыть файл или посетить сайт с вредоносным шрифтом. Жертве достаточно лишь открыть сайт в браузере, и атакующий получит контроль над ее компьютером.

В Windows Graphics Component также была исправлена уязвимость отказа в обслуживании, позволяющая атакующему вызвать сбой в работе системы.

Microsoft также выпустила исправления для критической уязвимости в Windows VBScript Engine (CVE-2018-1004), позволяющей удаленно выполнить код и затрагивающей все версии Windows. Для ее эксплуатации злоумышленник может заманить жертву на вредоносный сайт.

Уязвимости, позволяющие удаленно выполнить код и получить контроль над уязвимой системой, также были исправлены в Microsoft Office и Microsoft Excel. Еще шесть уязвимостей, включая три критические, были исправлены в Adobe Flash Player.

***

11.04.2018

Хакеры удалили самый просматриваемый клип на YouTube, коим был Despacito

10 апреля YouTube подвергся взлому: злоумышленники получили доступ к группе музыкальных каналов Vevo и удалили клип на песню Луиза Фонси и Дэдди Янки «Despacito» – самое просматриваемое видео за всю историю сервиса (IGate).

Хакеры заменили превью видео на изображение с вооружёнными людьми в костюмах и масках, а также оставили в описании к подмененном видео призыв «Освободите Палестину».

Помимо этого, неизвестные удалили ещё несколько популярных видео из YouTube. В списке пострадавших оказались клипы Криса Брауна, Шакиры, DJ Snake, Селены Гомес, Дрейка, Кэтти Пэрри и Тейлор Свифт. Некоторые ролики удалили полностью, а в других просто заменили описание и изображение предпросмотра.

Как отметило BBC News, один из предполагаемых хакеров, участвовавших в атаке на YouTube, написал в твиттере, что сделал это ради веселья: «Я просто использовал скрипт, меняющий названия музыкальных видео. Не судите меня, я люблю YouTube».

На данный момент удаленные видео восстановлены.

***

11.04.2018

Цукерберг отрицает сбор сведений о пользователях Facebook через микрофон

10 пареля начались слушания в американском сенате по делу об утечке пользовательских данных из Facebook. Марк Цукерберг давал свои показания. Один из вопросов касался сбора данных пользователей, и основатель социальной сети раскрыл некоторые подробности о методологии Facebook (InternetUA).

Сенатор Гэри Питерс прямо спросил: «Я слышал это много раз, в том числе от моего персонала. Правда или нет, что Facebook использует аудиофайлы с мобильных устройств для сбора личной информации о пользователях?» Цукерберг ответил: «Нет» и, «чтобы быть правильно понятым», пояснил, что имеет в виду.

По словам Цукерберга, информацию именно с микрофонов компания не использует. Но при этом люди загружают на Facebook видео, в которых обычно есть и голосовая речь. И звуковые дорожки из роликов компания уже использует в своих целях.

***

11.04.2018

Німеччина заявляє, що кібернапади на її урядові мережі організувала Росія

Експерти німецького Федерального відомства з охорони конституції стверджують, щао за кібернапади на комп'ютерні мережі уряду Німеччини відповідальна Росія (Espreso.tv).

Про це заявив керівник відомства Ганс-Георг Маассен, передає Deutsche Welle.

«Ми оцінюємо це як кібератаку російського походження», – заявив Маасен.

Водночас керівник німецької контррозвідувальної спецслужби зазначив, що у таких випадках не може бути 100 % точності під час встановлення справжнього винуватця кіберзлочину, тому не можна виключати й того, що хакери мали намір створити враження, що справжній організатор кібератак походить із Росії.

Попри це Маасен заявляє про «високу ймовірність» саме російського сліду в кібернападах.

***

11.04.2018

Новый интернет-стандарт избавит пользователей от ввода паролей

Консорциум Всемирной паутины (W3C) – организация, разрабатывающая единые стандарты веб-технологий, – и альянс FIDO (Fast Identification Online, быстрая идентификация онлайн) утвердили новый стандарт Web Authentication, позволяющий устанавливать личность человека без ввода учетных данных (InternetUA).

Это означает, что пользователи уже в скором времени смогут получить беспарольный доступ практически к любому онлайн-сервису, пройдя идентицикацию посредством сканера отпечатков пальцев, камеры или USB-ключа. Это снижает вероятность того, что кодовая фраза, скомпрометированная на одном сайте, может быть использована на другом.

Первой Web Authentication воплотила компания Mozilla в браузере Firefox. «В ближайшие несколько месяцев» она также будет реализована в Google Chrome и Microsoft Edge, сказано на сайте W3C. К инициативе намерена подключиться и Opera, однако о намерении Apple поучаствовать в реализации стандарта для Safari пока ничего не известно.

Многие пользователи предпочитают вводить один и тот же пароль для авторизации на разных сайтах. В конце прошлого года эксперты по защите данных компании SplashData составили рейтинг самых слабых и ненадежных кодовых фраз. На двух верхних строчках списка второй год кряду разместились «123456» и «password», популярность слова «football» резко упала, а «starwars» («Звездные войны») впервые попало в первую сотню, заняв сразу 16-е место.

***

12.04.2018

Firefox вслед за Chrome блокирует загрузку большинства FTP-подресурсов

Инженеры компании Mozilla решили пойти по стопам разработчиков браузера Google Chrome и начать блокировать загрузку FTP-подресурсов на

страницах, работающих по протоколам HTTP и HTTPS в программе Firefox. (InternetUA).

Под FTP-подресурсами подразумеваются файлы, загруженные через протокол FTP в теги img, script или iframe, которые имеют src = "ftp: //". При этом ссылки FTP, размещенные в обычных ссылках с тегом <a> или введенные непосредственно в адресной строке браузера, будут продолжать работать.

Решение связано с недостаточной безопасностью протокола FTP. Он не поддерживает современные методы шифрования и нарушает многие встроенные функции безопасности и конфиденциальности браузеров, такие как HSTS, CSP, XSA и пр.

Помимо этого, многие кампании по распространению рекламного вредоносного ПО часто полагаются на скомпрометированные FTP-серверы и перенаправляют или загружают вредоносы на компьютеры пользователей через подресурсы FTP.

По словам инженеров Mozilla, блокировка FTP-подресурсов появится в версии Firefox 61, выпуск которого запланирован на 26 июня 2018 года.

В сентябре минувшего года Google приняла аналогичное решение. Начиная с Chrome 63, браузер начал блокировать загрузку подресурсов FTP, а также отмечать ссылки FTP, доступные в адресной строке браузера, как небезопасные.

***

12.04.2018

Масове шахрайство з банкоматами: що варто знати українцям

Щорічно тисячі українців попадаються на вудку шахраїв, а пристрої для крадіжки інформацію стають все більш непомітними. За даними кіберполіції, в минулому році кількість крадіжок з банківських карт зросла на 70 %. При цьому злочинці найчастіше користуються двома методами: крадуть гроші безпосередньо в банкоматі, або отримують інформацію про банківську карту по телефону.

Докладніше

***

15.04.2018

7 правил безопасности в социальных сетях

Скандал с аналитической компанией Cambridge Analytica, собравшей информацию о 87 млн пользователей Facebook, всколыхнул глобальную сеть. Вслед за возмущением пользователи соцсети устроили бойкот, а некоторые даже пошли на радикальные меры: покинули просторы Facebook. По информации LikeFolio, в конце марта пользователи начали активно удалять аккаунты.

Докладніше

***

15.04.2018

Стало известно, сколько сайтов занимаются скрытым майнингом

Компания Ahrefs проанализировала 175 миллионов веб-сайтов в своей базе данных, чтобы узнать, сколько из них занимаются скрытым майнингом. Cryptojacking – это растущая проблема для владельцев веб-сайтов по всему миру. Хакеры устанавливают майнинг-скрипты на интернет ресурсы, позволяя злоумышленникам добывать криптовалюту на вычислительных мощностях посетителей без их ведома, а также без ведома владельцев веб-сайтов (InternetUA).

Некоторые недобросовестные владельцы сайтов могут сознательно использовать скрипты для майнинга, не предупреждая об этом посетителей. В обоих случаях посетители сайта не знают, что их компьютеры используются таким образом, за исключением случаев, когда они замечают, что работа их ПК замедляется, а нагрузка увеличивается.

В ходе своего исследования, Ahrefs обнаружила, что в общей сложности 23 872 уникальных веб-сайтов из 175 млн использовали скрипты для добычи криптовалюты. Это менее 1 %. В 94 % случаев, они использовали скрипт под названием Coinhive. Компания продолжила свой анализ и попыталась подсчитать, сколько посетителей заходят на данные интернет ресурсы: примерно 91 % сайтов из этого списка ежемесячно получали меньше 50 посетителей через Google.

Существует несколько причин настолько низкого трафика: хакеры могут ориентироваться на забытые и легко уязвимые веб-сайты, сайты с высокой посещаемостью лучше защищены и сами они сильно дорожат своей репутацией. Также, по слухам, Google Chrome блокирует сайты, на которых запущены подобные скрипты. Крупные сайты зарабатывают намного больше денег с рекламы, чем могли бы зарабатывать с помощью скрытого майнинга.

***

15.04.2018

Британия приготовилась к ответной кибератаке против России

Британские киберразведчики приготовились к атаке на компьютерные сети России, если российские хакеры атакуют их инфраструктуру. Об этом сообщает The Sunday Times со ссылкой на источники (InternetUA).

По данным издания, Британия готова провести кибератаку, если российские хакеры нападут на «критическую национальную инфраструктуру» Британии.

Центр правительственной связи и британское минобороны в настоящий момент уже «на изготовке», чтобы ответить «соответственно».

Помимо кибератак, разведка также уведомила премьер-министра Терезу Мэй, что российская сторона начнет публиковать «компромат» на британских официальных лиц.

***

15.04.2018

В Google Play нашли фишинговое приложение, нацеленное на пользователей 21 банка

Специалисты ESET обнаружили новую мошенническую схему, нацеленную на пользователей мобильного банкинга. В Google Play найдено «универсальное мобильное приложение» Universal Banking Poland для клиентов 21 банка (InternetUA).

Исследователи пишут, что целью мошенников являются пользователи банковских приложений из Польши. Приложение предлагало доступ к личным кабинетам в 21 системе интернет-банкинга. Пользователю предлагалось выбрать из списка банк, в котором у него открыт счет, а затем ввести логин и пароль в специальную форму.

Как не трудно догадаться, веденные данные отправлялись на удаленный сервер злоумышленников, после чего использовались для кражи денег со счетов. Приложение обходило двухфакторную аутентификацию – пользователь не видел SMS-сообщений от банка о списании средств, поскольку доступ к SMS перехватывали атакующие.

Приложение Universal Banking Poland появилось в Google Play 20 марта 2018 года и было удалено из официального магазина после предупреждения ESET. Аналитики предупреждают, что фальшивка по-прежнему доступна на сторонних площадках.

Нужно отметить, что похожая атака была обнаружена ESET в конце 2017 года. Она так же была нацелена на клиентов 14 банков польских банков. Тогда малварь маскировалась под приложения для мониторинга курсов криптовалют Crypto Monitor и StorySaver, а также инструмент для загрузки историй из Instagram.

***

15.04.2018

За $10 данные ваших аккаунтов не попадут в сеть

Хакеры – это самые настоящие преступники 21 века, которые совершают противоправные действия с использованием различной электроники. Буквально на днях в мире заработал клон популярного веб-сайта Have I Been Pwned, позволяющего выяснить, были ли данные той или ной учетной записи взломаны, или же нет. Поддельный веб-сайт, как пишет издание The Next Web, содержит базу из нескольких миллиардов логинов и паролей от учетных записей в различных сервисах (InternetUA).

Поскольку многие пользователи сети Интернет везде используют одинаковых связку логин + пароль, это может стать большой проблемой. Злоумышленники требуют заплатить им $10 за каждую учетную запись, чтобы данные о ней были скрыты, тогда как в противном случае они обещают выложить данные от аккаунта в сеть, в результате чего он станет доступен для использования всем пользователям.

Хакерский сайт не только показывает информацию о том, были бы скомпрометированы личные данные или нет, но еще и требуется выкуп за удаление сведений из базы. За это хакеры хотят по $10 с каждого пользователя, а принимают деньги они через криптовалюты Bitcoin, Ethereum, Bitcoin Cash и Litecoin. Не менее интересно и то, что пока пользователь находится на вредоносном сайте, его компьютер используется как ферма для майнинга криптовалют, благодаря чему хакеры получат дополнительную прибыль.

Издание The Next Web не раскрывает точный адрес сайта хакеров, чтобы не позволить им заработать деньги. Эксперты считают, что злоумышленники купили в «даркнете» базу из более чем 1,4 млрд работающих учетных записей от различных сервисов, а затем при помощи ПО обеспечили ее работу в паре с сайтом. По задумке хакеров, благодаря своим действиям, они должны стать богаче на $14 000 000 000, то есть на 14 млрд долларов. Увы, но все логины и пароли в базе являются подлинными. Специалисты советуют сменить пароли от своих аккаунтов в наиболее важных местах, чтобы не стать жертвами вымогателей.

***

15.04.2018

Android P убережет ваши данные от рук злоумышленников

Android P запретит приложениям использовать незащищенное интернет-соединение для связи с сервером, сообщает AndroidCommunity. Это позволит обезопасить данные пользователей от несанкционированного доступа третьих лиц, пользующихся изъянами незашифрованных соединений (InternetUA).

Протокол TLS

С выходом финальной сборки Android P разработчики приложений, совместимых с актуальной версией ОС, будут должны внедрить поддержку протокола TLS (Transport Layer Security). Он представляет собой аналог расширения https, который, в отличие от http, защищен от проникновения извне.

Сейчас поддержка приложениями протокола TLS не является обязательным требованием, оставляя мошенникам пространство для маневра. Все разработчики, чьи программы собирают те или иные данные пользователей, наряду с внедрением TLS, должны в обязательном порядке указывать домены, с которыми связываются приложения.

***

15.04.2018

Защита от отслеживания теперь включена в Firefox для iOS по умолчанию

Mozilla выпустила новую версию Firefox для iOS, в которой по умолчанию включена защита от отслеживания. С ней сайты не смогут следить за вашими действиями и получать доступ к вашей личной информации, пока вы сами того не захотите (InternetUA).

Функция была доступна в браузере и раньше, но её приходилось включать самостоятельно. Теперь она активирована сразу – и в обычном, и в приватном режиме. В последнем, помимо прочего, Firefox блокирует рекламу и другой нежелательный контент, а также не сохраняет историю ваших посещений.

Защита от отслеживания в Firefox для iOS работает на базе той же технологии, которая блокирует рекламу и трекеры в Firefox Focus для iOS и Android, а также в Firefox для Android и настольных устройств. Система берёт данные из чёрного списка Disconnect.

«Mozilla всегда верила, что важно уважать конфиденциальность пользователей и давать им право решать, какой информацией они хотят делиться, а какой нет, – заявил разработчик браузера. – Сегодня больше потребителей, чем когда-либо, требует этого от компаний, которым предоставляют свои данные».

Преимущество защиты от отслеживания состоит ещё и в том, что сайты загружаются быстрее, поскольку не загромождены отслеживающими скриптами. Это, в свою очередь, экономит пользователям интернет-трафик и заряд аккумулятора.

Среди других нововведений Firefox для iOS – возможность изменять порядок вкладок на iPad и перетаскивать ссылки из браузера в другие приложения.

***

16.04.2018

Кибершпионы стали чаще использовать маршрутизаторы в своих атаках

Исследователи из «Лаборатории Касперского» сообщили об участившихся случаях использования взломанных маршрутизаторов кибершпионскими хакерскими группировками (InternetUA).

«Мы видели множество попыток взлома маршрутизаторов на протяжении нескольких лет. Очень хорошим примером является вредоносное ПО SYNful Knock для маршрутизаторов Cisco, которое было обнаружено компанией FireEye и хакерскими группировками Regin и CloudAtlas. Обе группировки владели проприетарным ПО для взлома устройств», – отметили специалисты.

По словам экспертов, количество группировок, использующих маршрутизаторы для атак, стремительно выросло в минувшем году, и данная тактика продолжает пользоваться популярностью в 2018 году.

Например, хакерская группировка Slingshot, предположительно связанная с армией США, использовала взломанные маршрутизаторы MikroTik для заражения жертв вредоносными программами.

Подобным образом группировка Frontline взламывала домашние маршрутизаторы и построила сеть прокси-серверов, которые можно было использовать для атаки UPnProxy.

«Мы также обнаружили APT LuckyMouse [использующую маршрутизаторы] для размещения своих C&C-серверов, что само по себе довольно необычно. Мы считаем, что им удалось взломать маршрутизатор с помощью уязвимости в протоколе SMB, позволившей им загрузить скрипты CGI для управления и контроля», – добавили эксперты.

Как отметили исследователи, атаки с использованием маршрутизаторов пользуются популярностью у хакеров и существует вероятность, что множество атак происходят незаметно как для пользователей, так и для ИБ-экспертов.

***

16.04.2018

Михаил Сапитон

Telegram – новый источник пиратского контента

Издание The Outline обратило внимание на то, что пользователи Telegram используют мессенджер для загрузки пиратского контента. Количество каналов с нелегальными копиями фильмов, музыкальных альбомов, приложений и прочего перевалило за тысячи.

Докладніше

***

16.04.2018

«Київстар» під час перевірок програмою Bug Bounty виявив 52 випадки кібервразливості *// Однак випадків витоку даних з систем мобільного оператора зафіксовано не було*

Мобільний оператор «Київстар» під час перевірок програмою Bug Bounty виявив 52 випадки кібервразливості. Про це компанія повідомила в прес-релізі (mind).

Так, з листопада минулого року компанія проводить програму Bug Bounty на базі Bugcrowd – краудсорсингової платформи для вирішення проблем кібербезпеки.

Згідно з повідомленням, «Київстар» підкреслює, що останнім часом у світі виникає все більше скандалів, пов'язаних із витоком даних клієнтів і різними порушеннями прав суб'єктів даних.

Так, програма стартувала у закритому режимі. Протягом перших чотирьох місяців digital-сервіси компанії перевіряли кіберспеціалісти зі всього світу. За цей час було виявлено понад 20 потенційних вразливостей, які були усунені спеціалістами компанії.

У період з 13 по 27 березня «Київстар» відкрив доступ до програми. Тоді кожен охочій міг повідомити про знайдену вразливість у digital-сервісах і ресурсах компанії та отримати фінансову винагороду. За цей час у програмі взяли участь більше 160 спеціалістів з кібербезпеки з усього світу.

Після закінчення відкритої частини програми Bug Bounty, найбільш активних кіберспеціалістів запросили продовжити тестувати digital-сервіси і ресурси компанії у межах закритого режиму.

За даними «Київстар», до, під час і після тестування не було зафіксовано випадків витоку даних з систем мобільного оператора.

***

17.04.2018

Check Point: 97 % компаний не готовы к кибератакам «Пятого поколения»

Check Point Software представил результаты исследования 2018 Security Report. В отчете представлены киберугрозы, с которыми сталкиваются организации различных отраслей.

Докладніше

***

17.04.2018

США и Британия обвинили хакеров из РФ в заражении роутеров по всему миру

Национальный центр по кибербезопаности Великобритании вместе с Федеральным бюро расследований и Министерством внутренней безопасности США заявили о масштабной кибератаке, организованной хакерами, которых поддерживает правительство России (InternetUA). Об этом сообщает Politico.

По данным британской и американской разведок, хакеры пытались заразить вредоносными программами миллионы роутеров по всему миру.

Атака была направлена на то, чтобы перехватывать информацию, проходящую через зараженные устройства. Также хакеры пытались взломать файерволы.

Целью атаки мог стать кибершпионаж или кража интеллектуальной собственности. Ее объектами оказались интернет-провайдеры, государственные организации и крупные компании.

Координатор Белого дома по вопросам кибербезопасности Роб Джойс заявил, что американское правительство знает про атаку.

В качестве ответных мер он допустил введение новых санкций и ответные хакерские атаки.

Российское посольство в Лондоне в свою очередь заявило, что в Великобритании в последнее время звучало много предупреждений о возможной кибератаке со стороны России в ответ на авиаудары по Сирии и расследование отравления Скрипалей.

***

17.04.2018

Android-троянец из Google Play подписывает пользователей на платные услуги

Вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play троянца Android.Click.245.origin, который по команде злоумышленников загружает сайты, где пользователей обманом подписывают на платные контент-услуги (ITnews).

В некоторых случаях оформление подписок выполняется автоматически после нажатия мошеннической кнопки для «скачивания» программ.

Злоумышленники распространяли Android.Click.245.origin от лица разработчика Roman Zencov и маскировали троянца под известные приложения. Среди них – еще не вышедшая на платформе Android игра Miraculous Ladybug & Cat Noir, нашумевшая в начале весны программа GetContact для звонков и работы с телефонными контактами, а также голосовой помощник Алиса, который встроен в приложения от компании «Яндекс» и как отдельное ПО пока недоступен. Одна из троянских программ входила в тридцатку наиболее популярных новинок каталога Google Play.

Специалисты «Доктор Веб» уведомили корпорацию Google об Android.Click.245.origin, после чего он был удален из каталога. В общей сложности приложения-подделки успели установить свыше 20 000 пользователей. У всех этих программ нет никаких полезных функций. Их основная задача – загрузка веб-страниц по команде злоумышленников.

После запуска Android.Click.245.origin соединяется с управляющим сервером и ожидает от него задания. В зависимости от IP-адреса подключенного к сети зараженного устройства троянец получает ссылку на определенный сайт, который необходимо загрузить. Вредоносная программа переходит по полученной ссылке и с использованием WebView отображает нужную киберпреступникам страницу. Если мобильное устройство подключено к Интернету через Wi-Fi, пользователю предлагается установить интересующее приложение, нажав на соответствующую кнопку. Например, если жертва запускала программу-подделку голосового помощника Алиса, для «скачивания» может быть подготовлен файл под названием «Alice Yandex.apk».

При попытке загрузки указанного файла у владельца мобильного устройства запрашивается номер мобильного телефона для некоей авторизации или подтверждения скачивания. После ввода номера пользователю отправляется проверочный код, который необходимо указать на сайте для завершения «загрузки». Однако никаких программ после этого жертва не получает – вместо этого она подписывается на платную услугу.

***

17.04.2018

Шахраї запустили фейкову криптогривню // *Творці наразі невідомі*

Шахраї вирішили заробити на зборі коштів від запуску фейкової національної криптовалюти України. Про це пише Ліга Бізнес Інформ (mind).

Згідно з повідомленням, 16 квітня один із ресурсів про криптовалюту повідомив, що Національний банк України запустив свій проект на Blockchain – українську криптовалюту, яка отримала назву eUAH. Ресурс також опублікував скріншот сайту проекту із знаком питання в заголовку.

Сайт проекту було зареєстровано 16 березня. Творці наразі невідомі, однак в описі йдеться про те, що ініціатором випуску кріптогривні є українські держоргани – Держагентство з електронного урядування, Нацбанк і Мін'юст. Проект нібито почався в березні.

«У 2018 році заплановано випустити у вільний обіг до 10 % запасу токенів. Початок життя електронної гривні», – йдеться на сайті.

У eUAH також є «біла книга», зроблена в стилі презентацій НБУ. У ній говориться, що в наступному році криптовалюту використовуватимуть у всіх сферах економіки країни й на неї доведеться 15 % транзакцій.

Засновник криптовалютної біржі Kuna Exchange Михайло Чобанян назвав запуск української криптовалюти фейком і заявив, що в країні створенням кріптогривні займається лише він та НБУ. За його словами, будь-який шахрай може оформити такий проект за десять хвилин, ще день витратити на запуск сайту.

У Нацбанку й Держагентстві з електронного урядування також спростували участь у проекті. У НБУ повідомили, що їх проект поки перебуває на стадії розробки, інформація про нього не розголошується.

«Він не виноситься на широкий загал і проводиться на умовах волонтерства», – уточнили в НБУ.

***

17.04.2018

Киберполиция предупредила о масштабной вирусной рассылке в «Фейсбуке» от друзей

В Интернете зафиксировано массовое распространение вируса через социальную сеть Facebook. Впервые он был зафиксирован в 2017 году, а сейчас распространяется по всему миру, в том числе и на территории Украины.

Докладніше

***

18.04.2018

Facebook удалила порядка 120 занимавшихся киберпреступной деятельностью групп

Журналист Брайан Кребс сообщил о закрытии социальной сетью Facebook порядка 120 групп, занимавшихся киберпреступной деятельностью. В общей сложности в группах состояло около 300 тыс. участников (InternetUA).

По словам Кребса, группы предлагали широкий спектр незаконных услуг, включая спам-рассылки, мошенничество, взлом банковских счетов, уклонение от налогов, осуществление DDoS-атак на заказ, а также создание ботнетов. В среднем большинство групп действовали на платформе Facebook порядка двух лет.

Самая большая из запрещенных групп рекламировала продажу и использование украденных кредитных и дебетовых карт. Помимо этого, были закрыты крупные сообщества, распространявшие инструменты для массового взлома учетных записей на различных сервисах, таких как Amazon, Google, Netflix, PayPal, а также банков.

Facebook закрыла группы в течение нескольких часов после того, как Кребс уведомил компанию о своих находках.

***

18.04.2018

Ирина Фоменко

Российская разведка могла взломать и ваш Wi-Fi

16 апреля было зафиксировано несколько миллионов хакерских атак, сообщает The Guardian. США и Великобритания обвиняет Россию в глобальной кампании хакерства, которая включает взлом миллионов компьютеров и других устройств, в том числе, и маршрутизаторов Wi-Fi (InternetUA).

В Великобритании находятся сотни тысяч устройств, которые могут стать целью хакеров, – так почему же Россия так сильно хочет взломать ваше Интернет-соединение?

Конечно, маловероятно, что Путин или его агенты разведки пытаются проникнуть в учетные записи Amazon или взломать широкополосную связь – пусть и преступники могут украсть у вас деньги, либо использовать ваши устройства для майнинга криптовалюты.

Хакерство разведывательных агентств бывает различным. К счастью, эксперты утверждают, что большинству незачем беспокоиться – по крайней

мере, в краткосрочной перспективе. Хакерские организации часто позволяют атаке распространяться на любое уязвимое устройство с целью взломать домашний компьютер для получения полезной целевой информации.

Это не означает, что не стоит принимать меры безопасности, если вы не работаете на MI6, однако есть огромное количество разных интеллектуальных целей. Если вы сотрудничаете с крупной вычислительной компанией, с сетью коммунальных служб или с другой областью ключевой инфраструктуры, вы можете представлять для хакеров серьезных интерес. Страны «взламывают друг друга», поэтому, если они и когда-нибудь начнут войну, они могут отключить важные системы перед атакой – например, электростанции.

Не только Россия ведет такую деятельность, среди других стран – Израиль, США и Великобритания. Глобальный, невидимый, незначительный конфликт происходит в Интернете, и возможно, ваш маршрутизатор был взломан. Вероятно, стоит лишний раз проверить брандмауэр и антивирус.

***

18.04.2018

8 из 10 организаций обеспокоены проблемой соблюдения сотрудниками политики безопасности

Корпорация Oracle и аналитическая компания KPMG недавно провели глобальный опрос 450 ИТ-специалистов. Он показал, что организации всеми силами пытаются защитить свои данные на фоне растущего числа нарушений безопасности.

Докладніше

***

18.04.2018

Android-троянец из Google Play подписывал пользователей на платные мобильные услуги

Вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play троянца Android.Click.245.origin, который по команде злоумышленников загружает сайты, где пользователей обманом подписывают на платные контент-услуги. В некоторых случаях оформление подписок выполняется автоматически после нажатия мошеннической кнопки для «скачивания» программ.

Докладніше

***

20.04.2018

Уязвимость в LinkedIn позволяла тайно собирать данные пользователей

Исследователь безопасности Джек Кейбл (Jack Cable) обнаружил опасную уязвимость в социальной сети LinkedIn. Проблема могла быть проэксплуатирована для тайного сбора информации о пользователях (Центр информационной безопасности).

Уязвимость связана с функцией LinkedIn AutoFill, активирующей кнопку «Автозаполнение с помощью LinkedIn». При нажатии она делает запрос на сайт LinkedIn, извлекает данные пользователя и вставляет их в форму заявки. Данная функция используется в основном на порталах по поиску работы.

Как выяснил исследователь, любой сайт может злоупотреблять данной функцией для скрытого сбора данных пользователя. Кнопку можно тайно установить на странице, изменив ее размер и сделав ее прозрачной путем изменения ряда настроек CSS. Таким образом пользователь может неосознанно предоставить свои данные, всего один раз нажав на любую страницу.

Кейбл уведомил команду безопасности LinkedIn о проблеме 9 апреля, после чего социальная сеть временно ограничила использование кнопки, а затем выпустила полноценное исправление.

***

20.04.2018

Хакеры могут взломать мозговые имплантаты и прочитать мысли

Незащищенные сигналы имплантируемых нейростимуляторов могут быть взломаны с помощью легкодоступного оборудования. К таким выводам пришла команда бельгийских исследователей, протестировавших безопасность беспроводных мозговых имплантатов (Центр информационной безопасности).

Нейростимуляторы представляют собой устройства, вводимые в полость черепа человека для лечения нейродегенеративных заболеваний, таких как болезнь Паркинсона. Поскольку имплантат непосредственно взаимодействует с серым веществом мозга, последствия могут быть катастрофическими. К примеру, изменение вольтажа нейростимулятора может привести к смерти человека.

Результаты исследования были представлены в докладе «Обеспечение безопасности беспроводных нейростимуляторов» на конференции ACM Conference on Data and Application Security and Privacy в прошлом месяце. По словам исследователей, им удалось осуществить реверс-инжиниринг неназванного имплантата и обнаружить серьезные проблемы с безопасностью.

Передача сигналов в устройстве не шифруется и не аутентифицируется. Исследователи считают, что в будущем для корректировки лечения нейротрансмиттеры будут использовать информацию, полученную из мозговых волн наподобие P-300. Если злоумышленникам удастся перехватить и проанализировать эти сигналы, они смогут в буквальном смысле прочитать мысли пациента. Однако этого можно избежать, если использовать инновационную архитектуру безопасности, считают исследователи.

***

23.04.2018

За 2017 год случаи скрытого майнинга участились в 340 раз

Случаи скрытого майнинга растут в геометрической прогрессии. По данным антивирусной компании Symantec, за 2017 год они участились в 340 раз.

Докладніше

***

23.04.2018

Дмитрий Демченко

Кабмин предложил ужесточить наказание за кибератаки и создание и распространение вредоносного ПО

Кабинет министров Украины подготовил поправки в Уголовный кодекс, который ужесточает ответственность за кибератаки на критически важные объекты инфраструктуры. Соответствующий законопроект № 8304 был зарегистрирован 19 апреля, сообщает «Громадське» (AIN.UA).

Авторы законопроекта предлагают назначить уголовную ответственность за киберпреступления, связанные с критическими объектами инфраструктуры. Наказание предполагает лишение свободы сроком от 6 до 8 лет. За повторное аналогичное преступление авторы предлагают наказывать лишением свободы сроком до 10 лет.

Проект закона также имеет поправки касательно создания и распространения вредоносного ПО. Новые правки предполагают увеличение суммы штрафа за подобные правонарушения с тысячи до 3000-5000 необлагаемых минимумов доходов граждан (51 000-85 000 гривен).

Такими мерами авторы хотят усилить безопасность на фоне роста киберугрозы со стороны России.

***

23.04.2018

Пользователи Gmail получили спам от самих себя

Некоторые владельцы почтовых ящиков Gmail заметили, что им приходят рекламные письма с их же адреса. Об этом сообщает Mashable (InternetUA).

По словам пользователей, спам приходил и отображался в разделе «Отправленные» даже после того, как они включали двухфакторную аутентификацию и меняли пароли учетных записей.

По словам представителей Google, никакого взлома не было. Спамеры нашли способ обойти защиту от рекламы: они использовали поддельные заголовки электронной почты, в результате чего все приходящие письма попадали в папку «Отправленные».

«Мы не имеем оснований полагать, что какие-либо учетные записи были скомпрометированы во время этого инцидента. Если вы заметили необычное письмо, мы рекомендуем вам помечать его, как спам», – заявили руководители Gmail. Они также отметили, что компания уже приняла меры по защите от атаки злоумышленников.

***

23.04.2018

NIST представил новую версию руководства по защите от киберугроз

Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) представил новую редакцию руководства по усилению кибербезопасности критической инфраструктуры Cybersecurity Framework v1.1 (InternetUA).

Согласно заявлению NIST, версия 1.1 фокусируется на сферах, жизненно важных для обеспечения национальной и экономической безопасности, включая энергетический, банковский, телекоммуникационный и оборонный секторы. Новый вариант фреймворка доработан с учетом отзывов специалистов на предыдущие проекты документа. В частности, обновлены рекомендации относительно аутентификации и идентичности, обеспечения кибербезопасности в цепочках поставок, а также раскрытия информации об уязвимостях. В документ добавлен новый раздел, поясняющий, как организации могут использовать фреймворк для оценки рисков кибербезопасности.

Позднее в текущем году NIST намерен выпустить обновленную сопутствующую «дорожную карту» для улучшения кибербезопасности критической инфраструктуры, в которой будут описываться ключевые области разработки, согласования и сотрудничества.

***

23.04.2018

Британские спецслужбы заявили о невозможности полной защиты от кибератак

Глава центра национальной кибербезопасности (NCSC) Великобритании Киаран Мартин заявил, что сотрудники британских спецслужб не могут обеспечить полную защиту страны от предполагаемых кибератак, пишет The Telegraph (InternetUA).

В частности, Мартин выразил уверенность в том, что Британия столкнется с кибератаками России, назвав неизвестным только время, «когда это случится». Он отметил, что в настоящий момент ведомство занимается работой по обеспечению устойчивости к кибератакам на энергетические системы, системы водоснабжения, интернета, транспортной сети и службы здравоохранения.

«Абсолютная защита не является ни возможной, ни целесообразной; речь идет о большей устойчивости систем, о которых мы беспокоимся больше всего, тех, потеря обслуживания которых окажет наибольшее влияние на наш образ жизни», – сказал Мартин.

Сообщается также, что правительству страны было направлено письмо со списком мер, которые необходимо предпринять для защиты от кибератаки.

***

24.04.2018

Неизвестные взломали сайт Минэнерго и требуют за разблокировку 0,1 Bitcoin

Неизвестные взломали сайт Министерства энергетики и угольной промышленности и просят 0,1 Bitcoin (примерно 24 тыс. гривен) за его разблкировку (InternetUA).

Об этом свидетельствует главная страница сайта mev.gov.ua, передают Українські Новини.

«Ваши важные файлы сайта зашифрованы. Многие из ваших .php, .css, .js и других файлов больше недоступны, поскольку они были зашифрованы. Возможно, вы заняты поиском способа восстановить свои файлы, но не тратьте свое время! Никто не может расшифровать ваши файлы без нашей специальной службы дешифрования», – говорится в сообщении на сайте Минэнерго.

Согласно сообщению неизвестных, у Министерства есть 10 часов для оплаты 0.1 Bitcoin.

***

24.04.2018

Trend Micro использует искусственный интеллект, чтобы выявлять мошеннические электронные письма

Компания Trend Micro представила разработку в области информационной защиты от атак, построенных на использовании деловой переписки по электронной почте. Это анализатор стиля текста Writing Style DNA, работающий по алгоритмам искусственного интеллекта. Как утверждается, он способен выявлять письма, авторы которых пытаются выдать себя за руководителей или других высокопоставленных пользователей (InternetUA).

Анализатор учитывает более 7000 характеристик стиля. Подозрительные электронные письма проверяются на модели, обученной на образцах текста, и в случае выявления подделки рассылается уведомление отправителю, получателю и в отдел ИТ.

В 2017 году 94 % всех программ-вымогателей, заблокированных средствами информационной защиты Trend Micro, распространялись по электронной почте. В то же время, потери от мошенничества с использованием деловой переписки по электронной почте в этом году прогнозируются на

уровне 9 млрд долларов. Другими словами, средства защиты от таких атак весьма востребованы, а технологии искусственного интеллекта позволяют повысить эффективность этих средств.

Анализатор Writing Style DNA будет интегрирован в различные продукты Trend Micro. Уже в июне он войдет в состав средств информационной защиты для Microsoft Office 365 и ScanMail for Microsoft Exchange (SMEX).

ДОДАТКИ

Додаток 1

23.04.2018
Ирина Фоменко
Ключевые моменты новой политики данных Facebook

Пользователи Facebook уже давно жаловались, что настройки конфиденциальности и информация о сборе данных службы слишком сложны и их трудно найти. Стремясь уменьшить эту путаницу, компания опубликовала новое руководство, чтобы ознакомить пользователей с обновленной политикой сбора данных. Об этом сообщает The Fortune (InternetUA).

Изменения соответствуют новым правилам Европейского Союза, которые вступают в силу 25 мая. Согласно им, компании должны больше контролировать уровень конфиденциальности и четко объяснять, как и почему они собирают пользовательские данные. Изменения повлияют на всех пользователей Facebook независимо от их местонахождения, но в первую очередь затронут жителей Европы.

Несмотря на то, что новые правила конфиденциальности и сбора данных Facebook изложены более четко, информации все еще достаточно много. Вот ключевые моменты новой политики данных.

Facebook собирает данные обо всем, чем вы делитесь

Новое руководство по политике данных в Facebook разъясняет, какой именно информацией о пользователе делится компания и с кем. В частности, Facebook собирает данные пользователей при регистрации, загрузке или обмене контента, при общении с другими людьми на Facebook.

Facebook также собирает данные, когда кто-то публикует фотографию с вами, про вас, загружает или синхронизирует вашу контактную информацию или сообщения.

У Facebook может быть информация о вашей кредитной карте

У пользователей Facebook есть несколько вариантов, на что потратить деньги в социальной сети, в том числе, на внутренние игровые покупки. Всякий раз, когда вы оплачиваете что-то через сайт, Facebook собирает информацию о транзакции, включая информацию о платеже – номера дебетовых и кредитных карт, данные об аутентификации, а также информацию о доставках и счетах.

Facebook делится некоторой информацией с рекламодателями

Вопрос, который неоднократно возникал, когда основатель и генеральный директор Facebook Марк Цукерберг дал показания перед Конгрессом в начале этого месяца, заключается в том, продает ли Facebook рекламодателям данные об отдельных пользователях. Цукерберг каждый раз отвечал, что Facebook не делает этого и не использует информацию для целевой рекламы.

Новая политика данных более четко объясняет, как именно Facebook обрабатывает объявления и пользовательскую информацию. Facebook также предоставляет некоторую информацию поставщикам услуг, а также технической и клиентской службам поддержки.

Большая часть политики данных Facebook осталась без изменений

Facebook вносит некоторые изменения в работу социальной сети. Среди них – спрашивать у пользователей, хотят ли они продолжать обмен политической или религиозной информацией и разрешат ли целевую рекламу. У пользователей уже была возможность отключать целевые объявления и удалять религиозную или политическую информацию из своих профилей, но теперь их будут спрашивать об этом.

Так, пользователи в ЕС и Канаде должны разрешить Facebook использовать технологию распознавания лиц, чтобы друзья могли отмечать их на фотографиях и видео или для определения попыток использования вашей фотографии как изображения профиля.

Общий регламент по защите данных больше обезопасит несовершеннолетних от сбора данных и обеспечит должный уровень конфиденциальности. У Facebook уже есть определенные настройки безопасности для пользователей в возрасте от 13 до 18 лет, но теперь им также потребуется разрешение родителя или опекуна, чтобы включить некоторые функции, например, просмотр целевых объявлений в определенных странах (Facebook не сообщает, как проверить, получал ли ребенок согласие родителей). Тем не менее, Facebook продолжит собирать информацию о использовании несовершеннолетними социальной сети независимо от их предпочтений в отношении таргетинга.

Однако для большинства пользователей сбор данных Facebook и выбор пользователем определенных методов сбора данных не изменятся. Вместо этого их будут спрашивать, поэтому информация о том, какие именно компания получает данные, будет более четко раскрыта. В Facebook заявили, что социальная сеть не просит новых прав «собирать, использовать, делиться своими данными на Facebook» или изменять предыдущие варианты конфиденциальности пользователей.

(вгору)

Додаток 2

24.04.2018
Дмитрий Демченко

Facebook опубликовала свои секретные правила по работе с контентом

Facebook опубликовала ранее неизвестные общественности правила, по которым в компании работают с контентом. Таким образом, соцсеть предоставила намного больше деталей о запрещенных темах на своих платформах, чем когда-либо. Также компания разрешила подавать апелляции по решениям, принятым по конкретным постам. Об этом сообщает Reuters (AIN.UA).

У Facebook на протяжении многих лет были «Нормы сообщества», которые определяли правила публикации контента. Но в публичном доступе была только краткая версия этих норм, к детальному документу имели доступ лишь сотрудники компании. По словам начальника департамента глобальной политики Facebook Моники Бикерт, сейчас соцсеть предоставляет более обширный документ, чтобы устранить путаницу и быть более открытой для людей.

Более длинная версия документа «Норм сообщества» охватывает более 8000 слов и изображений, которые может цензурировать Facebook, с подробным обсуждением каждой категории. Например, публикации видео, где изображаются люди, пострадавшие от каннибализма, не разрешены в соцсети. Впрочем, такая картинка разрешена с предупреждающим экраном, если события происходят в больнице.

Также появились новые детали касательно публикаций о наркотиках. По правилам, контент, где человек признается в том, что употребляет или продает наркотики не в медицинских целях, не разрешен на Facebook. Но из документа можно понять, какие другие высказывания на эту тему не разрешены.

В документе подробно излагаются случаи преследования и запугивания, например, запрет на «проклятия в адрес несовершеннолетних». Также запрещается контент, который исходит от взломанного источника, «за исключением ограниченных новостных случаев».

Вместе с тем, эти нормы не включают отдельные процедуры, в соответствии с которыми правительства могут требовать удаления контента, нарушающего местное законодательство. Такие решения принимаются лишь на основании юридических заключений.

Кроме этого, Facebook разрешил подавать апелляции касательно удаления конкретной записи. Ранее соцсеть разрешала оспаривать лишь удаление аккаунтов, групп и страниц. Теперь Facebook будет чаще указывать причину удаления контента.

(вгору)

Додаток 3

18.04.2018

Как бороться со смартфонозависимостью: версия создателя iPod

Производителям смартфонов следует лучше осведомлять потребителей о рисках, связанных с чрезмерным увлечением гаджетами. Об этом в колонке для журнала Wired написал Тони Фаделл – бывший инженер Apple, один из авторов медиаплеера iPod и основатель производителя «умных» термостатов Nest, впоследствии купленного Google (InternetUA).

«Возьмите в качестве аналогии здоровое питание: у нас есть рекомендации от ученых и диетологов насчет количества белка и углеводов, которое следует включить в наш рацион; у нас есть стандартизированная мера измерения, позволяющая узнавать вес; и у нас есть нормы, предписывающие частоту занятия физическими нагрузками», – написал Фаделл.

По его мнению, ответственность за умеренное «цифровое питание» также должны взять на себя производители электроники и создатели приложений. «Мы должны быть в состоянии видеть, на что тратим время, и, если захотим, быть способны изменить свою активность соответствующим образом. Нам нужны 'весы' для нашего цифрового веса, какие у нас есть для физического», – считает инженер.

Фаделл посоветовал пользователям не «переедать», а разработчиков призвал создать инструмент, который мог бы отображать историю использования устройством. Приложение должно быть похожим на выписку по банковской карте – «чтобы люди могли видеть, сколько времени они проводят за чтением электронной почты, например, или за прокруткой постов», заключил он.

Как показывает недавно проведенное в США исследование, чрезмерное использование смартфонов может привести к тревожности, депрессии, проблемам со сном, неспособности сконцентрироваться на значительное время и другим проблемам. По результатам опроса Deloitte, среднестатистический американец обращается к смартфону примерно 47 раз в день. Однако частота использования продолжает расти среди самых молодых пользователей (18–24 года): она увеличилась за минувший год с 82 до 86 раз в день.

(вгору)

Додаток 4

21.04.2018

Чи заважають соцмережі складати іспити?

Невже багатозадачність підлітків сягнула такого рівня, що вони безболісно можуть відповідати на повідомлення в Snapchat, WhatsApp та Instagram, дивитися кумедні відео про тваринок у YouTube, та ще й вчитися (InternetUA)?

Наближається гаряча пора підготовки до іспитів у школах та університетах. Батьки намагатимуться виховувати, прекрасно розуміючи – хоч би що вони сказали, суперечка, мабуть, неминуча.

Багато шансів, що перед вашим носом гримнуть дверима, якщо ви, хай навіть обережно, порадите підлітку на п'ять хвилин вимкнути мобільний телефон й зосередитись на підручниках.

Міфи про багатозадачність

Але чи справді молоді люди здатні одночасно реагувати на таку величезну кількість різних подразників? Хіба собака Павлова не вмер би від виснаження, якби його змусили весь час так реагувати?

Том Беннетт, вчитель, батько й консультант британського уряду з питань поведінки в школах, стверджує: підлітки не багатозадачні. Вони не можуть одночасно користуватися соцмережами, розважальними сайтами та навчатися. Це міф, каже він.

Пан Беннетт – директор та засновник компанії ResearchEd Group, яка займається поширенням результатів досліджень у галузі освіти серед учителів. За його словами, все свідчить про те, що інтернет справді заважає й шкодить навчанню.

Для підготовки до іспитів необхідна уважність і зосередженість, пояснює він. Але безжальні соцмережі вимагають постійної уваги, тому вони вщент розбивають будь-яку концентрацію.

«Проблема дуже серйозна, вона турбує освітян та батьків», – підкреслює пан Беннетт.

Він розповідає, що в підлітків спостерігається «реакція звикання» до телефонів, тому вони постійно зазирають у соцмережі, щоб перевірити оновлення та реакції.

Заборона телефонів

Ця залежність заважає не лише домашнім завданням. Іншою проблемою є неспокійний сон та тривожність, яку спричиняє онлайн-культура, зазначає пан Беннетт.

«Діти, на яких вона впливає найдужче, майже напевно почнуть сильно відставати в навчанні», – застерігає освітянин.

І його занепокоєння підкріплені результатами міжнародних досліджень.

Група вчених, серед яких були наукові співробітники Массачусетського технологічного інституту, провела дослідження серед учнів шкіл, розташованих у Бостоні та околицях. Було виявлено «зв'язок між підвищеним рівнем багатозадачності та погіршенням результатів навчання у підлітків».

Подібні результати американські вчені також отримали, коли розглянули академічні успіхи в школах Англії, де заборонили користуватися мобільними телефонами. Таким чином, принаймні частину робочого дня дітей звільнили від переписки та соцмереж.

Луїс-Філіппе Белан з Університету штату Луїзіана та Річард Мерфі з Університету штату Техас в Остіні, дійшли висновку: «Завдяки забороні покращилась не лише успішність учнів. Найбільшу користь отримали учні з поганою успішністю й учні з бідних сімей».

Раніше вчені зі Стенфордського університету виявили, що вплив на людей численних онлайн-подразників не пришвидшує їхню реакцію. Навпаки,

в них знижується продуктивність праці та погіршуються показники тестів на перевірку пам'яті.

«Не кажіть їм просто вимкнути»

Але чи матиме це хоч якийсь вплив на залежного від гаджетів підлітка, якого від мобільного телефона треба відлучати хірургічним шляхом?

Частково проблема полягає в тому, що для підготовки учню потрібні матеріали в інтернеті. Тож, робота й розваги перебувають на відстані одного кліку.

Соцмережі чатують на тому самому екрані, що й підготовчі матеріали. Ігровий майданчик та бібліотека зручно розташувалися в одному й тому ж місці.

Можливо, YouTube – це звуковий супровід, який сильно заважає роботі. Але водночас – і один з найбільших неофіційних підготовчих сервісів на планеті.

Google може бути відправним пунктом для пошуку веб-сайтів, де повно безплатних матеріалів та онлайнових навчальних програм.

Доктор Сандра Літон Грей, старший лектор з питань освіти в Інституті освіти при Університетському коледжі Лондона, не радить батькам вимагати, щоб дитина «негайно вимкнула»". Це буде помилкою.

«Значно розумніше буде діяти в обхід. Спитайте: “Ну як там справи в інтернеті?”. Поцікавтеся, чи дитину ніщо не відволікає», – каже вона.

За її словами, підлітків краще вмовляти, а не жорстко перелічувати їм усі небезпеки від марнування часу в інтернеті.

«Лихі та дивовижні»

Доктор Літон Грей пояснює: підлітки можуть одночасно обговорювати підготовку до іспитів та спілкуватися на інші теми. Не завжди можна провести чітку межу між навчанням та відповіддю на повідомлення у соціальних мережах.

Але постійне користування соцмережами лекторка вважає фактором стресу, а не способом розслабитись у пору іспитів.

Вона проводить паралелі між користуванням соцмережами та «фастфудним мисленням»: є миттєва винагорода, а далі – триваліше відчуття «незадоволеності» та тиску через необхідність відповідати вимогам «стадного світогляду» інших підлітків.

Ця онлайнова культура для підлітків «лиха та дивовижна водночас», зазначає доктор Літон Ґрей.

Але медіа-звички змінюються. В цьогорічній доповіді йдеться про те, скільки часу діти проводять на самоті, переглядаючи відео на екранах комп'ютерних пристроїв.

За словами Тома Беннетта, батьки досі відчувають труднощі, намагаючись іти в ногу з темпами цих змін.

Але також він наголошує на тому, що проблему «забагато часу в інтернеті» тепер усвідомлюють краще – а під час напружених тижнів перед іспитами це актуально, як ніколи.

«Можливо, ми наближаємося до переломного моменту», – підсумовує він.

(вгору)

Додаток 5

20.04.2018

В Twitter фейки распространяются быстрее настоящих новостей

В последнее время проблема распространения фейковых новостей все чаще обсуждается мировым сообществом, так как очевидно ее влияние на политическое, экономическое и социальное благополучие человечества (Siteua).

Исследователи Соруш Восау, Деб Рой и Синан Арал из Массачусетского технологического института проанализировали более 126000 фейковых новостей, которые были опубликованы в Twitter за все время его существования – с 2006 по 2017 годы, – чтобы оценить масштаб проблемы.

В своем исследовании ученые классифицировали новости как истинные или ложные, используя информацию от шести независимых организаций по проверке фактов.

Выяснилось, что 126 000 ложных новостей получили распространение с помощью трех миллионов человек, которые сделали четыре с половиной миллиона ретвитов. Установлено, что наиболее популярные фейки видят от 1000 до 10 000 человек, тогда как настоящие новости редко получают охват более 1000 читателей. Причем фейки распространяются быстрее и масштабнее правды, независимо от тематики. Наиболее активно люди делятся фейковыми политическими новостями, далее идут неправдивые сообщения о террористических угрозах, природных катаклизмах, науке, финансах и различные городские легенды.

Проанализировав комментарии, исследователи пришли к выводу, что ложные новости чаще вызывают у читателей такие эмоции, как страх, отвращение и удивление, а настоящие – печаль, радость или доверие.

«Фейковые новости обычно более романтичны, фантастичны. Мы полагаем, что проблема фейковых новостей отчасти обусловлена тем, что люди предпочитают распространять информацию, которая им кажется необычной, выбивающейся из повседневной рутины», – отметили исследователи.

Также установлено, что, вопреки общепринятому мнению, боты не оказывают значительного влияния на скорость распространения информации – как фейковой, так и правдивой.

«Это значит, что причина, по которой проблема фейковых новостей сегодня стоит ребром, кроется все же в людях, а не в ботах», – заключили ученые.

(вгору)

Додаток 6

18.04.2018

Microsoft, Facebook та ще 30 компаній підписали декларацію про відмову від участі в кібератаках // *Google, Apple та Amazon поки що до угоди не долучилися*

Більше 30 високотехнологічних компаній на чолі з Microsoft та Facebook підписали угоду про відмову від участі в кібератаках, які можуть бути організовані урядом будь-якої країни. Про це повідомляє The New York Times (mind).

Цим вони демонструють прагнення Кремнієвої долини відгородитися від урядових кібервоєн.

Принципи угоди зобов'язують компанії прийти на допомогу будь-якій нації в боротьбі з кібератакою, незважаючи на те, чи мотив нападу є «злочинним або геополітичним». Хоча список компаній, які підписали угоду є доволі довгим, кілька компаній її не підписали, принаймні поки що. До їх числа потрапили Google, Apple та Amazon.

Важливим є також і те, що жодна з компаній, яка долучилася до підписання спільної угоди, не представляла країни, з яких надходить найбільша кіберзагроза, такі як Росія, КНДР, Іран та Китай.

Нагадаємо: днями США та Британія опублікували своє перше попередження про кібератаки, які здійснює Росія.

Поштовхом до цього значною мірою послужили заяви президента та головного юрисконсульта Microsoft Бреда Сміта, який протягом останніх років твердить, що світу потрібна «цифрова Женевська конвенція», яка б встановлювала норми поведінки для кіберпростору так само, як Женевська конвенція встановлює правила ведення війни в фізичному світі.

На його думку, першими підтримати цю ініціативу мають американські компанії, оскільки саме вони та їхні клієнти найчастіше стикаються з кібератаками.

«Ця проблема стала набагато більшою, і я думаю, що за останні кілька років ми зрозуміли, що нам треба працювати разом і посилено», – зазначив він.

Компанія Microsoft зіграла центральну роль у спробі здолати атаку вірусом WannaCry минулого року, яка вразила британську систему охорони здоров'я та компанії по всьому світу. Адміністрація Трампа та уряди інших країн пізніше звинуватили в нападі Північну Корею. Минулого року атака вірусом NotPetya вразила Україну. Іран підозрюють у нещодавньому нападі на саудівський нафтохімічний завод.

Втім, не усі країни, імовірно, підтримають спільну угоду про кібербезпеку, частково тому, що принципи, які вона пропонуватиме, суперечитимуть їхнім власним секретним зусиллям створити кіберзброю.

(вгору)

Додаток 7

18.04.2018

Роскомнадзор в ярости: всё валится, а Telegram стоит, – правозащитник

Из-за действий Роскомнадзора многие россияне утратили доступ к банковским и торговым сервисам (InternetUA).

Попытка российских властей заблокировать мессенджер Telegram связана с желанием контролировать распространение информации в стране, заявил в комментарии изданию «ГОРДОН» российский политик и правозащитник Лев Шлосберг, информирует news.eizvestia.com.

«В мире существуют возможности, чтобы и дальше беспрепятственно заходить в Telegram. В моих каналах и группах в последние дни существенно увеличилось число участников. Мы не испытываем никаких проблем с коммуникацией. Попытка заблокировать Telegram не связана с желанием выполнять законодательство. Это чистая цензура. Спецслужбы хотят круглосуточно следить за российскими гражданами и читать переписку определенных людей. А Telegram стал одним из ведущих в РФ источником получения информации. В нем зарегистрирован каждый десятый житель страны – это политически значимая аудитория. Информацию в Telegram нельзя поддать цензуре. А это не входило в планы российских властей. Объем независимой политической, криминальной информации и сведений о преступлениях высших должностных лиц стал просто огромен», – подчеркнул Шлосберг.

По его словам, из-за действий Роскомнадзора многие россияне утратили доступ к банковским и торговым сервисам.

«Мы в два клика преодолели формальные преграды Роскомнадзора. Но при этом в своем стремлении заблокировать Telegram они похожи на питекантропов, пытающихся угнаться за сверхзвуковым самолетом. Это выглядит смешно. Роскомнадзор в ярости. Блокируются миллионы IP – люди утратили доступ к банковским и торговым сервисам. Все валится, а Telegram стоит. Что касается Facebook, то он, на мой взгляд, не несет такой угрозы властям РФ. Другое дело, что оттуда метлой вымели большое количество кремлевских троллей. Я охотно верю, что Роскомнадзор может попытаться заблокировать любые соцсети и мессенджеры, чьи базы данных хранятся за пределами России. Пока что мы видим абсолютное бессилие российского государства в борьбе с прогрессом», – сказал собеседник.

По его мнению, несмотря на блокирование, работу в России продолжат все мессенджеры.

«Действия государства, которые мы наблюдаем, просто стирают в пыль обещания президента РФ о продвижении и обеспечении цифрового прогресса в стране. Но в целом я бы к происходящему относился спокойно: разум все равно сильнее мракобесия. Думаю, все мессенджеры продолжат работать в России. Ведь для полной их блокировки страну нужно полностью отключить от интернета. Сложно сказать, готова ли нынешняя власть пойти на подобный шаг. Но экономические последствия такой блокады будут просто чудовищные.

Пока что мы видим сплочение российского гражданского общества из-за действий государства», – резюмировал Шлосберг.

(вгору)

Додаток 8

18.04.2018

Павел Дуров объявил о старте движения «Цифровое сопротивление» и пообещал гранты держателям прокси и VPN

Основатель Telegram Павел Дуров подвёл итоги первых суток с начала блокировки мессенджера в России и пообещал наградить держателей прокси и VPN-сервисов. На выплаты в рамках движения «Цифровое сопротивление» он собирается потратить «миллионы долларов» в 2018 году (IGate).

«Как показали последние сутки, в своей войне с прогрессом надзорные органы России готовы блокировать миллионы IP-адресов облачных хостингов, не считаясь с потерями посторонних проектов.

Помимо этого власти России борются и с независимыми сервисами прокси и VPN, многие из которых перестают работать (если это произошло, отключите прокси в настройках Telegram и попробуйте найти другой).

Хотя российский рынок не составляет существенной доли пользовательской базы Telegram, он важен нам по личным соображениям.

В рамках «Цифрового сопротивления» – децентрализованного движения в защиту цифровых свобод и прогресса — я начал выплачивать биткоин-гранты администраторам прокси и VPN. В течение этого года буду рад пожертвовать миллионы долларов личных средств на эти цели. Призываю всех присоединяться и участвовать – настройкой прокси/VPN серверов или их финансированием», – заявил Дуров.

Первое упоминание «Цифрового сопротивления» появилось в день блокировки Telegram, 16 апреля – Дуров опубликовал на своей странице во «ВКонтакте» рисунок собаки в капюшоне, подписав его фразой Digital Resistance. 17 апреля он добавил изображение с логотипом Роскомнадзора, стилизованным под флаг Третьего рейха.

В своём Telegram-канале Дуров сказал, что компания рассчитывает обходить блокировки с помощью услуг облачных сервисов, а также поблагодарил Google, Amazon и Microsoft за нежелание участвовать в «политической цензуре». Он заверил, что мессенджер не зафиксировал значительного падения активности пользователей.

«На Россию приходится около 7 % от общего количества пользователей, и даже если мы потеряем этот рынок целиком, наш органический рост в других регионах компенсирует эти потери за несколько месяцев. Но мне важно сделать всё для наших российских пользователей», – добавил он.

(вгору)

Додаток 9

23.04.2018
Владимир Кондрашов
ФБР ищет в Украине своего «контрагента»

Прокуратура США по Восточному округу штата Висконсин, Федеральное бюро расследований и Налоговая служба США проводят расследование относительно пользователя под псевдонимом «parkerproo». Хакера (или группу хакеров – Ред.) из Украины подозревают в нарушении уголовного законодательства США, а именно – в незаконном получении через компьютер персональных данных 1 тысячи человек, которые «parkerproo» рекламировал и продавал другим (InternetUA).

Об этом говорится в постановлении Шевченковского райсуда Киева, передает InternetUA.

Как стало известно, в рамках проводимого американцами расследования 8 февраля 2017 секретный агент ФБР приобрел похищенные федеральные налоговые формы W-2, что подаются в НС США, за 2016 фискальный год, которые рекламировал для продажи в сети «parkerproo». «Parkerproo» продал агенту ФБР за биткоины формы W-2 с персональными данными 7 человек. Позже, 21 и 22 февраля 2017, ФБР приобрело у «parkerproo» похищенные федеральные налоговые формы W-2 за 2016 фискальный год, содержащие персональные данные более 270 человек.

Во всех этих операциях агент ФБР передавал биткоины на «биткоин-адрес» предполагаемого злоумышленника. Когда криптовалюта поступала на его счет, «parkerproo» доставлял формы W-2 агенту ФБР через сайт sendspace.com. Точнее, «parkerproo» сообщал агенту ФБР, когда именно можно скачать формы с вебсайта, пользуясь несколькими унифицированными локаторами ресурса.

– Данные с вебсайта sendspace.com свидетельствуют, что похищенные налоговые формы, полученные ФБР от «parkerproo», были загружены на унифицированные локаторы ресурсов sendspace.com с компьютера, который использовал IP-адрес 188.163.81.167, – говорится в постановлении украинского суда.

Следственные органы США установили, что формы W-2, полученные от «parkerproo» секретным агентом, являются аутентичными налоговыми формами и содержат персональные данные граждан Соединенных Штатов. Примерно десяток форм W-2, полученных от «parkerproo», были похищены с предприятия, которое находится в Восточном округе штата Висконсин. Данные, полученные американским следствием, свидетельствуют, что с компьютера с IP-адресом 188.163.81.167 был осуществлен противоправный доступ к защищенному аккаунту, которым пользовалось это предприятие для составления налоговых деклараций.

Онлайновые источники свидетельствуют о том, что этот IP-адрес 188.163.81.167 зарегистрирован на ЧАО «Киевстар», в связи с чем у американцев возникла необходимость следственных действий на территории

Украины. Прокурор Киевской местной прокуратуры № 10 г. Киева Адский В.А. подал в суд ходатайство о временном доступе к вещам и документам, находящимися в собственности «Киевстар», по ходатайству компетентных органов Соединенных Штатов Америки об оказании международной правовой помощи по уголовному делу по факту незаконного доступа к персональным данным неустановленным лицом с псевдонимом «parkerproo».

– Информация, которую мы запрашиваем, поможет Органам США установить местонахождение и личные данные лица или лиц, причастных к совершению данного правонарушения, а также задокументировать их противоправные действия, – говорится в ходатайстве прокурора.

Суд ходатайство удовлетворил. На данный момент дальнейшая судьба «parkerproo» неизвестна.

(вгору)

Додаток 10

11.04.2018

7 млн пользователей загрузили фальшивые антивирусы из Google Play

Компания ESET сообщила, что ее специалисты обнаружили в Google Play 35 рекламных приложений, замаскированных под антивирусы. Подделки скачали в общей сложности до 7 миллионов пользователей (Компьютерное Обозрение).

Чтобы ввести в заблуждение пользователя, рекламные приложения имитируют настоящие мобильные продукты для безопасности. Однако их «механизмы детектирования» примитивны и неполны, что приводит к постоянным ложным срабатываниям, а настоящее вредоносное ПО легко избежит обнаружения.

Изученные приложения имитируют работу антивируса одним из четырех методов:

– Белые и черные списки приложений

В белые списки входят наиболее популярные программы (Facebook, Instagram, LinkedIn, Skype и др.), в черные – всего несколько приложений.

– Черные списки разрешений

Все приложения, включая легитимные, помечаются как вредоносные, если для работы им нужны некоторые из перечисленных, потенциально опасных разрешений (например, отправка и получение смс, доступ к данным о местоположении, доступ к камере устройства и др.)

– Белые списки ресурсов

Все приложения, кроме загружаемых из Google Play, помечаются как вредоносные (даже если они легитимны и безопасны).

– Черные списки активностей

Все приложения, выполняющие операции из заданного списка (например, показ рекламы), помечаются как вредоносные. В черный список входят и легитимные сервисы.

Несколько фальшивых антивирусов имеют характерные особенности. Один из них не является полностью бесплатным – в нем предусмотрен переход на коммерческую «расширенную версию». Еще одно приложение помечает остальные подделки как вредоносное ПО.

Часть приложений предлагает функцию менеджера паролей. Однако она не способна обеспечить защиту из-за небезопасного хранения данных – для злоумышленника не составит труда получить к ним доступ.

«В обнаруженных приложениях нет функции шифратора, банкера или других вредоносных возможностей, – отмечает Лукас Стефанко, вирусный аналитик ESET. – Они мешают пользователю ложными срабатываниями и показом рекламы, а также создают ощущение безопасности. Проблема в том, что миллионы неосторожных пользователей, загрузивших фальшивые антивирусы, легко могли бы установить настоящее вредоносное ПО, использующее ту же маскировку».

Антивирусные продукты ESET детектируют подделки как Android/Blacklister.A. Нежелательные приложения удалены из Google Play после уведомления со стороны ESET.

(вгору)

Додаток 11

12.04.2018

Масове шахрайство з банкоматами: що варто знати українцям

Шахраї встановлюють спеціальні пристрої на банкомати: кеш-треппінг, скіммінг і знімні клавіатури, крадуть інформацію з банківських карт або ж просто забирають готівку. Щорічно тисячі українців попадаються на вудку шахраїв, а пристрої для крадіжки інформацію стають все більш непомітними. За даними кіберполіції, в минулому році кількість крадіжок з банківських карт зросла на 70%. При цьому злочинці найчастіше користуються двома методами: крадуть гроші безпосередньо в банкоматі, або отримують інформацію про банківську карту по телефону (InternetUA).

«Обозреватель» розібрався, як впізнати “зіпсований” шахраями банкомат і не втратити свої гроші, передає Народна Правда.

Скіммінг і кеш-треппінг

Найпростіший спосіб вкрасти готівку з банкомату – встановити на вікно видачі коштів кеш-треппінг. Це спеціальна клейка стрічка, до якої прилипає частина купюр. За раз такий пристрій, як розповіли «Обозревателю» у одному з українських банків, може «затримати» до 1500 грн. Помітити таку стрічку складно, тому краще після того, як банкомат видав готівку, перерахувати її перед камерою на банкоматі. Якщо це технічна помилка, то її повинен буде

виправити банк, якщо ж частина грошей залишилося на кеш-треппінгу, то дістати стрічку можна буде самостійно.

У банку радять звернутися до співробітників фінустанови, набрати номер «гарячої лінії» і нікуди не йти. За допомогою такого пристрою вкрасти всі гроші з картки не вийде, тому кібепреступнікі придумали т.зв. скіммінг. Це магнітна стрічка, яка встановлюється в роз'єм для банківської карти.

Найчастіше в наборі з таким приладом йде панель з відеокамерою, спрямованою на клавіатуру, або ж спеціальна накладка на клавіатуру банкомату. Скіммінг копіює інформацію з магнітної стрічки банківської карти, а за допомогою накладки або камери злочинці дізнаються пароль від неї. Після цього вони можуть виготовити «двійник» справжньою банківської карти і зняти з неї всі кошти вже в працюючому банкоматі. У минулому році правоохоронці зняли з банкоматів близько 1000 подібних приладів.

Найчастіше зловмисники встановлюють їх на день або кілька годин, а потім знімають. Жертва дізнається про злочин тільки після того, як кіберзлочинці виготовляють карту і знімають з неї гроші. До того моменти скімінг з банкомату знімають.

Правда, іноді зловмисників вдається затримати на гарячому. Так, як повідомляють в поліції, в минулому році в Харкові вдалося затримати чоловіка в момент, коли він діставав з банкомату кеш-треппінг.

Як не попастися на вудку шахраїв

Найчастіше зловмисники використовують банкомати, які не перебувають під цілодобовим наглядом: на вулиці, в закритих від камер частинах торгових центрів і т.д. Тому кіберполіції рекомендує використовувати ті банкомати, які знаходяться у відділенні банків або в приміщеннях, які знаходяться під наглядом і закриваються на ніч.

Також важливо перед тим, як вставляти карту, уважно оглянути банкомат. На ньому не повинно бути сторонніх предметів, вікно для видачі готівки повинно бути порожнім, а на роз'ємі для банківських карт не повинно бути сторонніх предметів. При цьому важливо прикривати рукою клавіатуру при наборі пін-коду (на випадок, якщо зловмисники встановили камеру), а видані кошти перераховувати перед камерою банкомату. У такому випадку, якщо станеться технічний збій, співробітникам банку можна буде без перерахунку залишку довести, що банкомат не видав частина списаних грошей.

(вгору)

Додаток 12

15.04.2018

7 правил безопасности в социальных сетях

Скандал с аналитической компанией Cambridge Analytica, собравшей информацию о 87 млн пользователей Facebook, всколыхнул глобальную сеть. Вслед за возмущением пользователи соцсети устроили бойкот, а некоторые даже пошли на радикальные меры: покинули просторы Facebook. По

информации LikeFolio, в конце марта пользователи начали активно удалять аккаунты (InternetUA).

Не остались в стороне от скандала и чиновники. Сразу несколько госструктур, включая Федеральную торговую комиссию США и Офис комиссара информации Великобритании, начали расследовать, правомерно ли получение и использование такого количества информации о пользователях.

Рынок отреагировал на это, откатив стоимость акций Facebook сразу на 13%, пишет NBC News. Посыпались требования ввести общественный контроль за действиями Facebook. И пока буря вокруг Cambridge Analytica не утихла, попробуем разобраться, что можно сейчас сделать, чтобы уберечь свой аккаунт.

Отнеситесь к безопасности серьезно

Безопасность и социальные сети – вещи, на первый взгляд, если не противоположные, то, по крайней мере, сложно совместимые. Регистрируясь в социальной сети, пользователи, за редкими исключениями, не соблюдают анонимность. Мы делимся фотографиями, предпочтениями в музыке, подписками на интересующие страницы – все это элементы профайла, по которым нас найдут ваши друзья и знакомые… и маркетологи. А значит, всю эту информацию можно продать.

Проблема в том, что многие владельцы данных за деньги поделятся не только информацией о товарах, которые вы искали онлайн, но и более личными данными. Так что контент, который вы не готовы афишировать на весь мир, нельзя загружать в интернет вовсе: ни в закрытые альбомы, ни в личные сообщения, никуда. Отнеситесь к этому серьезно и определите для себя, какую информацию не жалко «слить» даже в самом худшем случае.

Не оставляйте страницы без присмотра

Сможете навскидку вспомнить, сколько и в каких социальных сетях вы создавали аккаунтов? А какая часть из них остались утерянными, заброшенными из-за забытого пароля? С ростом популярности соцсетей каждый такой аккаунт может представлять интерес для хакеров.

Получив доступ к заброшенному аккаунту, можно использовать его в дискредитирующей вас форме, публиковать с его помощью рекламную и не только информацию. Чтобы избежать этого, используйте инструменты для контроля сразу за несколькими аккаунтами. Это может быть, например, сервис Hootsuite или Socialbakers. Они позволят контролировать работу ваших страниц.

Следите, кого добавляете в друзья

По информации The Telegraph, Facebook признал, что 270 млн аккаунтов в социальной сети – фальшивые или дубликаты уже существующих. По определению Facebook, фальшивый аккаунт – это аккаунт, владелец которого выдает себя за кого-то несуществующего, или аккаунт выдуманного человека, животного, организации и знаменитости.

Опасность таких аккаунтов в том, что их часто используют для распространения рекламной информации, фейковых новостей и даже

пропаганды насилия и экстремизма. Наличие такого «друга» в вашей истории может негативно сказаться на репутации страницы или, что опаснее, использоваться для получения доступа к вашей персональной информации.

Используйте сложные пароли

Избегайте таких шаблонных решений, как непрерывная очередность цифр, последовательности простых символов, букв на клавиатуре. Не используйте в качестве пароля свое имя, фамилию, страну происхождения и все то, на что в первую очередь обратит внимание потенциальный взломщик вашего аккаунта.

В идеале пароль должен содержать хотя бы 10 символов. Это должна быть почти случайная комбинация букв в разном регистре, цифр и специальных символов. Чтобы запомнить такую сложную последовательность, можно, к примеру, создавать пароль по принципу аббревиатуры. Придумайте фразу (можно абсурдную, смешную) и используйте в качестве пароля первые буквы слов. Дополните цифрами и другими символами. И, конечно, никому не рассказывайте о своем шифре.

Еще один способ – использовать менеджеры паролей вроде Splashdata. Они помогут и подобрать эффективные пароли, и сохранить их.

Настройте двухфакторную аутентификацию

Еще один инструмент, позволяющий повысить уровень безопасности для страницы в социальной сети, – двухфакторная аутентификация. Facebook так описывает эту функцию: «Двухфакторная аутентификация – это функция безопасности, которая помогает защищать аккаунт Facebook в дополнение к защите паролем».

Суть в том, что кроме пароля понадобится еще одно подтверждение входа. Данная социальная сеть предлагает несколько вариантов такой верификации: текстовые сообщения с кодом на телефон, коды безопасности из генератора кодов или стороннего приложения, одобрения попытки входа с другого, уже распознанного устройства и даже 10 кодов, которые вы можете распечатать и носить с собой.

Читайте пользовательские соглашения

Обязательно ознакомьтесь с правилами социальной сети, в которой регистрируетесь, прежде чем создать аккаунт. Особое внимание уделите принятой в данной сети политике безопасности. Настройте параметры безопасности под себя.

Как минимум, вы можете сделать записи приватными и запретить доступ к данным различным приложениям. К слову, о приложениях: когда устанавливаете аппликейшн на телефон или планшет, не забывайте проверять, какие доступы он запрашивает. Если не понимаете, зачем нужен определенный доступ (например, зачем плееру использовать телефонную книгу), то лучше от этого приложения отказаться.

Не делитесь конфиденциальной информацией

Не используйте страницу в социальной сети для регистрации на сайтах, которые запрашивают доступ к вашей личной информации и информации о

ваших друзьях. Многие сайты сейчас предлагают авторизоваться через соцсети, чтобы проголосовать в опросе, оставить комментарий или узнать результаты какого-нибудь теста. Поберегите данные, обойдитесь без информации о том, каков ваш психологический возраст или кто вы из героев «Гарри Поттера».

Кроме того, не анонсируйте на странице свои планы. Информацией о том, что вы в ближайшие выходные собираетесь в другую страну, могут воспользоваться квартирные грабители.

Всегда обращайте внимание на то, что вы публикуете и чем делитесь на своей странице. Не делитесь запрещенным или подозрительным контентом. Следите за комментариями. Речь не только о комментариях, которые вы оставляете на других ресурсах, но и о комментариях, который другие оставляют на вашей странице. Иногда худший удар по онлайн-репутации наносят не взломы и «сливы» данных, а необдуманные шутки, в которых кто-то может увидеть грубость, или неосторожные высказывания ваших же друзей.

(вгору)

Додаток 13

16.04.2018

Михаил Сапитон

Telegram – новый источник пиратского контента

Издание The Outline обратило внимание на то, что пользователи Telegram используют мессенджер для загрузки пиратского контента. Количество каналов с нелегальными копиями фильмов, музыкальных альбомов, приложений и прочего перевалило за тысячи. Редакция AIN.UA приводит сокращенный перевод материала (AIN.UA).

Автор текста Мариша Сингх пообщалась с владельцами пиратских каналов – они утверждают, что не встречали никакого сопротивления со стороны сервиса. При этом Telegram, как и Google с Facebook, формально придерживается политики «нулевой толерантности» по отношению к нарушениям копирайта.

В то время как некоторые каналы получили более 100000 подписчиков, распространяя музыку, фильмы и телешоу, компания забанила всего несколько сотен пиратов, даже не догадываясь о масштабе проблемы. Мариша приводит следующий пример: свежую премьеру от Netflix, научно-фантастический фильм «Аннигиляция» можно было скачать, просто вбив в глобальный поиск запрос «Netflix» и перейдя по первой ссылке (сейчас поиск выдает другие результаты – прим. ред.).

Ситуация стала «открытым секретом» – многие пользователи, ежедневно пользующиеся услугами пиратских каналов, не говорят об этом публично, опасаясь их закрытия. Не догадываются об этом и те, кто не знаком с особенностями глобального поиска – в описании инструмента не указано, что он, в том числе, ищет по открытым каналам и медиафайлам в них.

Популярность пиратства во многом упирается в простоту использования мессенджера – файлы можно загружать напрямую с сервера компании, по одному тапу. Торрент-трекеры, для сравнения, требуют установки дополнительного ПО. Это отметил в комментарии Сингх анонимный пользователь мессенджера из России: «Думаю, люди полюбили простоту Telegram, его схожесть с сайтами 1990-2000-х годов, когда интернет действительно был островом свободы для всех».

The Outline пообщались с 13-ю администраторами и владельцами пиратских каналов. Они объяснили – приложение удобно из-за возможности сохранять анонимность и отсутствия контроля. Один из админов, который уже два года ведет канал с новыми болливудскими фильмами, сравнивает: «Facebook регулярно банит наши группы, Telegram не делает ничего подобного». Поскольку приложение имеет только лимит на размер одного файла (1,5 ГБ), но не ограничивает их количество, это тоже развязывает администраторам руки. Автор канала с болливудским кино, по собственным подсчетам, загрузил на сервера Telegram более 10 Тб контента. Сингх отмечает: сжатый при помощи кодека HEVC двухчасовой фильм, с битрейтом от 400 Кб/с до 2 Мб/с, укладывается в этот лимит.

Некоторые зарабатывают на платформе деньги – среди таких, например, автор канала по продаже обучающих курсов с ресурсов Lynda, Udemy, Masterclass и The Teaching Company. Активизировался на платформе и рынок по продаже учетных данных для популярных сервисов. Ранее такая деятельность велась на подпольных форумах или в даркнете, но Telegram предоставил более удобный способ найти аудиторию. Сингх смогла получить более трех десятков паролей и логинов для Netflix, Spotify, Hulu, HBO, CBS, EA Sports, Lynda, Sling, WWE Network, Mega и других сервисов – все они скомпрометированы в ходе предыдущих утечек информации, что проверялось по сайту Have I Been Pwned. При этом, несмотря на публичную известность каналов с подобной информацией, их не закрывают.

Сингх указывает, что одним из немногих публичных действий сервиса стал прошлогодний бан музыкального канала «Всякая годная попса». Его создатель, россиянин Антон Вагин, рассказал, что не получил никаких уведомлений от сервиса: «В один момент я просто увидел, что мой канал забанили, вот и все».

The Outline также пообщались с авторами музыки, чьи работы размещаются в пиратских каналах – по их словам, они отправляли репорты в Telegram и «выражали недовольство» Apple по поводу доступности приложения в App Store и Mac App Store. Пресс-секретать Telegram Маркус Ра ответил на запрос журналистов следующим образом: «Мы постоянно улучшаем свои инструменты для модерации публичного контента».

Apple, при этом, уже удаляла официальный и альтернативный клиенты Telegram и Telegram X из App Store – в феврале они пропали из электронного магазина на день. Тогда причиной послужил некий «недопустимый контент», но уже через день программы вернулись в магазины.

Наконец, Сингх цитирует твит Павла Дурова, который в декабре 2017-го указывал: его компания не ограничивает пользователей, пока те не начнут выражать публичные призывы к насилию, распространять порнографию или контент, нарушающий авторские права.

Информация о рекламе в Твиттере и конфиденциальность

И даже к этим ограничениям нас принуждают мобильные платформы, угрожая удалить Telegram из App Store и Google Play, за то что мы слишком либертарианские. На самом деле, вы не можете получить больше свободы, чем в приложения Telegram на iOS и Android.

(вгору)

Додаток 14

17.04.2018

Check Point: 97 % компаний не готовы к кибератакам «Пятого поколения»

Check Point Software представил результаты исследования 2018 Security Report. В отчете представлены киберугрозы, с которыми сталкиваются организации различных отраслей (ITnews).

2018 Security Report опирается на данные многочисленных исследований среди ИТ-директоров и руководителей бизнеса, а также отчетов Check Point's Threat Cloud и Threat Intelligence Report. Исследование охватывает все современные угрозы, направленные на различные отрасли, такие как здравоохранение, промышленность и государственные структуры. Согласно отчету 2018 Security Report, более 300 мобильных приложений, распространяющихся через официальные магазины, содержат вредоносный код. Также специалисты Check Point отмечают, что количество облачных угроз, атак криптомайнеров, уязвимостей MacOS и IoT-устройств продолжает расти.

«Сегодня мы наблюдаем новое поколение кибератак – это многовекторные, крупномасштабные и стремительно распространяющиеся атаки "Пятого поколения" (GenV), – отмечает Питер Александер, директор по маркетингу Check Point Software Technologies. – 77 % ИБ-директоров выразили обеспокоенность тем, что организации не готовы к таким современным кибератакам и что подавляющее большинство инфраструктур безопасности компаний безнадежно устарели».

Чтобы получить больше информации о современном ландшафте киберугроз, Check Point опросил 443 ИТ и ИБ-специалистов по всему миру о вызовах, с которыми они сталкиваются, отражая атаки «Пятого поколения». Результаты исследования показали, что защита большинства компаний отстаёт на 10 лет и как минимум на два поколения от современных кибератак Gen V. Это говорит о глобальной повсеместной уязвимости перед атаками «Пятого поколения». Эксперты Check Point подготовили 2018 Security Report, который содержит сведения, решения и рекомендации для предотвращения кибератак «Пятого поколения».

«Согласно данным 2018 Security Report, кибератаки Gen V становятся все более частыми, – отметил Дуг Кахил, руководитель группы и старший аналитик по кибербезопасности Enterprise Strategy Group. – Риску подвержены все: медицинские учреждения, государственные сервисы, крупные корпорации и т.д. Сегодня 97 % компаний не обладают решениями, способными противостоять кибератакам Gen V, и это нужно менять».

(вгору)

Додаток 15

17.04.2018

Киберполиция предупредила о масштабной вирусной рассылке в «Фейсбуке» от друзей

Правоохранители предоставили рекомендации пользователям Google Chrome: как удалить вирусные приложения (InternetUA).

В Интернете зафиксировано массовое распространение вируса через социальную сеть Facebook. Впервые он был зафиксирован в 2017 году, а сейчас распространяется по всему миру, в том числе и на территории Украины.

Об этом сообщила пресс-служба национальной полиции Украины со ссылкой на Департамент киберполиции.

Так, спам-сообщения с «вирусной» ссылкой направлялись пользователям Facebook`а от имени их друзей. В сообщениях указывалась ссылка на специально подготовленную страницу, имитирующую видеохостинг и предлагающую добавить в Google Chrome приложение для получения возможности просмотра этого видео.

Этот тип вируса распространяется с целью майнинга непосредственно в браузере пораженного компьютера, пользуясь его ресурсами. Размещенный в веб-магазине Chrome плагин только за четверо суток набрал 30.000 загрузок.

Специалисты по киберполиции отмечают, что в случае получения подобного сообщения необходимо максимально быстро предупредить об этом пользователя, с аккаунта которого распространяется такая информацию. У себя такое сообщение нужно обозначить как спам.

«Этот вирус может похитить данные, которые пользователь вводит в формы на сайтах, включая логины и пароли на всех страницах. Выявлено, что этот тип вируса распространяется с целью майнинг непосредственно в Вашем браузере, пользуясь ресурсами Вашего компьютера», – сообщили в киберполиции и предоставили рекомендации по удалению вирусного приложения.

Это стандартное Google Chrome приложение, которое можно удалить по стандартной процедуре:

– В углу экрана нажмите «Панель запуска» – стрелка вверх.

– Правой кнопкой мышки нажмите на приложении, которое нужно удалить.

– Нажмите «Удалить».

– Еще раз нажмите «Удалить».

Как удалить расширение:

– Откройте Chrome.

– Нажмите на значок с тремя точками – Инструменты – Расширения.

– Нажмите значок «Удалить» возле расширения.

– Для подтверждения нажмите «Удалить».

Совет: чтобы удалить расширение со значком на панели инструментов браузера, нажмите значок правой кнопкой мышки и выберите опцию «Удалить» из Chrome.

(вгору)

Додаток 16

18.04.2018

8 из 10 организаций обеспокоены проблемой соблюдения сотрудниками политики безопасности

Корпорация Oracle и аналитическая компания KPMG недавно провели глобальный опрос 450 ИТ-специалистов. Он показал, что организации всеми силами пытаются защитить свои данные на фоне растущего числа нарушений безопасности. Согласно результатам отчета «Cloud Threat Report, 2018», 90 % специалистов по информационной безопасности классифицируют более половины своих данных, хранимых в облаке, как конфиденциальные. Более того, 97 % опрошенных разработали правила использования облаков, однако подавляющее большинство (82 %) обеспокоены тем, соблюдают ли сотрудники эти правила (Компьютерное Обозрение).

Расширенная стратегия безопасности имеет ключевое значение для мониторинга и защиты данных для предприятий, хранящих конфиденциальные данные в облаке. Действительно, 40% респондентов указывают, что выявление инцидентов, связанных с облачной безопасностью, и реагирование на них в настоящее время является главной задачей в области ИБ. Чтобы решить ее, 4 из 10 опрошенных компаний предпринимают такие меры, как найм архитекторов по облачной безопасности, а 84% респондентов для эффективной защиты от сложных угроз идут по пути повышения автоматизации.

Другие ключевые выводы:

- Изменение ландшафта угроз создает новые проблемы: лишь 14 % опрошенных сообщили, что могут эффективно анализировать события безопасности, касающиеся большей части (75-100 %) своих данных, и эффективно реагировать на них.
- Рост расходов на обеспечение кибербезопасности: 89 % респондентов ожидают увеличения инвестиций в кибербезопасность в своей организации в следующем финансовом году.
- Несогласованность в облачных политиках: 26 % респондентов считают одной из главных проблем отсутствие единой политики в разветвленной инфраструктуре.

- Переосмысление облачных стратегий при изменении нормативных правил: Общий регламент по защите данных (General Data Protection Regulation, GDPR) будет влиять на выбор облачной стратегии и поставщиков услуг. Так считают 95 % респондентов, которые должны соблюдать нормативные требования.
- Мобильность усложняет задачи управления идентификацией и доступом (Identity And Access Management, IAM) в организациях: 36 % респондентов заявили, что использование мобильных устройств и приложений затрудняет контроль и мониторинг доступа.
- Машинное обучение в помощь: 29 % опрошенных практикуют ограниченное использование машинного обучения, 18 % – расширенное, а еще 24 % теперь дополняют возможностями машинного обучения существующие инструменты безопасности.

(вгору)

Додаток 17

18.04.2018

Android-троянец из Google Play подписывал пользователей на платные мобильные услуги

Вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play троянца Android.Click.245.origin, который по команде злоумышленников загружает сайты, где пользователей обманом подписывают на платные контент-услуги. В некоторых случаях оформление подписок выполняется автоматически после нажатия мошеннической кнопки для «скачивания» программ (Компьютерное Обозрение).

Злоумышленники распространяли Android.Click.245.origin от лица разработчика Roman Zencov и маскировали троянца под известные приложения. Среди них – еще не вышедшая на платформе Android игра Miraculous Ladybug & Cat Noir, нашумевшая в начале весны программа GetContact для звонков и работы с телефонными контактами, а также голосовой помощник Алиса, который встроен в приложения от компании «Яндекс» и как отдельное ПО пока недоступен. Одна из троянских программ входила в тридцатку наиболее популярных новинок каталога Google Play.

Специалисты «Доктор Веб» уведомили корпорацию Google об Android.Click.245.origin, после чего он был удален из каталога. В общей сложности приложения-подделки успели установить свыше 20 000 пользователей. У всех этих программ нет никаких полезных функций. Их основная задача – загрузка веб-страниц по команде злоумышленников.

После запуска Android.Click.245.origin соединяется с управляющим сервером и ожидает от него задания. В зависимости от IP-адреса подключенного к сети зараженного устройства троянец получает ссылку на определенный сайт, который необходимо загрузить. Вредоносная программа переходит по полученной ссылке и с использованием WebView отображает

нужную киберпреступникам страницу. Если мобильное устройство подключено к Интернету через Wi-Fi, пользователю предлагается установить интересующее приложение, нажав на соответствующую кнопку. Например, если жертва запускала программу-подделку голосового помощника Алиса, для «скачивания» может быть подготовлен файл под названием «Alice Yandex.apk».

При попытке загрузки файла у владельца устройства запрашивается номер мобильного телефона для некоей авторизации или подтверждения скачивания. После ввода номера пользователю отправляется проверочный код, который необходимо указать на сайте для завершения «загрузки». Однако никаких программ после этого жертва не получает – вместо этого она подписывается на платную услугу.

Если же зараженное устройство подключено к Интернету через мобильное соединение, загружаемый троянцем сайт выполняет несколько перенаправлений, после чего Android.Click.245.origin открывает конечный адрес в браузере Google Chrome. На загружаемой странице для скачивания некоего файла пользователю предлагается нажать на кнопку «Продолжить», после чего он перенаправляется на другой сайт, с которого якобы и происходит загрузка. После нажатия на кнопку «Начать загрузку» жертва с использованием технологии Wap-Click автоматически подписывается на одну из дорогостоящих услуг, за использование которой каждый день будет взиматься плата. При этом доступ к таким сервисам предоставляется без предварительного ввода номера телефона и кодов подтверждения из СМС.

Подключение ненужных контент-услуг – один из самых распространенных и давно известных способов незаконного заработка злоумышленников. Однако оформление таких премиум-подписок через сервис Wap-Click представляет особую опасность, т. к. фактически происходит без какого-либо явного информирования абонентов и часто используется недобросовестными контент-провайдерами.

(вгору)

Додаток 18

23.04.2018

За 2017 год случаи скрытого майнинга участились в 340 раз

Случаи скрытого майнинга растут в геометрической прогрессии. По данным антивирусной компании Symantec, за 2017 год они участились в 340 раз (InternetUA).

Только в марте 2018 года, согласно отчету антивирусной компании Malwarebytes, было зафиксировано 16 млн попыток скрытого майнинга криптовалют. За первые три месяца 2018 года количество таких случаев выросло на 4000 % по сравнению с предыдущим кварталом.

В то же время, отмечают исследователи, на 35 % снизилось число атак с участием вирусов-вымогателей. Хотя еще недавно такие атаки были наиболее популярными – вспомнить хотя бы нашумевшие вирусы WannaCry и Petya.

Согласно исследованию Национального центра кибербезопасности Великобритании, скрытый майнинг будет главной угрозой для интернет-пользователей как минимум в ближайшие два года.

Как уточняется, скрытый майнер – stealth miner, майнер-бот, ботнет – программа, которая в автоматическом режиме ведет майнинг незаметно для пользователя. Это стороннее программное обеспечение, которое устанавливается на компьютер, использует его ресурсы и перечисляет заработок на кошелек разработчика. Жертвой скрытого майнера может стать каждый. Под угрозой – не только серверы крупных компаний, но и домашние компьютеры, особенно игровые. Майнеры работают на всех платформах, устройствах, операционных системах и браузерах. Следовательно, от них не защищен никто.

Согласно рекомендациям ISSP, следует проверить «Диспетчер задач», где при наличии майнера будет отображаться большой процент загрузки центрального или графического процессоров – в пределах от 70 % до 100 %.

Первые симптомы присутствия майнера – сбои в работе информационной системы, быстрая разрядка аккумулятора и перегрев устройства, наличие запущенных подозрительных процессов, нетипичное повышение громкости работы видеокарты, повышение уровня используемой электроэнергии.

Специалисты ESET рекомендуют устанавливать и использовать актуальные версии антивирусов, которые блокируют угрозы на этапе загрузки. Если компьютер все же был инфицирован, нужно выполнить его полное сканирование и удалить нежелательные и потенциально опасные программы.

При попадании на инфицированный сайт нужно его закрыть и очистить кэш браузера. Если указанный сайт был добавлен в закладки, его следует удалить. Если пользователь столкнулся с ботнетом, который не поддается этим мерам, то лучше обратиться к специалисту, чтобы не усугубить ситуацию.

Для сканирования устройства на наличие вредоносного ПО можно использовать бесплатную утилиту Malwarebytes и ее дополнение AdwCleaner.

Первое приложение проверяет жесткий диск и оперативную память на наличие вирусов, второе – на рекламные программы. Регулярное сканирование с большой вероятностью обезопасит гаджеты от скрытого майнинга.

Как одну из мер предосторожности в браузере можно использовать расширения ScriptBlock, NoCoin и MinerBlock, которые блокируют пиратские скрипты и останавливают потенциально опасные алгоритмы.

(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.