СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(9.05–23.05)

2018 № 10

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(9.05–23.05)
№ 10

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

10.05.2018

В Android-приложении Twitter обнаружена скрытая функция

В Android-приложении Twitter обнаружена скрытая функция «секретного чата», который позволит пользователям отправлять зашифрованные с помощью технологии сквозного шифрования сообщения (InternetUA).

Функция обмена зашифрованными сообщениями была впервые обнаружена в APK-файле Twitter исследователем Джейн Манчун Вонг (Jane Manchun Wong). APK-файлы часто содержат код функций, которые компании тестируют перед запуском.

Представители пресс-службы Twitter никак не прокомментировали ситуацию. В настоящее время неясно, когда именно будет официально запущена данная функция.

***

13.05.2018

Facebook запустила сервис «Проверка безопасности» после нападения с ножом в Париже

Социальная сеть Facebook активировала услугу «Проверка безопасности» (Safety Check) в Париже после нападения с ножом, совершенного в центре города в субботу вечером. Об этом сообщил телеканал BFM TV (InternetUA).

Отмечается, что пользователи сети после произошедшего в Париже могут предложить или получить помощь, а также сообщить своим близким о том, что их жизни ничто не угрожает. Кроме того, опция позволяет пользователям социальной сети оперативно дать знать, что они уцелели в случае теракта, стихийного бедствия или катастрофы.

***

15.05.2018

YouTube предложит сделать паузу

Новая версия мобильного YouTube начала напоминать пользователям, которые смотрят видео в течение длительного времени, о необходимости сделать перерыв. Функция «Напоминать мне, что нужно отдохнуть от просмотра» уже появилась в Android- и iOS-версиях приложения (InternetUA).

Пользователи могут настроить таймер на 15, 30, 60, 90 или 180 минут. По истечении заданного времени воспроизведение ролика будет приостановлено, а на экране появится напоминание с предложением немного отдохнуть. Счетчик

также учитывает время, когда приложение закрыто или видео поставлено на паузу.

Чтобы активировать функцию, нужно нажать на иконку профиля, открыть «Настройки» и перейти на вкладку «Общие». При желании оповещение можно пропустить либо вовсе отключить.

YouTube стала первой программой, которая воплощает идею «цифрового здоровья» (Google Wellbeing). Эта концепция, направленная на формирование у пользователя полезных привычек, была изложена на прошлой неделе на конференции Google I/O.

В Android P, которая выйдет этой весной, одним из проявлений Google Wellbeing станет новая информационная панель, показывающая, когда, как часто и как долго запускались те или иные приложения. Появится возможность ограничить время использования программ: например, на Instagram можно будет установить получасовой лимит в сутки, после чего его иконка станет черно-белой.

***

16.05.2018

Скоро в Instagram появится невероятно полезная функция

Instagram тестирует несколько новых функций для мобильных приложений сервиса. В скором времени пользователи получат инструмент Usage Insights, позволяющий следить за временем, потраченным в социальной сети, боковую панель с быстрым доступом к некоторым разделам, а также кнопку для мгновенного импорта сториз в «Истории» Facebook (InternetUA).

Во вкладке Usage Insights пользователь сможет посмотреть, сколько времени он провел за просмотром основной ленты, «Историй» или в сообщениях Direct. Также функция позволит установить временные рамки на использование сервиса, например, приложение не даст листать основную ленту более 30 минут в день. Очень крутая фишка для тех, кто хочет сократить время своего прибывания в соцсетях.

Также в приложения сервиса будет добавлено новое меню, вызвать которое можно с главного экрана. На момент запуска нововведения в нем будут расположены четыре кнопки: архив сториз, сохраненные публикации, раздел «Интересные люди» и функция Usage Insights.

В меню опубликованных «Историй» появится кнопка «поделиться в Facebook». Одним нажатием пользователи смогут мгновенно расшарить сториз из Instagram в свой аккаунт Facebook. Это нововведение было анонсировано еще в 2017 году, но появится в сервисе только сейчас.

***

16.05.2018

Telegram сохранил основную аудиторию в России за месяц блокировки властями

По данным аналитической компании SimilarWeb на 14 мая приложение Telegram было установлено на 20,47 % всех устройств, работающих на платформе Android в России (InternetUA).

На 16 апреля, когда мессенджер начали блокировать в России, этот показатель составлял 19,9 %, передает БизнесЦензор со ссылкой на РБК.

По данным SimilarWeb, из тех, у кого было установлено приложение, его использовали 31,7 % пользователей против 51,59 % 16 апреля.

SimilarWeb не анализирует показатели для iOS. Но, по данным Deloitte, более 70 % основных телефонов пользователей в России на середину 2017 года были именно на Android.

При этом аудитория популярных Telegram-каналов не снизилась, а наоборот, увеличилась. В частности, с 13 апреля по 16 мая количество подписчиков канала «Сталингулаг» выросло на 18,5 %, до 287 тыс. человек.

Однако в исследовании сервиса аналитики Telegram-каналов TGStat.ru отмечается, что активная аудитория Telegram за месяц после блокировки снизилась на 7 п.п. Сервис проанализировал 2,8 млн подписчиков каналов: в период со 2 по 8 апреля 82 % аудитории мессенджера была активной, то есть заходила в сервис хотя бы один раз в течение недели. С 7 по 13 мая этот показатель составлял 75 %.

***

16.05.2018

В WhatsApp появились новые функции, аккуратно украденные из Telegram

WhatsApp в своем блоге анонсировала крупное обновление мессенджера для iOS и Android. Нововведения коснулись только групповых чатов. В компании выделяют пять новых функций (InternetUA):

•Описание группы. Теперь при подключении к группе новые участники увидят ее описание в верхней части экрана. Создатель сообщества в краткой аннотации может описать ее цели, правила или основные темы.

•Функции управления для админов. У администраторов группы появилась возможность контролировать в настройках, кто может изменять тему, картинку и описание чата.

•Наверстать упущенное. Если пользователь долго отсутствовал в групповом чате, он сможет быстро просмотреть сообщения, адресованные ему. Для этого появилась предназначена кнопка «@».

•Поиск участника. Профиль любого участника можно найти по имени через поиск на странице информации о группе.

•Теперь админы могут лишать прав на управление группой других участников, а создателей чатов больше нельзя удалить.

Примечательно, что все функции, появившиеся сегодня в WhatsApp, уже давно есть в Telegram – одном из главных конкурентов мессенджера. В

будущем в WhatsApp будут добавлены стикеры, которые также уже несколько лет присутствуют в Telegram.

***

21.05.2018

YouTube будет показывать какие аудиотреки звучат в видео

YouTube станет показывать подробную информацию о музыке, которая звучит в видеороликах. Для этого сервис будет использовать платформу Content ID, которая автоматически определяет контент, защищённый авторским правом, и позволяет владельцам композиций принимать дальнейшие решения (IGate).

«YouTube стремится к признанию всех людей, который вносят вклад в творческий процесс, и это лишь начало, – написала компания. – С помощью наших партнёрств мы расширим масштабы и улучшим качество данных, чтобы все авторы получали столько, сколько им положено».

Нажав на кнопку «Ещё» под роликом, вы увидите полный список людей, которые создавали и лицензировали композицию. Это касается всех видео, будь то официальный клип или любительская видеозапись с музыкой на фоне. В последнем случае в описании можно будет обнаружить ссылку на официальный клип. Если песня доступна в каком-либо из сервисов Google, то вы без проблем найдёте соответствующую ссылку.

Компания хочет привлечь к сервису как можно больше исполнителей, лейблов и издателей, а затем продемонстрировать им серьёзность своих намерений в плане выплат. Как минимум отчасти это связано с тем, что Google как раз анонсировала музыкальный потоковый сервис YouTube Music, который станет доступен на следующей неделе.

***

21.05.2018

WhatsApp обогнал социальные сети по количеству просмотров Stories

Сначала Instagram «украл» идею с исчезающими историями у Snapchat. Затем Facebook добавил точно такую же функцию в свое приложение и на сайт. Позже всех добавил возможность создания исчезающих Stories мессенджер WhatsApp, который сейчас, на удивление, обходит по просмотрам всех своих предшественников (Телекритика).

На сайте TechCrunch были опубликованы данные о просмотрах историй в различных соцсетях и мессенджерах.

Так Snapchat, «отец» функции Story, оказался всего лишь на третьем месте – ежедневно истории в этом приложении смотрят 191 миллион человек.

На втором месте – Instagram с 300 миллионами ежедневных просмотров историй.

На первом месте оказался WhatsApp – истории (или статусы) в мессенджере смотрят 450 миллионов человек ежедневно.

Казалось бы, почему именно WhatsApp просматривают больше? Возможно, это связано с тем, что в мессенджере отсутствует реклама (только если у вас нет чатов с компаниями, которые постят истории с рекламой товаров или услуг). Второй причиной может быть то, что статусы в WhatsApp состоят из историй, которыми делятся наши друзья и родственники, что делает этот контент более привлекательным.

***

22.05.2018

В WhatsApp скоро появятся групповые звонки

Групповые звонки WhatsApp – одна из тех функций, которые были анонсированы во время конференции Facebook F8 2018 в начале мая (IGate).

Компания без сомнения, проверяет эту функцию и наблюдает за проблемами, с которыми она может столкнуться при полноценном запуске. Поэтому возможность протестировать новинку появилась лишь у ограниченного количества пользователей.

Существует метод, с помощью которого можно проверить, доступны ли групповые звонки или нет. Необходимо просто сделать видеовызов кому-то, и если функция присутствует, во время разговора на экране появятся новая кнопка. Кнопка называется «Добавить участника» и позволяет добавить других пользователей.

Доступ к групповым звонкам для всех пользователей может занять некоторое время. В общей сложности 4 человека могут принимать участие в видеозвонке одновременно.

Другая функция, которая засветилась на F8 для WhatsApp – возможность прикреплять стикеры. Сейчас она находится на стадии бета-тестирования в Android и нет никаких сведений о возможной дате релиза.

***

22.05.2018

Скандал с Cambridge Analytica позитивно отразился на посещаемости Facebook

Скандал крупнейшей социальной сети с британской аналитической компанией, которая хранила и анализировала данные около 80 млн пользователей Facebook без их ведома, увеличил посещаемость социальной сети на 7 % (Телекритика).

Как сообщает американский инвестиционный банк Goldman Sachs в апреле посещаемость Facebook выросла до 188,6 млн уникальных пользователей мобильных устройств.

Помимо этого, увеличилось и количество времени (в среднем более 35 минут в день), которое люди проводят в соцсети. В процентном отношении это составляет около 20 %.

Решение Facebook удалить 583 млн фейковых аккаунтов, связанных с вмешательством России в президентские выборы в США, также не сыграло большой роли, практически никак не повлияв на охват аудитории.

***

23.05.2018
В Instagram появилась кнопка «Игнорировать»

Социальная сеть представила новую функцию, которая позволяет прятать посты и Stories от определенных аккаутов, не отписываясь от них. Пользователи теперь смогут сами выстраивать свою ленту, чтобы доступная им информация была «более персонализируемой». Юзеры смогут видеть посты на странице профиля и получать уведомления о комментариях и постах, на которых были отмечены. Сами аккаунты не будут знать, что их поставили в режим игнорирования. Чтобы воспользоваться функцией необходимо нажать на значок '…' в верхнем правом углу поста и выбрать, игнорировать только посты или посты и Stories профиля (Marketing Media Review).

***

23.05.2018
В Instagram появилась самая важная функция

В версии обновления Instagram 46.0 появилась новая возможность, позволяющая фильтровать комментарии, которые задевают или оскорбляют пользователей (InternetUA).

«Наше Руководство сообщества прямо запрещает травлю в Instagram, и мы приложим все усилия, чтобы устранить эту проблему», – сказано в послании разработчиков.

Представители Instagram обещают, что новая функция позволит сделать использование соцсети еще приятнее и улучшит обстановку.

«Уверены: вместе мы сможем поддержать дружелюбную и позитивную атмосферу в Instagram», – подчеркнули они.

Включить модерацию можно изменив соответствующие настройки в разделе «Комментарии». Там можно составить список недопустимых слов или использовать список по умолчанию.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

15.05.2018

Ради спасения украинского моряка от казни одесситы публикуют фото в сети и собирают подписи под петицией // Украинцу, которого подозревают в убийстве матроса, грозит казнь

Одесситы запустили в сети флешмоб в поддержку моряка Андрея Новичкова, который уже полтора года находится под следствием в Иране по обвинению в убийстве матроса. По словам близких подозреваемого и правозащитников, Андрея считают повинным в случившемся лишь потому, что он последним видел погибшего матроса в живых и был единственным «не мусульманином» на судне. Ему грозит смертная казнь (Сегодня).

Пользователей соцсетей просят публиковать свои фото с призывами помочь Новичкову. Цель акции – распространить информацию о моряке и собрать 25 тысяч подписей под петицией к президенту, которая призывает решить проблему на дипломатическом уровне.

За первые два дня петицию подписали больше 3000 человек. Ее авторы утверждают, что по закону шариата Новичкову грозит «кисас» – «воздаяние равным за равное». Подписать документ можно на сайте президента.

***

14.05.2018

Теперь в Facebook и Instagram можно будет увидеть фотографии родов

Отныне в популярных соцсетях больше не будут цензурировать фотографии деторождения (Телекритика).

Это стало возможным благодаря активистке Кэти Вигос, которая продвигает проект о рождении Empowered Birth Project. Петицию, которую запустила Вигос, на сегодняшний день подписали более 23 тысяч человек. Там говорится, что ранее социальные сети приравнивали фотографии родов к «порнографическим снимкам, изображениям сцен насилия и нецензурной брани».

***

20.05.2018

Соцсети потешаются над безлюдным Крымским мостом

В сети пользователи отреагировали на публикацию фотографий построенного оккупантами Крымского моста, на котором нет ни одного автомобиля (InternetUA).

Снимки опубликовала на своей странице в Twitter пользователь RoksolanaToday&Крым.

«Мне не интересно, но Госдеп требует. Вчерашние (за 18 мая. – Ред.). Только для эвакуации нужен из Крыма. Пока не спешат. Увы...», – сказано в сообщении.

«Приготовили путь для быстрого исчезновения в критический момент... Наверно, думают удирать очень скоро, потому как данное сооружение проживет до первого сезонного катаклизма осень-зима; зима-весна....», – написала Светлана.

«В первый день многие сделали 2-3 оборота (набили статистику)», – пояснил пользователь «Крымец».

«А где сто миллионов туристов?» – задал вопрос один из пользователей.

Некоторые отметили, что мост на некоторое время был закрыт на профилактику.

***

22.05.2018

Неординарний священик з Тернопільщини проводить служби в «Інстаграмі»

Греко-католицький священик з Тернопільщини Василь Германюк – доволі непересічна особистість. Попри те, що він є духовним наставником Скала-Подільської громади, йдучи «в ногу з часом», отець практикує молитву в мережі «Інстаграм» (InternetUA).

Мало не щодня до поціновувачів діяльності о. Василя приєднуються все нові й нові користувачі. Вже зараз на його акаунт підписані більше 1600 людей. Що цікаво, більшість з них – молодь.

Керівництво церкви ініціативу неординарного священика підтримує. Свої прямі трансляції з ранковими та вечірніми молитвами Василь Германюк проводить о 08:30 та 21:30 год. Долучитись можуть усі бажаючі, адже після цього вони отримують благословення на день чи на ніч.

Та не лише молодь приєднується до онлайн-молитви – останнім часом серед підписників побільшало заробітчан, водіїв та, навіть, військових.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

14.05.2018

Ирина Фоменко

Facebook задумывается над созданием собственной криптовалюты

Facebook может заинтересоваться созданием собственной криптовалюты, сообщает The Fortune. Криптовалюта социальной сети упростит для пользователей покупку товаров друг у друга «без государственных валют» (InternetUA).

Непонятно, как именно Facebook будет использовать свою цифровую валюту, но монета наподобие Bitcoin облегчит людям продажу продуктов на международном уровне через маркетплейсы.

Facebook собрал новую команду, которая будет заниматься технологией blockchain, лежащей в основе популярных криптовалют, например, Bitcoin и XRP. Компания перевела лидера своей службы Messenger Дэвида Маркуса в новую команду, чью работу он будет контролировать.

В Facebook не рассказали, что компания планирует делать с blockchain, но, по словам Маркуса, социальная сеть будет начинать с нуля. Маркус когда-то был президентом PayPal, сейчас он также является членом совета директоров Coinbase.

11 мая глава отдела IBM по blockchain Бриджит ван Кралинген заявила, что технология blockchain может помочь Facebook справиться с некоторыми из недавних споров о конфиденциальности данных компании. «Она может быть полезла для конфиденциальности, связанной с людьми, которые хотят лучше понять, как их данные используются и распространяются через различные рекламные услуги», – прокомментировала Бриджит.

«Эта технология позволит решить некоторые проблемы компании, с которыми они сталкиваются. Думаю, они правы, что относятся к этому очень серьезно», – утверждает ван Кралинген.

***

15.05.2018

Skype – заложник бизнес-стратегии Microsoft?

Купив в 2011 г. лидирующий сервис интернет-телефонии за 8,5 млрд долл., чтобы уменьшить свою зависимость от персонального компьютера, Microsoft переориентировала Skype на корпоративный рынок, сделав его менее интуитивным и сложным в использовании. Это побудило многих приверженцев Skype перейти на аналогичные сервисы, предоставляемые Apple, Google, Facebook и Snap.

Докладніше

***

16.05.2018

Владимир Кондрашов

Российские соцсети и сервисы остаются в списке самых популярных сайтов среди украинцев

В списке 25 самых посещаемых украинскими пользователями сайтов продолжают оставаться российские социальные сети и сервисы, но их влияние сокращается (InternetUA).

Об этом говорят обнародованные Интернет Ассоциацией Украины данные исследований интернет-аудитории Украины за апрель, сообщает InternetUA.

Как сообщается, на заседании Комитета Интернет Ассоциации Украины по вопросам интернет-рекламы оглашены данные исследований интернет-аудитории Украины за апрель, которое выполняется по заказу ИнАУ компанией Factum Group Ukraine.

По итогам апреля 2018 г. на базе медиа-панели численностью 5 тыс. человек определен список популярных доменов, посещаемых украинскими пользователями.

В общем рейтинге, уже стабильно, первое место в предпочтениях украинской аудитории занял google, на втором месте – youtube.com, а третье занял facebook.com. «ВКонтакте» и «Яндекс» сохранили в апрельском рейтинге занимаемые ими ранее 4 и 7 места, но растеряли часть аудитории. Единственными из российских доменов, кто нарастил популярность в Украине за апрель, стали odnoklassniki (ok.ru), вернувшие себе утерянную 8 позицию в общем зачете, и mail.ru, которым совсем немного удалось обогнать rozetka (.ua/.com.ua) по отдельным показателям и оказаться на 13 строчке рейтинга.

***

22.05.2018

Лидеров мнений в Facebook скоро можно будет выбирать на специальной бирже

Крупнейшая соцсеть тестирует платформу Branded Content Matching, с помощью которой рекламодатели смогут искать инфлюенсеров для размещения в их аккаунтах спонсорского контента (Телекритика).

Биржа позволит брендам выбирать инфлюенсеров по критериям таргетинга и различной статистике об их аудитории, а затем связываться с ними для сотрудничества.

В Facebook уже подтвердили, что идет тестирование новой платформы. В соцсети отметили, что хотят помочь компаниям находить создателей контента, которые позволят им достигать целевой аудитории, а инфлюенсерам – монетизировать их публикации и базу подписчиков. Для участия в тестировании платформы лидеры мнений должны создать портфолио, в котором они покажут размер и показатели активности своей аудитории, а также продемонстрируют свой лучший брендированный контент.

В тестовом варианте биржи рекламодатели смогут искать инфлюенсеров по следующим параметрам таргетинга:

– страны, в которых популярен этот агент влияния;

– пол, возраст, интересы, образование, семейное положение подписчиков;

– параметры, связанные с проживанием пользователей.

Кроме того, рекламодателям будут доступны метрики о размере аудитории и средних просмотрах видео. А еще компании смогут выделять среди инфлюенсеров своих фаворитов.

На этапе тестирования соцсеть не будет взимать плату за пользование платформой, однако, возможно, в будущем Facebook все-таки введет комиссию.

Пока биржа будет работать только с инфлюенсерами Facebook.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

10.05.2018
Ирина Фоменко
Как социальные медиа нас «садят на крючок»

Социальные медиа-платформы используют те же методы, что и азартные игры, для создания психологической зависимости и интеграции своих продуктов в жизнь пользователей. Об этом сообщает The Guardian.

Докладніше

***

11.05.2018
Через соцмережі люди стають невпевненими в собі

Жінки, які проводять в соцмережах від години в день і більше, відчувають себе менш впевненими, застерігають британські психологи. Про результати дослідження вони розповіли на щорічній конференції Британського співтовариства психологів (Наша мама).

У дослідженні взяли участь 100 жінок. Дослідники з'ясували, скільки часу кожна з них проводить в соціальних мережах. Потім вони роздали учасницям анкети, де ті повинні були вказати, чи вважають вони стрункіх і засмаглих жінок привабливими або турбуються вони про те, наскільки добре виглядають в тому чи іншому одязі.

Виявилося, що чим більше жінки проводили в соцмережах, тим більше на них впливали стандарти краси і менш впевнено вони себе почували.

«Ідеали для жінок існували і раніше, але соцмережі зробили їх вплив набагато сильнішим. Жінки в соцмережах порівнюють себе з подругами, які покращують свою зовнішність за допомогою фільтрів», – пояснюють автори дослідження.

***

11.05.2018

Психологи рассказали, почему девушки очень зависимы от Instagram

Не секрет, что много девушек и женщин проводят в популярной социальной сети Instagram очень много времени. В данном приложении зарегистрировано больше одно миллиарда пользователей. Сейчас же психологи рассказали о причинах зависимости некоторых пользователей от Instagram. Дело в том, что проводящие много времени в соцсети девушки склонны к слишком заниженной самооценке, а публикация и просмотр фотографий придаёт им уверенность, создавая некую иллюзию (Аспекты.net).

Завотделом медицинской психологии научного центра психологического здоровья Сергей Ениколопов решил прокомментировать указанные выводы своих коллег. Он заявил, что Instagram и социальные сети можно сравнить с женскими журналами. По словам психолога, когда девушки просматривают фотографии, а затем сравнивают себя с другими девушками, это самым коренным способом влияет на их самооценку.

Сергей Ениколопов отмечает, что девушки могут начинать вести себя, как некие «злостные сплетницы», сравнивая себя с другими представительницами прекрасного пола в Instagram. Девушки под впечатлением просмотренного начинают или же менять свою одежду, или даже внешность, насмотревшись фотографий в сети. Однако такая часть женщин не обладает интеллектом. Есть и другой тип девушек, которые начинают сравнивать себя с другими. В социальных сетях этот процесс происходит куда быстрее, чем в реальном мире.

Психолог отмечает, что всё указанное происходит из-за комплексов, а нахождение в соцсетях только усугубляет их. Ениколопов добавляет, что нормальный человек в Instagram и других подобных сервисах проводить много времени не будут. А неуверенные и неудовлетворённые собой люди становятся зависимыми, тем самым подкрепляя свои комплексы.

Маніпулятивні технології

12.05.2018

Ким прикидались російські тролі в Facebook під час виборів у США

Росіяни намагались вплинути на більшу кількість американців через рекламу в Facebook протягом виборів 2016 року, аніж вважалось раніше. Комітет з розвідки Палати представників США оприлюднив тисячі рекламних сповіщень, які Росія використовувала для збільшення напруги серед американців протягом та після президентських виборів у США 2016 року.

Докладніше

***

15.05.2018

Журналисты обвиняют Facebook в разжигании ненависти и вражды

Социальные сети служат катализатором насилия и погромов в разных странах мира. И Facebook как самая популярная сеть в мире – в первую очередь. К такому выводу пришли журналисты из New York Times, проанализировав мусульманские погромы на Шри-Ланке (Телекритика).

Журналисты Аманда Тауб и Макс Фишер в своем недавнем материале на New York Times утверждают, что в погромах мусульманских магазинов и домов, устроенных радикально настроенным буддистами, ключевую роль сыграл Facebook. Ведь именно там появлялись слухи об убийствах мусульманами людей и звучали призывы к насилию.

Вина Facebook, по мнению журналистов, в том, что он «игнорирует неоднократные предупреждения о возможном насилии, не желает нанимать модераторов или создавать контактные пункты экстренной помощи». Таким образом его новостная лента становится площадкой для самых разных слухов, домыслов и пропаганды.

Проблема также и в том, что для жителей Шри-Ланки, как и для жителей многих других стран, Facebook является единственной социальной сетью. Поэтому к информации, которая появляется в нем, не привыкли относиться критично. Именно так был распущен слух, что мусульманские аптеки на Шри-Ланке забиты препаратом для стерилизации местных жителей.

Напомним, что на ежегодной конференции для разработчиков F8 Марк Цукерберг представил новый сервис для знакомств на базе Facebook.

***

16.05.2018

Facebook не справляется с модерацией постов

Согласно отчету компании, в первом квартале 2018 года вероятность появления в ленте пользователя запрещенных материалов выросла (Телекритика).

Количество изображений, содержащих сцены насилия, за этот период выросло на платформе на 183 %. Причиной тому в Facebook считают эскалацию войны в Сирии.

Кроме того, автоматические алгоритмы Facebook распознают лишь 38 % постов, разжигающих ненависть. Оставшиеся 62 % обнаруживаются благодаря жалобам пользователей. С другой стороны, компании удалось разработать алгоритмы, которые с вероятностью 99,5 % определяют пропагандистские посты ИГИЛ, Аль-Каиды и других экстремистских группировок. За три месяца из соцсети было удалено 1,9 млн сообщений такого содержания. По словам

главы отдела управления продуктами Facebook Гая Розена, методика будет совершенствоваться и в дальнейшем.

Компания также отчиталась о своих данных по фейковым аккаунтам в соцсети. Таковыми на данный момент являются порядка 3-4 % всех профилей, причем в первом квартале 2018 года были закрыты 583 млн аккаунтов-фейков.

***

17.05.2018

Facebook видалив понад 1,2 млрд фейкових акаунтів

З листопада 2017 року по травень 2018 року Facebook видалив 1,27 млрд фейкових акаунтів (Espreso.tv). Про це йдеться у офіційному блозі соцмережі.

У середньому за місяць фейкові акаунти складали 3-4 % від загальної кількості.

Facebook за допомогою автоматичної системи виявлення та звернення юзерів також заблокував 1,56 млрд дописів зі спамом, 42 млн з порно, 3 млн з пропагандою тероризму, 4,1 млн публікацій, розпалюючих ненависть та 4,6 млн зі сценами насильства.

У квітні соцмережа проінформувала про зростання прибутку та аудиторії у першому кварталі 2018 року, не зважаючи на скандал з витоком особистих даних. Щоденно Facebook відвідує близько 1,45 млрд людей.

***

15.05.2018

Монополия Facebook: спичка возле бочки с порохом

Facebook – это совершенно новый вид монополии. Все уже привыкли к компаниям, которые доминируют в нескольких юрисдикциях. Но до цифровой эры мало кто сталкивался с корпорацией, имеющей глобальную монополию.

Докладніше

***

21.05.2018

Искусственный интеллект Google удвоил усилия в освещении новостей

В своем обновленном новостном приложении Google удвоила использование искусственного интеллекта в рамках усилий по борьбе с дезинформацией и помощи пользователям в знакомстве с точками зрения за пределами их собственного «фильтрующего пузыря».

Докладніше

***

23.05.2018

Болгарские пользователи Twitter стали жертвами борьбы сервиса с троллями

Не так давно сервис микроблогов Twitter объявил об ужесточении борьбы с троллями: как уведомили в компании, теперь сервис будет чаще скрывать сообщения от вызывающих подозрения пользователей в диалогах и результатах поиска.

Докладніше

Спецслужби і технології «соціального контролю»

11.05.2018
Следить за киберпространством в Китае будет новая структура

Как сообщает Global Times, в нее вошли 277 китайских и 23 функционирующих в КНР иностранных компаний. Федерация будет сотрудничать с партийными организациями, поддерживать сетевую безопасность в стране и заниматься «очисткой киберпространства», отмечает издание (Центр информационной безопасности).

Управлять федерацией будет Администрация киберпространства КНР. Вице-президентами CFIS стали основатель Alibaba Джек Ма, председатель Tencent Ма Хуатэн и генеральный директор Baidu Робин Ли Яньхун.

Сообщается, что ряд компаний, входящих в CFIS, уже начали активную борьбу с контентом непристойного содержания, и изъяли из своих ресурсов более 1,5 млн записей, попавших в категорию "запрещенные" по законам КНР.

С начала 2018 года китайские власти проводят кампанию по ликвидации нелегальных платформ потокового вещания, онлайн-игр и различного противозаконного контента в интернете. К числу «запрещенных» относятся азартные игры, услуги гадателей и шаманов, а также информация порнографического и насильственного характера и публикации, пропагандирующие принципы и идеи ЛГБТ-движения.

В конце 2017 года стало известно, что крупнейшие технологические компании Китая, такие как Alibaba, Tencent и Baidu начали сотрудничать с китайским правительством по слежке за гражданами. ИТ-гиганты якобы беспрекословно стали передавать властям и полиции любые данные о своих клиентах.

***

15.05.2018
Конец эры свободного Интернета

Во всем мире усиливается контроль над Всемирной сетью. Исследования американской правозащитной организации Freedom House показали, что в 2017 году по меньшей мере в 32 странах снизился уровень сетевой свободы.

Докладніше

***

16.05.2018

Год без российских соцсетей: чем теперь пользуются украинцы и кто попал «под прицел» СБУ

Уже исполнился год, как в Украине под запрет попали российские соцсети «ВКонтакте», «Одноклассники», а также ряд популярных сайтов – mail.ru, yandex.ru, kinopoisk.ru и другие. Как выяснила «Сегодня», украинцы успешно «эмигрировали» из них, при этом ярым поклонникам соцсетей РФ блокировка не помешала пользоваться ими до сих пор.

Докладніше

***

17.05.2018

Ирина Фоменко

Ватикан ограничил посещение Twitter монахиням

Предполагается, что монастырские монахини в католической религии живут исключительно созерцая и служа. Но они могут отвлекаться на твиты, снапы и другие современные проявления социальных сетей, пишет The Fortune(InternetUA).

Поэтому, согласно новому своду правил Ватикана, монахини должны быть «рассудительными и благоразумными», когда позволяют себе посещать социальные медиа. В длинном документе содержатся всевозможные ограничения и нормы с небольшим новым разделом, посвященным использованию социальных сетей.

«Законодательство касательно средств социальной коммуникации, которые сегодня представлены во всем многообразии, направлено на сохранение сосредоточенности мысли и молчания», – говорится в документе Ватикана. – «Использование социальных медиа для образования или работы может быть разрешено в разумных пределах и только для общего блага».

Католической церкви может быть тысячи лет, но организация добилась успеха в принятии новых социальных медиа-сервисов, таких как Twitter. Папа Римский Фрэнсис – преуспевающий пользователь Twitter, на которого подписано почти 18 миллионов человек. По данным аналитического сервиса SocialBearing, его твиты просмотрели более 3,5 миллиардов раз за последние шесть месяцев, а репостнули почти 10 миллионов раз.

Но несколько недель назад группа монахинь в Испании привлекла всеобщее внимание из-за своей публикации на Facebook, где они выразили

протест против вердикта пятерке мужчин о невиновности в изнасиловании подростка в 2016 году.

Проблема чрезмерного посещения социальных сетей вряд ли ограничивается монастырскими монахинями. Даже Google и Apple недавно признали, что слишком частое использование приложений для смартфонов может сделать пользователя несчастным.

***

16.05.2018

Более 50 правозащитных организаций потребовали от российских властей отменить блокировку Telegram

53 международных и российских организации, занимающиеся защитой прав СМИ и интернет-свобод, осудили блокировку мессенджера Telegram и призвали Россию прекратить «атаку на свободу выражения мнения и неприкосновенность частной жизни в интернете».

Докладніше

***

21.05.2018

Роскомнадзор блокирует 80 сервисов VPN и прокси для доступа к Telegram

В Роскомнадзоре рассказали об ограничении доступа к 80 VPN- и прокси-сервисам, которые позволяли продолжать пользоваться мессенджером Telegram. Об этом пишет «Коммерсантъ» со ссылкой на пресс-службу ведомства (InternetUA).

Как отмечается, когда 10 VPN- и прокси-сервисов перестали обеспечивать доступ к мессенджеру в обход блокировки, они были разблокированы.

По данным источников издания, кампания по блокировке Telegram привела к тому, что продажи VPN-сервисов резко возросли.

***

23.05.2018

В России заговорили о блокировке еще одного крупного интернет-ресурса

Министерство культуры РФ потребовало от Федерального агентства по туризму (Ростуризм) рассмотреть предложение по запрету деятельности сервиса онлайн-бронирования жилья Booking.com на территории страны (InternetUA).

Об этом заявили в пресс-службе «Ростуризма», передает РБК.

Отмечается, что с инициативой блокировки иностранного ресурса выступил руководитель туроператора «Свой ТС» Сергей Войтович. Свое открытое письмо с таким предложением в адрес Минкультуры РФ он отправил еще в апреле.

Оценить такую инициативу в Минкульте поручили Ростуризму. В свою очередь в Ростуризме решили узнать мнение профильных профессиональных общественных объединений относительно этого предложения и направили им информационный запрос.

***

23.05.2018

В Баку задержали украинского хакера, укравшего миллионы из азербайджанских банков

В Азербайджане задержали гражданина Украины Андрея Серба и россиянина Павла Лунина по подозрению в хищении «миллионных сумм» у банков с помощью кибератак (InternetUA).

Об этом сообщает агентство «Тренд» со ссылкой на данные Службы государственной безопасности страны.

«Серб и Лунин арестованы, против них возбуждено два уголовных дела по подозрению в краже и незаконном получении компьютерной информации (ст. 177 и 272 УК Азербайджана)», – говорится в сообщении.

По информации СГБ, в мае 2018 года подозреваемые создали фиктивные компании и открыли на них счета в банках.

Подозреваемые в мошенничестве использовали POS-терминалы (устройства для приема к оплате платежных карт) азербайджанских банков для осуществления киберпреступлений, в результате чего им удалось заполучить миллионы, которые переводились в банки в СНГ. Сейчас счета Серба и Лунина заморожены.

Проблема захисту даних. DDOS та вірусні атаки

10.05.2018

Майя Яровая

У некоторых сотрудников Facebook есть полный доступ к аккаунтам пользователей. И они даже не узнают о вмешательстве

У небольшой группы сотрудников Facebook есть возможность получать доступ к аккаунтам пользователей, не уведомляя об этом последних. Вместе с тем, если один сотрудник Facebook получает доступ к аккаунту другого сотрудника, последний получит об этом уведомление на email или внутри соцсети. В компании такую «сигнализацию» называют Sauron alert (отсылка к всевидящему оку Саурона из трилогии «Властелин колец»). Об

этом сообщает The Wall Street Journal. В издании это назвали двойными стандартами Facebook в области приватности (AIN.UA).

В Facebook не пояснили, по каким причинам сотрудники могут получать доступ к чужим аккаунтам, однако заявили, что эта возможность существует много лет для контроля за опасными злоупотреблениями. Также журналистов заверили, что доступ к аккаунтам пользователей сотрудники могут получить, только если предоставят руководству компании весомые для того причины.

Тем не менее, благодаря такой возможности недобросовестные сотрудники могут использовать служебное положение, чтобы следить за пользователями. Ведь получая доступ к чужому аккаунту, они могут видеть очень чувствительную информацию, которую пользователь предпочел скрыть для всех: фото, видео или личные сообщения.

Начальник службы безопасности Facebook заявил, что сотрудники, которые злоупотребляют средствами контроля в социальной сети, будут уволены. Более того, случаи таких увольнений уже были. Недавно стало известно, что инженера по безопасности Facebook уволили за то, что тот, используя служебный доступ, следил за женщинами в соцсети.

***

10.05.2018

В Японии хакеры взломали камеры слежения Canon

Хакеры взломали десятки камер видеонаблюдения Canon по всей Японии и вставили фразу «I'm Hacked. Bye2» в видеопотоки скомпрометированных устройств. Об этом сообщило издание Sankei (InternetUA).

Согласно сообщениям в японских социальных сетях, подобные инциденты происходили в течение нескольких недель, начиная с середины апреля текущего года.

По словам чиновников из городов Ятие и Агео, злоумышленники получили доступ к устройствам, использовав пароли по умолчанию.

26 апреля, после первых сообщений о взломе, компания Canon Japan опубликовала рекомендации по безопасности, в которых посоветовала клиентам изменить пароли по умолчанию.

Японские пользователи и власти сообщили о взломе камер, расположенных в различных общественных местах, правительственных зданиях, возле путей водного сообщения, на рыбном рынке в Хиросиме, в медицинском центре для инвалидов в Кобе, а также в штаб-квартире одной из компаний в Нахе.

Только за 6 мая 2018 года было зафиксировано более 60 инцидентов. По словам экспертов, «умные» камеры и другие IoT-устройства могут использоваться в качестве точек входа в защищенные сети для их последующего взлома. Не измененные дефолтные пароли являются основной причиной взлома IoT-устройств и первым, что ищут IoT-ботнеты во время сканирования интернета на предмет уязвимых гаджетов.

***

10.05.2018

Apple удаляет приложения, ворующие GPS-данные пользователей

За последние несколько дней разработчики заметили, что цензоры AppStore удаляют приложения, которые отправляют данные о местоположении пользователей третьим лицам. После удаления Apple указывает на нарушение двух пунктов политики магазина (InternetUA).

Пункт 5.1.1 и пункт 5.1.2

Приложение передает данные о местоположении пользователя третьим лицам без явного согласия пользователя.

В качестве решения конфликта, Apple предлагает удалить любой код и фреймворки, нарушающие права пользователей. После чего возможна повторная публикация в AppStore.

Помимо того, что Apple требует от разработчиков предупреждать пользователей во время шеринга геопозиции и сборе данных о местоположении, владельцев приложений компания обязала предоставлять развернутую информацию об использовании таких данных.

Разработчики обязаны предоставить информацию о том, как и где будут использоваться получаемые данные.

Любые, собранные из приложение данные, не могут использоваться третьими лицами в целях, не связанных с улучшение пользовательского интерфейса или повышения производительности ПО.

По двум вышеуказанным пунктам Apple организовала массовую зачистку AppStore.

***

10.05.2018

Владимир Кондрашов

Украинские хакеры поздравили россиян с «днем победобесия»

Хактивисты объединения Украинский кибералъянс 10 мая взломали около двух сотен так называемых новостных ресурсов Российской Федерации и террористических организаций «ДНР» и «ЛНР».

Докладніше

***

10.05.2018

Рекомендованное Google приложение слило миллиарды личных фотографий

Приложение Drupe допустило утечку личных данных своих пользователей. Оно довольно популярное — на Android его установили

более 10 миллионов человек, и однажды оно даже попало в подборку Google Play Editor's Choice (InternetUA).

Drupe позволяет пользователям обмениваться фотографиями и аудиосообщениями. Как выяснилось, приложение использовало незащищённые сервера, с которых было украдено несколько миллиардов пользовательских файлов, в том числе фотографии крайне личного характера.

Разработчики Drupe пояснили изданию Motherboard, что утечка затронула данные не более 3 % пользователей – тех, что использовали функцию Walkie Talkie или отправляли сообщения во время звонка. Уязвимость, из-за которой возникла эта утечка, была оперативно закрыта, а приложение Drupe пропало из Google Play Маркета.

***

11.05.2018

Авторы PoS-вредоноса TreasureHunter раскрыли его исходный код

Исследователи в области кибербезопасности прогнозируют появление в ближайшие несколько месяцев значительного количества новых вредоносов для PoS-терминалов, разработанных на основе исходного кода вредоносной программы TreasureHunter, который был опубликован на одном из русскоязычных киберпреступных форумов в марте нынешнего года (Центр информационной безопасности).

Специалисты компании Flashpoint, первыми заметившими публикацию, подтвердили его действительность. По их словам, исходный код совпадает с кодами различных версий TreasureHunter, замеченных на протяжении последних нескольких лет. В настоящее время остается неясным, по каким причинам разработчики TreasureHunter решили выложить его исходный код. Не исключено, что вирусописатели работают над новой, переработанной версией вредоносной программы и старый код им больше не нужен.

Согласно исследованию компании FireEye, автором TreasureHunter является некто под псевдонимом Jolly Roger, который разработал вредонос для группировки BearsInc, занимающейся продажей данных кредитных карт на одном из киберпреступных форумов.

Само по себе вредоносное ПО не слишком сложное и работает по принципу всех PoS-вредоносов. Инфицировав систему под управлением Windows, TreasureHunter добавляет DLL-библиотеку для сохранения присутствия при загрузке, проводит сканирование на предмет процессов, связанных с платежными терминалами, извлекает данные платежных карт из памяти компьютера и загружает информацию на удаленный сервер, подконтрольный злоумышленникам.

***

11.05.2018

Набув чинності Закон «Про основні засади забезпечення кібербезпеки України»

Прес-служба Держспецзв'язку інформує, що 9 травня набув чинності Закон «Про основні засади забезпечення кібербезпекиУкраїни» (Державна служба спеціального зв'язку та захисту інформації України).

Цей Закон є ключовим у забезпеченні кібербезпеки країни, її критичної інфраструктури та інформаційних ресурсів. Він урегульовує комплекс питань з протидії сучасним кіберзагрозам, окреслює коло завдань, державних інституцій – основних суб'єктів забезпеченнякібербезпеки та визначає механізми координації в галузі кібербезпеки, взаємодії для виявлення кіберзагроз, запобігання й протидії їм.

Законом передбачено впровадження сучасних європейських практик управління інформаційною безпекою, застосування галузевих стандартизованих вимог до кіберзахисту об'єктів критичної інфраструктури, їх аудиту. Ці пріоритетні напрями, зокрема їх нормативне врегулювання, стануть основою державно-приватної взаємодії, об'єднають зусилля наукових установ та державних органів згідно з відповідними сферами компетенції.

Упровадження Закону «Про основні засади забезпечення кібербезпеки України» відкриває нову еру в забезпеченні кіберзахистукраїни, визначає якісно нові вектори розвитку сфери кібербезпеки та генерує додаткові можливості для держави та бізнесу в їх реалізації.

***

12.05.2018

Пользователям Facebook угрожает новая вредоносная кампания

Эксперты компании Radware предупредили о новой вредоносной кампании, в рамках которой злоумышленники через ссылки в социальной сети Facebook распространяют вредоносное ПО Nigelthorn, способное красть учетные данные пользователей и устанавливать майнеры криптовалюты.

Докладніше

***

13.05.2018

В США сообщили, что украинские хакеры атаковали сайт избиркома в Теннесси

В штате Теннесси сайт избиркома был выведен из строя на час в результате атаки, совершенной с с IP-адреса, зарегистрированного в Украине (InternetUA).

Об этом сообщает ТАСС со ссылкой на Associated Press.

Заместитель директора по информационным технологиям округа Нокс Дэвид Болл сообщил, что инцидент произошел во время голосования на первичных выборах 1 мая.

По его оценке, очевидно речь идет о кибератаке, последствия которой были усугублены «подозрительно большим числом иностранных пользователей», запросивших доступ на упомянутый выше сайт.

«Учитывая косвенные доказательства, особенно фактор одновременности злонамеренного внедрения с украинского IP-адреса, я считаю разумным по крайней мере предположить, что за событием стоял чей-то злой умысел», – отметил Болл.

По его словам, запросы на доступ на сайт 1 мая поступили от пользователей из около 100 стран.

Как заверил Болл, кибератака не нанесла ущерба голосованию и подведению его итогов. Сайт не функционировал в течение примерно одного часа после закрытия избирательных участков. Техникам понадобилось дополнительное время, чтобы наладить систему. Выявить источник атаки помогла специальная программа Sword & Shield.

***

14.05.2018

Сложный шифровальщик использует новую технику для обхода защиты

Аналитики «Лаборатории Касперского» обнаружили троянца-шифровальщика, который использует новую технику для обхода защитных решений и старательно избегает компьютеров с кириллической раскладкой на клавиатуре. Речь идёт о новой версии уже известного зловреда SynAck.

Докладніше

***

14.05.2018

Facebook зупинив роботу 200 додатків через скандал з Cambridge Analytica

Facebook зупинив роботу приблизно 200 додатків, які мали доступ до великого обсягу інформації користувачів (Espreso.tv).

Про це повідомляє Reuters.

Повідомляється, що зупинення роботи додатків стало результатом першого етапу розслідування, розпочатого після скандалу з консалтинговою компанією Cambridge Analytica.

За словами віце-президента компанії Айма Арчібонга, робота додатків припинена для проведення ретельної перевірки про неправомірне використання даних.

***

15.05.2018

Новая огромная утечка: в свободном доступе оказались данные миллионов пользователей Facebook

Исследователи Кембриджского университета разместили собранные через собственное приложение данные 3 миллионов пользователей крупнейшей соцсети на незащищенном сайте (Телекритика).

Как сообщает издание New Scientist – это уже вторая крупная утечка в соцсети после скандала с Cambridge Analytica.

Сотрудники университета собирали информацию через приложение myPersonality, которое позволяет пройти психологический тест и получить мгновенные результаты. Затем пользователю соцсети предлагалось делиться с авторами проекта ответами и личными данными из профиля.

Сообщается, что более шести миллионов человек прошли тесты в приложении и около половины пользователей согласились поделиться с проектом данными из своих аккаунтов в Facebook. Данные включали в себя возраст, пол, местоположение, результаты тестов и другие детали.

Затем создатели приложения собрали эти данные, сделали их анонимными и поместили на сайт, чтобы другие исследователи могли ими воспользоваться. Так была создана «одна из крупнейших баз данных исследований в области социальных наук».

***

15.05.2018

«Доктор Веб» выявил автора троянцев-шпионов

В конце марта компания «Доктор Веб» сообщила о распространении троянца, похищающего с зараженных устройств файлы и другую конфиденциальную информацию.

Докладніше

***

14.05.2018

Виталий Трулялякин

Chrome-приложения майнили почти на 100 тыс ПК

Специалисты безопасности выявили несанкционированный майнинг криптовалюты и кражу учетных данных через работу вредоносных расширений браузера Chrome без ведома пользователей. Примерно 100 000 ПК были заражены преступниками после установки расширений через официальный магазин Google (IT новости).

Хакеры украли данные учетной записи пользователей, установив майнеры криптовалют и мошеннические кликеры. Сотрудники Radware

утверждают, что с марта официально загружено семь таких дополнительных приложений. Группа безопасности Google прекратила работу пяти расширений, удалив их, а после данных от Radware еще двух. Причем одно было установлено в производственной компании, где имеется хорошо защищенная сеть. Вот семь расширений, наличие которых надо проверить у себя: Nigelify, PwnerLike, Alt-J, Fix-футляр, Divinity 2 Original Sin: Wiki Skill Popup, Keeprivate iHabno.

***

15.05.2018

В приложении Signal для Windows и Linux обнаружена критическая уязвимость

Исследователь безопасности Альфредо Ортега (Alfredo Ortega) обнаружил критическую уязвимость в популярном приложении для обмена зашифрованными сообщениями Signal для ОС Windows и Linux. Проблема позволяет удаленному злоумышленнику выполнить вредоносный код в системе получателя, просто отправив специально сформированное сообщение (InternetUA).

Как продемонстрировал исследователь в своем видео, код Javascript, отправленный через приложение Signal, может быть успешно выполнен в системе получателя, без какого-либо взаимодействия с ним.

В настоящее время технические данные об уязвимости не обнародованы, однако известно, что проблема, судя по всему, представляет собой уязвимость, дающую возможность выполнить произвольный код, или по меньшей мере осуществить XSS-атаку, потенциально позволяя злоумышленникам внедрить вредоносный код на целевых системах на базе Windows и Linux.

Как отметил исследователь, для успешной эксплуатации данной проблемы необходимо предварительно использовать ряд других уязвимостей. В настоящее время неясно, содержатся ли данные уязвимости только в исходном коде Signal, или также затрагивают популярную инфраструктуру web-приложений Electron, на которой основана данная программа. В случае если уязвимость находится в структуре Electron, она может также повлиять на другие популярные приложения, такие как Skype, Wordpress и Slack, которые также используют данную инфраструктуру.

Помимо этого, сообщество ИБ-экспертов обеспокоено потенциальной возможностью хищения секретных ключей шифрования Signal с помощью данной уязвимости.

Разработчик приложения, компания Open Whisper Systems, выпустила содержащие исправления версии Signal в течение нескольких часов после того, как исследователь уведомил ее о своей находке. Уязвимость была исправлена в версии Signal 1.10.1 и бета-версии 1.11.0-beta.3. Пользователям рекомендуется как можно скорее обновить приложение.

***

15.05.2018

В самом популярном способе шифрования писем обнаружили опасную дыру

Группа из девяти исследователей обнаружила критическую уязвимость в системах сквозного шифрования электронной почты OpenPGP и S/MIME. Об этом они рассказали в Twitter (InternetUA).

По словам экспертов, обнаруженная «дыра» под названием EFAIL позволяет хакерам расшифровать полученные и отправленные письма. При этом на данный момент нет никаких надежных способов для исправления этой уязвимости, говорит профессор Мюнстерского университета прикладных наук Себастьян Шинцель (Sebastian Schinzel).

Исследователи заявили, что опубликуют более подробную информацию 15 мая. Также они порекомендовали пользователям перестать использовать инструменты шифрования S/MIME и OpenPGP.

Эксперты связались с правозащитной организацией «Фонд электронных рубежей», представители которой опубликовали инструкции по отключению сквозного шифрования в электронной почте. Так, пользователям доступны гайды для почтовых клиентов Thunderbird, Apple Mail и Outlook.

Шифрование можно будет включить снова только после того, как «непосредственный риск эксплойта не пройдет», говорят представители фонда. Они посоветовали пользователям временно переключиться на мессенджеры, которые поддерживают сквозное шифрование.

***

15.05.2018

Нидерланды отказались от антивирусов «Касперского» из соображений безопасности

Правительство Нидерландов приняло решение, что больше не будет использовать антивирусное программное обеспечение от российской компании «Лаборатория Касперского» (InternetUA).

Министр безопасности и юстиции Нидерландов Фердинанд Грапперхаус сказал, что это является мерой предосторожности для гарантии национальной безопасности.

Компаниям, которые специализируются на вопросах защиты, также нужно завершить применение антивирусных программ «Лаборатория Касперского».

Дипломат заявил, что «Лаборатория Касперского» находится в подчинении у российского законодательства, которое обязывает компанию поддерживать российские разведывательные службы. У России имеется наступательная кибер-программа, направленная и на Нидерланды.

Он также сообщил, в Нидерландах не наблюдалось конкретных случаев злоупотребления со стороны российской компании, однако в будущем все возможно.

Мера, которую сейчас принимает правительство, относится только к антивирусу Kasperky Lab и абсолютно не касается услуг или других продуктов компании.

***

15.05.2018

Google обвинили в сборе данных за счет пользователей

Австралийская комиссия по вопросам конкуренции и защиты потребителей (ACCC) проводит расследование деятельности Google в связи с утверждениями о том, что компания собирает данные миллионов пользователей Android-смартфонов, которые невольно должны платить провайдерам телекоммуникационных услуг за гигабайты переданных данных. Об этом сообщило информагентство Reuters (InternetUA).

Как заявили представители Google в ответ на обвинения, у компании есть разрешение пользователей на сбор данных.

«Любые платежи за передачу данных по сотовому соединению, включая любые данные, связанные с местоположением, регулируются тарифным планом пользователя. Тип и количество данных, передаваемых пользовательским устройством, будут зависеть от продуктов или сервисов, которые они используют, а в некоторых случаях от настроек», – отметили представители компании.

Расследование началось после публикации компанией Oracle отчета о влиянии компаний Google, принадлежащей Alphabet Inc., и Facebook на австралийский рекламный рынок.

Как отметили специалисты по защите конфиденциальных данных, большинство потребителей вряд ли понимают, с чем именно они соглашаются при регистрации в смартфоне.

«Некоторые тарифные планы могут включать лишь несколько гигабайт данных, и сбор компанией Google большого количества информации может дорого обойтись потребителю», – добавили они.

***

16.05.2018

Новый вредонос крадет данные в браузерах Google Chrome и Firefox

Новое вредоносное программное обеспечение Vega Stealer, по мнению специалистов, может стать опасной угрозой для предпринимателей (InternetUA).

Цель нового вредоноса – похищать финансовую информацию, сохраненную в популярных браузерах Google Chrome и Firefox. Специалисты

выяснили, что Vega Stealer – продолжение вирусной программы August Stealer. С их помощью киберпреступники сливают конфиденциальные данные пользователей, в том числе данные платежных систем. Vega Stealer передает хакерам наиболее ценные данные: пароли, файлы cookie, информацию по кредитным картам и т.д. Новый вредонос немного усовершенствованный мошенниками: добавлена отдельная функция, отвечающая за кражу информации с Firefox, а также протокол, предназначенный для коммуникаций по сети.

Эксперты отмечают, что вредоносную программу используют в области маркетинга, рекламы и других сферах деятельности. Попадает вредонос на компьютер с помощью фишинговых электронных писем. К письму хакеры прикрепляют вложение «brief.doc», вирусные макросы которого отвечают за загрузку Vega Stealer. Сначала загружается обфусцированный документ JScript/PowerShell, который в свою очередь устанавливает Vega Stealer с главного сервера C&C.

***

16.05.2018

Поезда стали небезопасными: хакеры научились захватывать управление через Wi-Fi

В последнее время все больше железнодорожных компаний по всему миру настраивают в своих поездах сети Wi-Fi для пассажиров. Тем не менее, возможность пользоваться интернетом не только делает поездки гораздо комфортнее, но и развязывает руки хакерам. К такому выводу пришли исследователи безопасности на основании ряда тестов на проникновение, результаты которых опубликовал специалист компании Pen Test Partners Кен Манро (Ken Munro) (InternetUA).

В процессе тестирования исследователи обнаружили отсутствие разделения между сетями для пассажиров, сотрудников железной дороги и для управления поездом. Получив доступ к пассажирской сети, исследователям затем удалось получить доступ и к управлению поездом.

Вторая, обнаруженная исследователи проблема, заключалась в учетных данных по умолчанию. С их помощью специалисты смогли получить персональную информацию пассажиров и данные их платежных карт (в поездах некоторых компаний пассажиры второго класса должны платить за пользование Wi-Fi).

Манро не назвал компанию, в поездах которой были обнаружены описанные выше проблемы, но дал несколько рекомендаций по их исправлению. Прежде всего, отмечает исследователь, необходимо изолировать пассажирскую сеть от остальных (трафик должен проходить только между пользовательскими устройствами и интернетом). Интерфейс панели управления беспроводным маршрутизатором не должен быть доступен для пассажиров,

поэтому администраторам рекомендуется настроить список тех, кому разрешен доступ.

По словам Манро, лучший способ отделить сети друг от друга – использовать отдельное аппаратное обеспечение. Все оборудование должно находиться вне физической досягаемости злоумышленников, а ПО – регулярно обновляться. Все учетные данные администратора должны быть надежными, а спутниковые терминалы – изолированы от публичного интернета и регулярно получать обновления.

***

16.05.2018

В сети появился новый опасный вирус «Сталин»

Исследователи MalwareHunterTeam обнаружили вредоносный алгоритм, названный StalinLocker. Он блокирует все файлы, хранящиеся на компьютере, ставя на экран заглушку с портретом Иосифа Сталина. О находке специалистов сообщил портал BleepingComputer (InternetUA).

Программа-локер дает пользователю всего 10 минут на введение кода, отменяющего ее действия. Все это время на экране устройства, помимо счетчика, выводится фотография советского лидера, сопровожденная лозунгами советского времени, а на фоне играет гимн СССР. Если юзер не отгадывает шифр, то алгоритм запускает процесс удаления содержимого всех дисков.

Кодом разблокировки является разница между датой запуска файла на компьютере и числами 1922.12.30 (скорее всего, подразумевается дата утверждения договора об образовании СССР). По данным специалистов, при корректном введении шифра, локер сам отменяет автозапуск очистки компьютера. В противном случае программа переберет все имена дисков от A к Z и удалит все содержимое, к которому получит доступ.

В MalwareHunterTeam обратили внимание на то, что каждый раз при запуске программы времени на разблокировку у пользователя будет все меньше, так как в коде StalinLocker прописано деление текущего количества оставшихся секунд на три. Вредоносная программа сейчас находится в процессе разработки (пока она сбоит в самостоятельном планировании обновления драйвера на зараженном компьютере), но вскоре может стать полноценным оружием против юзеров по всему миру.

Специалисты по кибербезопасности утверждают, что локер можно «поймать» и обезвредить антивирусной программой, поэтому рекомендуют установить ее или обновить имеющуюся.

***

16.05.2018

В США нашли виновного в утечке данных ЦРУ

Власти США установили причастного к утечке информации из Центрального разведывательного управления (ЦРУ) в 2017 году, сообщает The Washington Post (InternetUA).

По данным прокуратуры, экс-сотрудник ЦРУ Джошуа Адам Шульте передавал информацию WikiLeaks.

В настоящий момент он находится в манхэттенской тюрьме по обвинениям, не связанным с утечкой данных управления.

В 2017 году ЦРУ при помощи ФБР в рамках расследования масштабной утечки информации «начало охоту» на предполагаемого информатора портала WikiLeaks в своих рядах. Отмечается, что доступ к засекреченным материалам имели сотни людей. Следствие проверило всех предполагаемых информаторов.

***

17.05.2018

За вами стежать: чим небезпечні VPN-сервіси

Інтернет-користувачі дедалі частіше намагаються захистити свої персональні дані. Одним із способів є використання VPN. Втім, цього недостатньо.

Докладніше

***

17.05.2018

Обнаружены уязвимости нулевого дня в продуктах Adobe и Microsoft

Специалисты ESET обнаружили две новые, ранее неизвестные уязвимости в Adobe Reader и Microsoft Windows. Эксплойты, использующие «двойную уязвимость», были внедрены во вредоносный PDF-файл.

Докладніше

***

17.05.2018

Ирина Фоменко

Распознавание лиц может стать угрозой в руках полиции

Сейчас распознавание лица стало реальностью. Полиция сканирует тысячи наших лиц – на протестах, футбольных матчах и музыкальных фестивалях – и сравнивает их с секретными базами данных.

Докладніше

***

17.05.2018

Меркель инициирует создание кибервойск в ответ на гибридную войну РФ

Германии следует создать кибервойска, поскольку гибридная война является частью военной доктрины России, заявила немецкий канцлер Ангела Меркель во время дебатов по оборонному бюджету в Бундестаге, передает Die Welt (InternetUA).

Она отметила, что выступает за увеличение оборонных расходов страны, подчеркнув, что такая инициатива направлена не на гонку вооружений, а на подготовку к возможной обороне.

При этом канцлер пояснила, что увеличение оборонного бюджета позволит бойцам Бундесвера достойно выполнять задачи международных миссий НАТО и национальной обороны.

«Конечно, мы должны быть готовы к обороне. Иначе у нас нет шансов», – сказала глава немецкого правительства.

Меркель подчеркнула все возрастающую важность для Германии «защиты на уровне страны и Альянса» и акцентировала внимание на патрулировании воздушного пространства стран Балтии и обязательствах Бундесвера в Румынии и Болгарии.

***

18.05.2018

SAS: только 7 % компаний готовы к новому европейскому регламенту по защите данных

Только 7 % компаний, работающих на международном рынке, полностью готовы к вступлению в силу нового регламента по защите данных General Data Protection Regulation (GDPR), сообщает SAS.

Докладніше

***

18.05.2018

Пользователям Airbnb угрожает фишинговая атака

Компания ESET предупредила о фишинговой атаке на пользователей сервиса аренды жилья в путешествиях Airbnb. Кампания нацелена на кражу банковских данных владельцев недвижимости (Компьютерное Обозрение).

Атака начинается с фишинговой рассылки. Потенциальная жертва получает письмо, в котором эксплуатируется тема вступления в силу с 25 мая 2018 года нового Общего регламента по защите данных (GDPR – General Data Protection Regulation). Регламент унифицирует правила обработки персональных данных в Евросоюзе.

В письме сообщается, что Airbnb обновляет политику конфиденциальности в связи с вступлением в силу нового GDPR. Чтобы и дальше пользоваться всеми функциями сервиса, владельцу жилья предлагается «обязательно» принять новые условия, перейдя по ссылке в письме.

Ссылка вела на фишинговую страницу с анкетой для «обновления личной информации». Помимо прочих сведений, владельцу жилья нужно было ввести данные банковской карты и аккаунта на Airbnb. Попав в распоряжение мошенников, эти данные могут использоваться для снятия средств со счета жертвы или последующей перепродажи.

В связи с вступлением в силу нового GDPR компании во всем мире адаптируют политики конфиденциальности и информируют пользователей об изменениях. По мнению специалистов ESET, этот факт будет и дальше использоваться мошенниками.

«Получив серьезное сообщение от известного человека или организации, важно сохранять бдительность и проверять адрес отправителя, – комментирует Камиль Садковский, эксперт вирусной лаборатории ESET. – В случае с Airbnb, настоящие письма рассылаются с адреса на домене @airbnb.com, а фишинговые – с домена @mail.airbnb.work».

***

20.05.2018

Хакерские атаки через Microsoft Office заметно участились

Компания «Лаборатория Касперского» представила результаты исследования, посвященного хакерским атакам при помощи уязвимостей в программном обеспечении Microsoft Office (InternetUA).

По данным аналитиков компании, в первом квартале 2018 года количество пользователей, которые пострадали от зараженных документов офисных приложений, увеличилось более чем в четыре раза по сравнению с аналогичным периодом 2017-го. Доля эксплойтов (вредоносные программы, используемые для атак через уязвимости в ПО) для Microsoft Office за год выросла почти вдвое, составив около 50 %.

В «Лаборатории Касперского» выявили в офисных приложениях столько различных уязвимостей, сколько в 2017 году находили только в Adobe Flash.

Доля Flash-эксплойтов, напротив, снижается: в первом квартале 2018 года она составила чуть менее 3 %. Этот спад объясняется результатом работы разработчиков, включая Adobe, которые прикладывают немало усилий, чтобы затруднить недобросовестное использование Flash Player, отмечают эксперты.

Хакерские атаки с применением эксплойтов считаются очень опасными, поскольку не требуют дополнительного взаимодействия с пользователями (вредоносный код внедряется незаметно). К ним часто прибегают как киберпреступники, ищущие незаконные источники прибыли, так и государственные субъекты, преследующие злонамеренные цели.

В январе-марте 2018 года было обнаружено более 1,3 млн установочных пакетов, что на 11 % меньше показателя трехмесячной давности.

***

20.05.2018

Мошеннические ICO уже принесли своим создателям свыше $1 млрд

18,6 % из общего количества стартапов, проводящих первичные предложения монет (ICO), потенциально могут оказаться скамом и уже принесли своим создателям свыше $1 млрд. Об этом говорится в исследовании Wall Street Journal, основанном на анализе 1450 ICO-кампаний (InternetUA).

В отчете говорится, что 271 проект использовал «вводящие в заблуждение или даже мошеннические тактики».

«Такие тактики заключались в сокрытии важной информации или предоставлении ложной информации о расположении организатора кампании или его финансовой деятельности, плагиате whitepaper, обещании гарантированной и необычайно высокой доходности, а также использовании мнимой связи со знаменитостями», – отмечается в исследовании.

Одним из таких мошеннических проектов оказался платежный сервис Denaro.

«В качестве фотографии “сооснователя компании Джереми Бокера” злоумышленники использовали фото польского банкира Дженишa Минари, который разместил его на своем личном сайте и никогда не слышал о Denaro. Остальных членов команды, якобы уже сумевшей привлечь $8 млн, идентифицировать вообще не удалось», – сообщили аналитики.

Отметим, что некоторые обнаруженные изданием подозрительные стартапы закрылись самостоятельно или были закрыты регуляторами, нанеся инвесторам ущерб в $273 млн.

Ранее в мае Комиссия по ценным бумагам и биржам США в образовательных целях запустила сайт для продвижения несуществующего и мошеннического ICO HoweyCoin.

***

21.05.2018
Михаил Сапитон
Google много обо мне знает. Но почему он не так страшен, как Facebook

В апреле 2018-го журналист The New York Times Брайан Чен провел над собой эксперимент. Он скачал все данные, которые о нем узнала Facebook и детально изучил их. Результаты исследования его удивили и напугали.

Докладніше

***

21.05.2018
Владимир Кондрашов
Новая угроза для украинских IT компаний

25 мая начинает действовать Общий регламент Европейского Союза по защите данных (GDPR). Этот документ приходит на замену ныне действующей Директиве ЕС и вносит существенные коррективы в европейскую политику защиты персональных данных.

Докладніше

***

21.05.2018

Новый вирус крадёт данные банковских карт

Эксперты в области безопасности компании Proofpoint сообщили о новом вирусе Vega Stealer, угрожающем пользователям Google Chrome и других популярных браузеров. С помощью вредоносного ПО злоумышленники крадут данные банковских карт и прочую важную информацию (InternetUA).

Vega Stealer является модифицированной версией обнаруженного ещё в декабре 2016 года вируса August Stealer. Он распространяется по электронной почте и передаёт злоумышленникам сохранённые пароли, документы и конфиденциальные сведения жертв из Chrome, Firefox, Skype и Opera. Зачастую вирус приходит в письме от какой-то крупной компании с вложением в виде документа «brief.doc». Последний включает вредоносные макросы, которые и запускают работу Vega Stealer. После заражения компьютера вирус проверяет рабочий стол жертвы, крадёт важные данные и отправляет их злоумышленникам на удалённые сервера.

«И хотя Vega Stealer не является самым сложным или скрытым вирусом, он демонстрирует гибкость вредоносного ПО, стремление его авторов и участников для достижения своей цели. Vega Stealer может в перспективе повлечь за собой более серьёзные последствия, если продолжит развиваться и распространяться», – отметили сотрудники Proofpoint.

Специалисты в очередной раз посоветовали пользователям быть внимательными, когда они открывают неизвестные и подозрительные письма.

***

21.05.2018

Зловред Roaming Mantis атакует пользователей через взломанные роутеры

Аналитики «Лаборатории Каперского» обнаружили зловред Roaming Mantis, который поначалу атаковал преимущественно пользователей азиатско-тихоокеанского региона, однако теперь достаточно быстро стал распространяться по миру.

Докладніше

***

21.05.2018

Десятки тысяч детей оказались в опасности из-за слежки родителей

Эксперты по безопасности обнаружили критическую уязвимость в приложении для отслеживания действий ребенка в социальных сетях и мессенджерах TeenSafe. Об этом сообщает ZDNet (InternetUA).

По словам специалистов, два сервера компании, размещенные на облачном сервисе Amazon, остались без защиты паролем. Это значит, что учетные записи тысяч родителей и их детей были практически в открытом доступе.

Исследователь Роберт Виггинс (Robert Wiggins) заявил, что на одном сервере хранилось более 10 тысяч записей в базе данных, в числе которых находились электронные письма для регистрации в системе. Там же можно было найти связанные с аккаунтом электронные адреса Apple ID.

Кроме того, записи содержали имена смартфонов, уникальные идентификаторы и незашифрованные пароли от Apple ID детей. Так как TeenSafe требует, чтобы двухфакторная аутентификация на устройствах была отключена, это позволяло хакерам без труда взломать смартфон ребенка из базы.

Разработчики компании уже закрыли доступ к одному из серверов после того, как эксперты сообщили им об опасной уязвимости.

Представители TeenSafe заявили, что начали предупреждать клиентов, чьи данные могли попасть в руки злоумышленников.

TeenSafe позволяет родителям постоянно следить за тем, что их ребенок делает на смартфоне. Приложение выдает родственникам всю историю поисковых запросов в браузере, историю звонков, переписку в сторонних соцсетях и мессенджерах, а также историю активности в дейтинг-сервисах. Программа работает на смартфонах под управлением Android и iOS. Только в США ее используют более миллиона человек.

***

21.05.2018

Мобильное приложение Facebook затребовало полный доступ к устройствам

В конце прошлой недели приложение Facebook для Android-устройств неожиданно стало запрашивать права суперпользователя, чем вызывало весьма неоднозначную реакцию у пользователей. Оно и немудрено, ведь, учитывая недавний скандал с аналитической компанией Cambridge Analytica, далеко не каждый согласится предоставить приложению полный доступ к своим данным (InternetUA).

Как сообщают столкнувшиеся с проблемой пользователи, на экране стало появляться вплывающее уведомление, прямым текстом запрашивающее «предоставление полного доступа к устройству». Источником уведомления является оригинальное приложение Facebook для Android-устройств.

Некоторые пользователи уже сталкивались с подобной проблемой 8 мая текущего года, но тогда она была менее распространенной. Изначально права суперпользователя требовала версия приложений 172.0.0.12.93, тогда как теперь речь идет о версии 172.0.0.66.93.

По мнению ряда исследователей, отображение запросов на получение прав суперпользователя было вызвано программной ошибкой. Эксперт компании Avast Николаос Крисаидос (Nikolaos Chrysaidos) изучил исходный код приложения и предположил, что проблема связана с встроенным в него SDK. В частности, за появление запроса на получение полного доступа ответственен пакет WhiteOps SDK – инструмент для обнаружения мошеннической рекламы и внесение доменов в черные и белые списки.

Как сообщает Bleeping Computer, пресс-служба Facebook подтвердила связь проблемы с программной ошибкой. «Нам не нужно подобное разрешение (на полный доступ к устройствам –ред.), и мы уже исправили ошибку. Приносим свои извинения за причиненные неудобства», – сообщили представители компании.

***

22.05.2018

За киберпреступления в Украине хотят наказывать более строго

Глава Департамента киберполиции Нацполиции Украины Сергей Демедюк предложили усилить ответственность за совершение незаконных действий в сети Интернет. Об этом сообщает пресс-служба Министерства внутренних дел (МВД) (IGate).

По словам Демедюка, киберпреступники наносят очень большой ущерб стране. Поэтому надо увеличить меру наказания за незаконные действия в сети.

«Речь идет о миллиардных убытках. Поэтому условный срок до пяти лет и штраф за такие действия - абсолютно несправедливое наказание», – заявил Демедюк.

Как утверждает главный киберполицейский, его департамент предложит внести изменения в законодательство с целью обеспечения безопасности в киберпространстве. Сообщается, что на поставщиков контента, в частности провайдеров интернет-связи, будут возлагаться обязанности по хранению незаконной информации и операций в сети. Эти данные должны храниться на протяжении 90 суток по запросу правоохранительных органов.

Глава киберполиции подчеркнул, что подобная система существует в США и многих странах Европы, среди которых Германия, Великобритания, Италия, Швейцария.

«Сама процедура блокировки – как временная или частичная, так и постоянная – должна существовать. Я не думаю, что кто-то будет против запрета на распространение детской порнографии, призывов к войне, терроризма, экстремизма и других подобных вещей. Это будет вполне

конкретный список преступлений, предусмотренных в Европейской конвенции», – добавил Сергей Демедюк.

Ранее в Верховной Раде был зарегистрирован законопроект №8304, который должен усилить наказание за киберпреступления. Согласно проекту закона, за нелегальную деятельность в сети виновный должен отсидеть за решеткой 8 лет. Также запланировано увеличить размер штрафа за создание и распространение вредоносного ПО.

***

22.05.2018

Сетевое оборудование компании DrayTek находится под атакой

Тайваньский производитель сетевого оборудования DrayTek предупредил о том, что злоумышленники эксплуатируют уязвимость нулевого дня в роутерах компании и подменяют настройки DNS (InternetUA).

Компания признала проблему после того, как пользователи Twitter стали массово жаловаться на изменение настроек DNS на своих устройствах, которые после атак начинали указывать на неизвестный сервер, расположенный по адресу 38.134.121.95. Вероятнее всего, таким образом атакующие пытались осуществить атаку man-in-the-middle, к примеру, для перенаправления пострадавших на фальшивые версии легитимных сайтов.

Представители DrayTek опубликовали сразу два бюллетеня безопасности, немного отличающихся друг от друга. Первым стал бюллетень, размещенный на британском сайте компании. Он подробно рассказывает, как изменить настройки DNS на правильные, а также гласит, что разработчики уже готовят новую прошивку, защищающую от атак. Вторым стал более детальный бюллетень, размещенный на международной версии сайта.

Изначально ИБ-эксперты предполагали, что злоумышленники попросту брутфорсят роутеры DrayTek или используют учетные данные по умолчанию, которые пользователи могли не поменять. Эти теория оказалась неверной, так как многие владельцы пострадавших девайсов сообщили, что меняли логины и пароли от своих устройств. К тому же на Reddit пострадавшие пользователи рассказывали о том, что в логах вообще нет данных о каких-либо входах в систему, то есть эксплоит атакующих не требует даже этого.

Издание Bleeping Computer отмечает, что, согласно информации с форума Sky Community, атаки на роутеры DrayTek длятся уже около двух недель. По данным Shodan, в интернете можно обнаружить порядка 800 000 устройств DrayTek, однако неизвестно, какой процент от этого количества уязвим перед эксплоитом атакующих

***

22.05.2018

Владимир Кондрашов

Ровенские полицейские майнили криптовалюту прямо в помещении областного ГУНП

Должностные лица отдела связи и коммуникации ГУ Нацполиции в Ровенской области около четырех месяцев занимались майнингом криптовалют непосредственно на рабочем месте (InternetUA).

Информация об этом содержится в постановлении судьи Ровенского городского суда, сообщает InternetUA.

Как стало известно, следственным отделом Ровенского ОП ГУНП в Ровенской области осуществляется досудебное расследование в уголовном производстве по ч.1 ст.185 УК Украины по факту кражи электроэнергии.

– Досудебным расследованием установлено, что с начала 2018 года должностные лица отдела связи и коммуникации ГУНП в Ровенской области, злоупотребляя своим служебным положением, действуя вопреки интересам службы, самовольно использовали электрическую энергию ГУНП в Ровенской области в собственных целях, для надлежащего функционирования оборудования для добычи криптовалют, чем нанесли существенный вред интересам ГУНП в Ровенской области, – говорится в постановлении.

***

22.05.2018

Владимир Кондрашов

За утечкой данных Запорожской АЭС стоят сотрудники отдела ядерной безопасности

Полиция открыла уголовное дело по факту несанкционированного вмешательства в работу компьютерных сетей ОП «Запорожская АЭС» ГП НАЭК «Энергоатом». Вмешательство повлекло утечку информации с ограниченным доступом ЗАЭС.

Докладніше

***

23.05.2018

Опасный вирус стремительно захватил сотни тысяч устройств по всему миру

Американская телекоммуникационная компания Cisco Systems предупредила пользователей об активном распространении вредоносного программного обеспечения VPNFilter. Подразделение кибербезопасности компании Talos решило опубликовать незавершенное исследование компании из-за слишком стремительного распространения по всему миру (InternetUA).

VPNFilter заразил уже 500 тысяч компьютеров как минимум в 54 странах.

Вирус поражает сетевую аппаратуру, в частности роутеры (такие как Netgear и TP-Link) и сетевые накопители производства Qnap. В докладе

говорится, что программа способна перехватывать трафик, управлять устройством и вывести устройства из строя, поодиночке или группами, «потенциально отрезая от интернета сотни тысяч жертв по всему миру».

***

23.05.2018
Почему не стоит подключаться к незнакомым сетям Wi-Fi

Миллионам пользователей Android угрожает зловред под названием Roaming Mantis, распространяемый посредством скомпрометированных Wi-Fi-маршрутизаторов, сообщает «Лаборатория Касперского». Когда устройство подключается к сети, транслируемой инфицированным роутером, инициируется загрузка вредоносного файла, способного взламывать учетные записи Google (InternetUA).

Загрузка вредоносного компонента осуществляется под видом обновления для веб-браузера или клиента социальной сети Facebook. Попав на устройство, вредонос направляет пользователю запрос на получение нескольких разрешений, которые впоследствии используются им для взлома двухфакторной аутентификации и захвата контроля над учетными записями Google.

Изначально опасность заражения Roaming Mantis угрожала пользователям из Японии, Южной Кореи, Китая, Индии и Бангладеша, однако на данный момент к числу потенциальных жертв относят жителей большинства европейских стран. Кроме того, теперь вредонос научился атаковать пользователей iOS, перенаправляя их на поддельный веб-ресурс, имитирующий официальный сайт Apple, – якобы для уточнения платежных данных.

ДОДАТКИ

Додаток 1

15.05.2018
Skype – заложник бизнес-стратегии Microsoft?

Купив в 2011 г. лидирующий сервис интернет-телефонии за 8,5 млрд долл., чтобы уменьшить свою зависимость от персонального компьютера, Microsoft переориентировала Skype на корпоративный рынок, сделав его менее интуитивным и сложным в использовании. Это побудило многих приверженцев Skype перейти на аналогичные сервисы, предоставляемые Apple, Google, Facebook и Snap (Компьютерное Обозрение).

Microsoft заявляет, что проблема преувеличена, однако компания не публикует общее количество пользователей Skype с 2016 г., тогда их было 300 миллионов. Некоторые аналитики подозревают, что цифры в лучшем случае остались те же, а два бывших сотрудника утверждают, что они падают.

Сегодня Microsoft использует Skype for Business, чтобы лучше продавать подписки на облачный Office 365 и переманивать клиентов от Cisco. Как доказательство того, что эта стратегия работает, Microsoft указывает на клиентов, среди которых Accenture и ряд крупнейших банков. General Electric в конце 2017 г. установила Skype for Business у 220 000 своих сотрудников и каждый день регистрирует 5,5 млн минут переговоров. Согласно опросу Forrester 6 259 работников сферы IT, 28 % используют для конференций Skype for Business, по сравнению с 21 % для продуктов Cisco.

Тем не менее, корпоративные особенности ПО, вступают в противоречие с потребителями, заинтересованными в простоте и интуитивности. Наличие двух разных приложений не решает проблему, так как основаны они на одной и той же технологии, разработанной с прицелом на офисных служащих.

Те, кто сохраняет лояльность Skype, часто жалуются и на качество сервиса – проблемы с дозвоном, обрывы соединений, исчезновение контактов после обновления ПО. По словам Ника Барбера (Nick Barber) из Forrester, у бизнес-клиентов – аналогичные проблемы.

Microsoft утверждает, что в прерывании звонка по большей части виновата сеть пользователя, а не Skype. Люди разочаровываются и переходят к другому приложению или сервису, только чтобы столкнуться с той же проблемой.

Генеральный менеджер Skype, Лори Райт (Lori Wright) считает, что ситуация стремительно улучшается. В октябре количество загрузок Skype для Android достигло миллиарда. Рейтинги тоже начинают восстанавливаться по мере того, как люди привыкают к изменениям. «Это был действительно радикальный редизайн, и мы ждали, то его встретят в штыки, – пишет она. – В действительности же мы увидели, что антагонизма больше не существует».

(вгору)

Додаток 2

10.05.2018
Ирина Фоменко
Как социальные медиа нас «садят на крючок»

Социальные медиа-платформы используют те же методы, что и азартные игры, для создания психологической зависимости и интеграции своих продуктов в жизнь пользователей. Об этом сообщает The Guardian (InternetUA).

Эти методы настолько эффективны, что они могут активировать мозговые механизмы, как кокаин, формируя психологическую зависимость и даже вызывая «фантомные звонки и уведомления» (когда пользователи ощущают жужжание смартфона, даже если сообщений нет).

«Facebook, Twitter и другие компании используют те же методы, что и игровая индустрия, чтобы удерживать пользователей на своих сайтах. В онлайн-экономике доход – это постоянное внимание потребителей, измеряемое кликами и затрачиваемым временем», – заявила автор «Addiction by Design»

Наташа Шюлл. – «Неважно, Snapchat ли это, лента новостей Facebook или CandyCrush – вы втягиваетесь в «игровую петлю» или повторяющиеся циклы неопределенности, ожидания и обратной связи – а вознаграждение заставляет вас продолжать».

«Если вы отключитесь, то получите небольшие бонусные предложения – так привлекают ваше внимание. Мы должны осознавать, сколько тратим времени на социальные сети. Это не просто игра – такие медиа-платформы влияют на нас финансово, физически и эмоционально», – утверждает Шюлл.

Как игровой автомат

«Механизмы «потяните вниз для обновления» и бесконечной прокрутки новостной ленты выглядит крайне похожими на технологию игрового автомата. Тяните рычаг и сразу получаете либо заманчивую награду, либо ничего», – уверен бывший сотрудник Google Тристан Харрис.

«Вознаграждение – это то, что психологи называют переменным графиком подкрепления, ключ к тому, что пользователи социальных сетей неоднократно проверяют свои телефоны», – заявил профессор и директор подразделения «Международные игровые исследования» Ноттингемского университета Марк Гриффитс. – «Социальные сети пытаются привлечь внимание пользователей, чтобы проверка медиа стала рутиной».

Подобно азартным играм, которые физически изменяют структуру мозга, использование социальных сетей непосредственно связано с депрессией. А негативное психологическое воздействие на пользователей нельзя игнорировать или недооценивать. Например, из-за зависимости от телефона нам иногда кажется, что телефон вибрирует, хотя на самом деле это не так.

«Фантомные звонки и уведомления связаны с нашей психологической зависимостью. Сообщения в социальных сетях могут активировать те же мозговые механизмы, что и кокаин, и это всего лишь один из способов их идентификации», – прокомментировал профессор Мичиганского университета Дэниел Крюгер. – «Существуют целые подразделения, пытающиеся сконструировать свои системы настолько эффективными, насколько это возможно. Они хотят, чтобы вы были постоянно в сети и сделают все возможное, чтобы вы снова обратили внимание на приложение или веб-страницу».

Число активных пользователей Facebook в прошлом году достигло 2,13 млрд человек, что на 14 % больше, чем в 2016. Несмотря на скандалы с конфиденциальностью данных, в первом квартале 2018 года доход компании составил 11,97 млрд долларов, что на 49 % больше, чем годом ранее.

Ключевая причина такой статистики – Facebook настолько вошел в нашу жизнь, что мы не можем от него отказаться. Поведенческий психолог Нир Эял концептуализировал, как люди привязаны к социальным медиа.

«Все начинается с триггера, действия, вознаграждения, а затем инвестиций и последовательных циклов. Это присутствует в большинстве продуктов: безусловно, в социальных сетях и азартных играх», – считает Эял.

По словам Нира, при появлении привычки триггеры уже не нужны – они заменяются или дополняются внутренним триггером, означающим, что мы формируем связь между желанием использовать этот продукт и стремлением удовлетворить эмоциональную потребность.

(вгору)

Додаток 3

12.05.2018

Ким прикидались російські тролі в Facebook під час виборів у США

Росіяни намагались вплинути на більшу кількість американців через рекламу в Facebook протягом виборів 2016 року, аніж вважалось раніше (InternetUA).

Комітет з розвідки Палати представників США оприлюднив тисячі рекламних сповіщень, які Росія використовувала для збільшення напруги серед американців протягом та після президентських виборів у США 2016 року.

Facebook заявляє, що ці рекламні сповіщення купувало пов'язане з Кремлем Агентство Інтернет-досліджень.

Нам вже відомо, що реклама просувала несправжні групи в соціальних мережах, які імітували ініціативу з боротьби за права афро-американців Black Lives Matter, вдавали себе за мусульман, або американців, які підтримують Дональда Трампа.

Однак, нові документи, розголошені Комітетом Палати представників США показують, що росіяни також намагались вплинути на американців мексиканського походження, повідомляє CNN.

Невідомо, коли точно було створено російську сторінку призначену для американців мексиканського походження, однак, в 2017 році вона нараховувала більш ніж 200 000 послідовників і багато записів мають тисячі поширень, вказують оприлюднені документи.

Сторінка називалась «Коричнева сила» і мала зображення стиснутого кулака на фоні прапора Мексики.

Одне з рекламних повідомлень сторінки твердило: «коричнева сила є платформа, створена, щоб освічувати, розважати та об'єднувати "чиканос" в США».

Багато російських тролів, які видавали себе за американців, не виступали на підтримку конкретного кандидата, але поширювали послання, що збурювали конфлікти з чутливих питань, таких як імміграція, чи расизм, особливо в тих штатах, де виборчі перегони були дуже конкурентними, такими як Пенсильванія, Вісконсин та Вірджинія.

Оприлюднені документи містять більше 3000 рекламних повідомлень в Facebook та Instagram.

Тиск на Facebook з підвищення стандартів прозорості посилився після того, як в лютому міністерство юстиції США висунуло звинувачення проти 13

росіян і трьох компаній, і висвітлило масштабні зусилля росіян зі спотворення виборів і підтримки кампанії Трампа.

(вгору)

Додаток 4

15.05.2018

Монополия Facebook: спичка возле бочки с порохом

Один из самых интересных моментов из недавнего пятичасового допроса Марка Цукерберга сенатской комиссией наступил тогда, когда сенатор Линдси Грэхэм спросил босса Facebook: «Кто ваш самый большой конкурент?» (InternetUA).

На видео видно, что Цукерберг сначала криво улыбается. Затем вяло пытается что-то рассказать о Google, Apple, Amazon и Microsoft, которые по-разному «пересекаются» с Facebook.

В конце концов, сенатор Грэхем прерывает мучения миллиардера и спрашивает Цукерберга напрямую, считает ли тот, что Facebook является монополией. «Мне это так определенно не кажется», – отвечает владелец соцсети.

По комнате разносится волна смеха. Наступает момент, понятный даже сенаторам. Менее понятно пока другое, – понимают ли в США и других странах масштаб проблемы?

Facebook – это совершенно новый вид монополии. Все уже привыкли к компаниям, которые доминируют в нескольких юрисдикциях. Но до цифровой эры мало кто сталкивался с корпорацией, имеющей глобальную монополию. Куда бы вы ни отправились в наши дни, Facebook часто будет самой влиятельной социальная сеть в стране. У нее вообще мало где в мире есть серьезные конкуренты.

Последствия подобного только сейчас начинают осознавать. В течение последних двух лет много говорится о пагубном влиянии Facebook на демократическую политическую систему и о необходимости как-то эту проблему решить. Впрочем, какой-то эффективной системы регулирования никто так и не предложил, и, поэтому, по большому счету, ничего не меняется. Но, по крайней мере, западные демократии с развитой системой СМИ и эффективной государственными институциями обладают определенной степенью иммунитета к дезинформации, распространяемой через Facebook. В других странах, особенно в развивающихся, нет сил, способных обуздать Facebook и там социальная сеть может причинить действительно серьезный ущерб.

Так, в последнее время появляется все больше информации о том, что именно Facebook был средой для разжигания антимусульманской истерии в Мьянме. Там, напомним, она переросла в полномасштабную этническую чистку. Одной из ключевых фигур тех событий был ультранационалист и по совместительству буддийский монах Ашин Вирату. Он использовал Facebook

для трансляции своих взглядов по поводу этнического меньшинства рохинджа уже после того, как правительство запретило ему проповедовать.

Вирату сравнивал мусульман рохинджа с бешеными собаками и размещал фотографии тел людей, которые, по его словам, были убиты мусульманами, – с предсказуемыми последствиями.

Должностные лица Организации Объединенных Наций открыто признают, что социальные медиа играют «определяющую роль» в борьбе с насилием против рохинджа в Мьянме. Но, на самом деле, под стыдливым названием «социальные сети» здесь можно прямо читать Facebook, потому что в Мьянме ему нет конкуренции.

Мьянма не единственный пример. Соцсеть играет аналогичную роль и в других развивающихся странах. Об этом не так давно вышла большая статья в New York Times. О чем там идет речь, понятно прямо из заголовка, – там государства сравнивают с пороховой бочкой, а Facebook – со спичками. Иллюстрацией к онлайн-изданию стало видео буддийской толпы, которая поджигает мусульманские магазины и дома на Шри-Ланке.

Текст New York Times основан на интервью с официальными лицами Шри-Ланки, жертвами и простыми пользователями соцсети. В статье говорится о том, что «новостная лента Facebook играет центральную роль почти на каждом этапе – от появления слухов до убийств». Журналисты винят Facebook в том, что он «игнорирует неоднократные предупреждения о возможном насилии, не желает нанимать модераторов или создавать контактные пункты экстренной помощи». Сам Facebook парирует в ответ, что он пытается удалять взрывоопасный контент.

Это возвращает нас к тому, с чего мы начинали – с констатации факта, что Facebook является глобальной монополией. Уже сейчас рынок компании на Западе достиг насыщения, и поэтому большая часть его будущего роста должна быть связана с увеличением проникновения в менее развитые регионы мира. Именно там он сейчас активно продвигает свои услуги, в том числе в виде «бесплатного» доступа для владельцев дешевых смартфонов.

В результате во многих странах третьего мира жители практически не отличают Facebook от Интернет. Соцсеть часто является их единственным источником онлайн-информации. И это делает людей уникально уязвимыми для вбросов. Таких, как слух о том, что мусульманские аптеки в Шри-Ланке забиты таблетками для стерилизации членов сингальской общины.

На Западе фейковые новости влияют на выборы. Это, конечно, большая проблема и там с этим вроде как собираются бороться. Но в остальном мире фейковые новости забирают жизни. И именно Facebook часто является главным распространителем таких новостей.

(вгору)

Додаток 5

21.05.2018

Искусственный интеллект Google удвоил усилия в освещении новостей

В своем обновленном новостном приложении Google удвоила использование искусственного интеллекта в рамках усилий по борьбе с дезинформацией и помощи пользователям в знакомстве с точками зрения за пределами их собственного «фильтрующего пузыря». Глава Google Сундар Пичаи, который представил обновленные Google News в начале этого месяца, рассказал, что «теперь приложение представляет интересующие вас новости из доверенных источников, при этом предоставляя полный спектр точек зрения на события» (InternetUA).

Google серьезно планирует оказаться в центре онлайн-новостей и попытается помочь издателям получить платных подписчиков через платформу техногиганта. По словам главного разработчика продукта Тристана Апстилла, новостное приложение «использует лучшее от искусственного интеллекта для поиска лучшего от человеческого интеллекта – отличных репортажей, которые поступают от журналистов со всего мира».

В то время как приложение позволит пользователям получать «персонализированные» новости, оно также будет включать в себя самые популярные истории для всех читателей, пытаясь сломить так называемый фильтрующий пузырь информации, который укрепляет у людей предубеждения и предрассудки.

«Чтобы беседа или спор были продуктивными, каждый должен иметь доступ к одной и той же информации», говорит Апстилл.

Он говорит, что «полное освещение» будет одинаковым для всех – «неперсонализированное представление о событиях из целого ряда надежных источников новостей».

Впрочем, некоторые ветераны индустрии журналистики скептически отнеслись к усилиям по замене редакторов-людей кураторами-машинами.

«Фантазии об алгоритмически персонализированных новостях существуют уже давно», говорит профессор журналистики Нью-Йоркского университета Мередит Бруссард. «Никто так и не сделал это правильно. Думаю, дизайнеры новостей и редакторы домашних страниц уже неплохо справляются с курированием».

Не стоит забывать также, что Google и Facebook критиковали за то, что компании забирали большую часть прибыли от онлайн-рекламы, и за распространение ложной информации. Посмотрим, что изменится в этот раз.

(вгору)

Додаток 6

23.05.2018

Болгарские пользователи Twitter стали жертвами борьбы сервиса с троллями

Не так давно сервис микроблогов Twitter объявил об ужесточении борьбы с троллями: как уведомили в компании, теперь сервис будет чаще скрывать сообщения от вызывающих подозрения пользователей в диалогах и результатах поиска (InternetUA).

Как пишет The Verge, новая политика Twitter привела к неожиданным последствиям: практически сразу же жертвами нововведений стали многие пользователи из Болгарии, учетные записи которых были заблокированы, а их сообщения в диалогах были скрыты. По всей видимости, причиной этого стал тот факт, что пострадавшие пользователи писали сообщения на кириллице. Вероятность попасть под блокировку увеличивалась, если пользователь упоминал в твите популярный аккаунт или отвечал на такую запись.

Наиболее вероятное объяснение этой ситуации заключается в том, что алгоритмы сервиса были настроены на борьбу с так называемыми кремлевскими ботами и троллями. Поскольку такие аккаунты зачастую публикуют сообщения на русском языке, то использование кириллицы является своего рода «черной меткой» для системы, создатели которой не учли, что кириллица используется не только в России, а также тот факт, что далеко не каждый пользователь, пишущий на кириллице, является троллем.

Пользователи, аккаунты которых были заморожены, могут довольно быстро восстановить их, однако после этого сервис воспринимает их как «цифровых изгоев», скрывая их ответы на записи других пользователей и скрывая от их подписчиков уведомления о новых публикациях. При этом в случае обращения в техподдержку пользователю сообщают, что его аккаунт не был забанен и все работает корректно.

Журналисты The Verge обратились в Twitter за комментарием и получили ответ только через два дня. В компании заявили, что разбираются с проблемой блокировки законопослушных пользователей и предпримут шаги для ее решения, но сервис продолжит борьбу со спамом и ботами.

(вгору)

Додаток 7

15.05.2018
Конец эры свободного Интернета

Во всем мире усиливается контроль над Всемирной сетью. Исследования американской правозащитной организации Freedom House показали, что в 2017 году по меньшей мере в 32 странах снизился уровень сетевой свободы. Вводятся ограничения на использование различных служб; власти осуществляют информационные манипуляции и распространяют фальшивые новости. Если свободной циркуляции информации будет нанесен чрезмерный ущерб, то это ограничит выбор пользователей и негативно скажется на экономической деятельности (InternetUA).

В начале апреля неожиданно навсегда было заблокировано китайское приложение для размещения видео Neihanshequ, которым пользовались около

200 миллионов человек. Поскольку власти выразили недовольство содержанием размещаемой информации, некоторое время невозможно было загрузить и другие многочисленные новостные приложения. С одной стороны, власти утверждают, что пользователи загружали порно и другие неподобающие материалы, а с другой, эксперты полагают, что цель была в том, чтобы усилить контроль.

В июне 2017 года в Китае вступил в силу закон о безопасности в Интернете, в результате чего выросло количество дел о незаконной информации. Были введены ограничения в отношении американской поисковой системы Google и других сервисов; также усиливается контроль над виртуальными частными сетями (VPN), которые используются для обхода ограничений. Freedom House отмечает, что в 2017 году интернет-свобода в стране находилась на самом низком уровне в мире, это фиксировалось три года подряд.

Это касается не только Китая. Freedom House ежегодно анализирует мировую ситуацию с трех сторон: препятствование подключению к Интернету, ограничение контента, нарушение прав сетевых пользователей. К несвободным были отнесены Китай, Россия и еще 19 стран. Количество несвободных стран продолжает расти, хотя в 2014 году их было всего пятнадцать.

Типичные меры, снижающие уровень свободы, – контроль подключения к Сети и ограничения использования различных сервисов. В Египте в 2017 году было заблокировано более 400 новостных сайтов и страничек правозащитных организаций. В России в середине апреля власти запретили мессенджер Telegram, которым пользуются примерно 15 миллионов человек. Это привело к крупномасштабным протестным акциям.

Также поражают информационные манипуляции. В 2017 году в 30 странах были зафиксированы случаи, когда власть или правящая партия нанимали людей, а также прибегали к другим мерам, косвенным образом распространяя благоприятную для себя информацию. По сравнению с 2016 годом к этому списку добавились семь стран. Активно используется программное обеспечение, которое автоматически распространяет большое количество информации и удаляет ненужную.

Для того чтобы предотвратить распространение фальшивых новостей, страны ЕС начали обращаться к крупным информационным компаниям.

«Фальшивые новости и искаженная информация, распространяемые в Сети, представляют серьезную угрозу безопасности общества», – подчеркнула Европейская комиссия, потребовав не позднее июля представить свод правил.

Тем не менее непросто разработать нормы определения фальшивых новостей и искаженной информации. 11 апреля в Малайзии вступил в силу закон о новостях. По информации местных СМИ, 30 апреля был признан виновным турист из Дании, сообщивший, что полиция медленно отреагировала на происшествие со стрельбой. Малайзийские правозащитные организации обеспокоены дальнейшим ограничением свободы слова; по их мнению, существует опасность судебного активизма.

Интернет, разработанный в военных и научных целях, начал распространяться в 1990-е годы. В настоящее время им пользуются около четырех миллиардов человек по всему миру.

«Сегодня Интернет необходим как воздух. Он является основой различной деятельности: экономики, медицины, образования и так далее», – отмечает профессор Университета Кэйо Дзюн Мураи.

Сейчас проблема заключается в том, как обеспечить свободу на фоне распространения по всему миру сетевых ограничений.

(вгору)

Додаток 8

16.05.2018

Год без российских соцсетей: чем теперь пользуются украинцы и кто попал «под прицел» СБУ

Уже исполнился год, как в Украине под запрет попали российские соцсети «ВКонтакте», «Одноклассники», а также ряд популярных сайтов – mail.ru, yandex.ru, kinopoisk.ru и другие. Как выяснила «Сегодня», украинцы успешно «эмигрировали» из них, при этом ярым поклонникам соцсетей РФ блокировка не помешала пользоваться ими до сих пор (InternetUA).

Решение СНБО, блокирующее доступ к соцсетям, было принято 15 мая 2017 года в рамках введения очередных санкций против России и с целью усиления информационной безопасности Украины. Несмотря на запрет, многие украинцы продолжают ими пользоваться в обход блокировки. Например, вчера днем запрещенной соцсетью «ВКонтакте» одновременно пользовались чуть более 375 тысяч украинцев – это почти 1 % всего населения страны! Ранее же, до введения запрета, ВК была в Украине самой популярной соцсетью, в ней было зарегистрировано более 27 млн страниц из Украины, а каждый день в соцсеть заходили 10 млн человек.

Сразу после введения запрета силовики призвали интернет-провайдеров, не дожидаясь спецпроверок, заблокировать доступ. В большинстве случаев они выполнили это требование. Как рассказал «Сегодня» глава Интернет Ассоциации Украины Александр Федиенко, по его информации, не было ни одного интернет-провайдера, который был бы наказан за неисполнение норм по блокировке сайтов. При этом Федиенко уточнил:

«Сейчас информпространство страны можно отнести к понятию критической инфраструктуры. Изменилось ли что-то в нем или нет за это время – это должны изучать незаангажированные госструктуры, которые бы мониторили уровень влияния информации на социум. Но сейчас такой структуры у нас нет».

Также он признался, что на днях провел небольшое расследование.

«Некоторые из моих знакомых госслужащих “живут” в ВК. Я увидел, что человек, который говорит, что он рьяный противник ВК, был там вчера либо позавчера, либо 13 минут назад. Это говорит о том, что люди все равно туда

заходят. Возможно, они заходят туда изучать аудиторию, может быть, считают, что врага нужно знать в лицо», – рассуждает Александр Федиенко.

В спецслужбах нам ответили, что практически все интернет-провайдеры оперативно выполнили требования. Но даже единицы компаний-нарушителей, которых поймали на ретрансляции запрещенных российских каналов (а не в открытом доступе к соцсетям), наказали предупреждением.

В то же время «под прицел» силовиков попали сотни украинцев, которые использовали запрещенные соцсети для пропаганды идей «ДНР» и «ЛНР», а также которые публично давали инструкции по обходу блокировки соцсетей и установке VPN-сервисов. Как рассказали «Сегодня» в СБУ, «трудовая» биография у таких граждан практически одинаковая: они были завербованы спецслужбами России, после чего стали администраторами сообществ в запрещенных соцсетях, а некоторые из них публично призывали обходить блокировку и давали подробные инструкции, как это сделать. Согласно госсреестру судебных решений, такие нарушители закона отделывались условными тюремными сроками.

Спустя год борьба за чистоту информпространства продолжается. В Мининформполитики «Сегодня» сообщили, что недавно по запросу журналистов обнародовали новый список из 21 интернет-ресурса, рекомендованного для запрета в Украине. В этот раз речь идет не о соцсетях, а об информационных «рупорах» самопровозглашенных республик и аннексированного Крыма. Как пояснили нам в министерстве, список названий пропагандистских сайтов уже передан в спецслужбы, и теперь дело за ними. Но, как убедилась «Сегодня», по состоянию на 10 мая все эти сайты-пропагандисты работали, рассказывая о «достижениях» псевдореспублик.

«Переселение» народа

Тысячи украинцев, в том числе и те, чей бизнес продвигался с помощью соцсетей, в первые дни запрета запаниковали, что, мол, теперь понесут убытки. Но эти прогнозы не оправдались – люди массово «переехали» в Facebook (около 2,5 млн за первый месяц), где их там в шутку прозвали «переселенцами». В то же время в интернете начали активно продвигаться украинские соцсети, но успеха они не снискали.

(вгору)

Додаток 9

16.05.2018

Более 50 правозащитных организаций потребовали от российских властей отменить блокировку Telegram

53 международных и российских организации, занимающиеся защитой прав СМИ и интернет-свобод, осудили блокировку мессенджера Telegram и призвали Россию прекратить «атаку на свободу выражения мнения и неприкосновенность частной жизни в интернете». Об этом пишет «Новая газета» со ссылкой на текст обращения (InternetUA).

В число организаций, выступивших в поддержку обращения, вошли Amnesty International, Transparency International, Access Now, Development of Democracy and Human Rights, «Репортеры без границ», Московская Хельсинкская Группа, правозащитный центр «Мемориал», Международная «Агора», Фонд защиты гласности и другие.

«Мы призываем российские власти остановить блокировку Telegram и прекратить беспрестанные нападки на свободу интернета в целом. Мы также призываем Организацию Объединенных Наций, Совет Европы, Организацию по безопасности и сотрудничеству в Европе, Европейский Союз, Соединенные Штаты Америки и другие заинтересованные правительства отреагировать на действия властей России и поддержать основополагающие права на свободу выражения мнения и неприкосновенность частной жизни в интернете и вне его. Наконец, мы призываем интернет-компании противостоять необоснованным и неправовым требованиям, нарушающим права их пользователей», – говорится в заявлении.

Кроме того, авторы обращения потребовали от российских властей отменить положения «закона Яровой», обязывающие операторов связи хранить трафик и записи разговоров абонентов, отменить закон о локализации персональных данных, отменить закон, запрещающий анонимность пользователей мессенджеров и закон о запрете сервисов обхода блокировок, позволяющих получить доступ к запрещенным ресурсам. Наконец, правозащитники призвали внести изменения в закон об информации, чтобы процесс блокировки веб-сайтов соответствовал международным стандартам.

«Возмущение общественности отражает степень вмешательства в работу интернета, вызванного попыткой российских властей заблокировать Telegram, и серьезное отрицательное воздействие на свободу выражения мнения и доступ к информации», – отметила директор Центра защиты прав СМИ Галина Арапова, подчеркнув, что российское общество постоянно сталкивается с ограничениями в интернете и с нарушением фундаментальных прав человека.

В свою очередь, исполнительный директор организации ARTICLE 19 Томас Хьюз заявил, что защита интернет-свобод требует решительной реакции со стороны всех заинтересованных организаций и компаний.

«Мы все должны быть обеспокоены, это не только российская проблема. Такие действия влияют на обмен информацией между нами и на слежку, которой мы подвергаемся в интернете, в особенности с учетом того, что Россия пытается принудить интернет-компании выполнять распоряжения, нарушающие права их пользователей, в том числе право на безопасное и конфиденциальное общение», – сказал Хьюз.

(вгору)

Додаток 10

10.05.2018
Владимир Кондрашов
Украинские хакеры поздравили россиян с «днем победобесия»

Хактивисты объединения Украинский киберальянс 10 мая взломали около двух сотен так называемых новостных ресурсов Российской Федерации и террористических организаций «ДНР» и «ЛНР» (InternetUA).

Соответствующую информацию на своей странице в Facebook разместил спикер Украинского киберальянса, известный под ником Шон Таунсенд.

– Дорогие россияне! Если вы думали, что Ukrainian Cyber Alliance о вас забыл, то вы ошибаетесь. Искренне поздравляем вас с прошедшим «днём победобесия» и берём на себя ответственность за взлом сайтов «Мой Донецк», «Инфорос». Всего более двухсот сайтов, – написал спикер УКА.

Среди взломанных, кроме «Мой Донецк» и «Инфорос», – новостные ресурсы большинства российских регионов от Астраханской области и Белгорода до Петербурга и Южно-Сахалинска. Также в списке несколько коммерческих порталов.

Текст «9 мая. Afterparty» появился на порталах сегодня около полудня.

– Нацизм не был уничтожен, он был захвачен Россией как самый ценный трофей. Вы поменяли миллионы жизней на возможность самим занять место агрессора. Снова устраивают рейды ряженые казаки, чтобы грабить, насиловать и убивать мирное население на Донбассе, снова российские оккупационные войска, нахлынули на мирных соседей, словно саранча. Пока похмельные российские свиньи отходят от «Великого дня Победы», мы помним, – говорится в опубликованном обращении. – Каждый российский оккупант, каждый коллаборант и предатель в Крыму и на Донбассе будет найден и понесёт заслуженное наказание. Пам’ятаємо. Перемагаємо.

Как уточнил спикер УКА в комментарии нашему изданию, сайты не подбирались каким-то специальным образом:

– Мы использовали для дефейса те, которые для нас уже больше не представляют ценности, чтобы понятным и доступным способом обозначить своё присутствие в информационном пространстве. С теми ресурсами, где есть возможность получить интересную информацию, мы продолжаем работать, не привлекая к себе внимания.

(вгору)

Додаток 11

12.05.2018

Пользователям Facebook угрожает новая вредоносная кампания

Эксперты компании Radware предупредили о новой вредоносной кампании, в рамках которой злоумышленники через ссылки в социальной сети Facebook распространяют вредоносное ПО Nigelthorn, способное красть учетные данные пользователей и устанавливать майнеры криптовалюты. Исследователи обнаружили 7 вредоносных расширений для Google Chrome, содержащих Nigelthorn, причем все они были размещены в официальном магазине Chrome Web Store (InternetUA).

Вредоносная кампания активна по меньшей мере с марта нынешнего года. С момента ее начала от Nigelthorn пострадало более 100 тыс. пользователей по всему миру. По данным Radware, злоумышленники внедряют вредоносный скрипт в копии легитимных расширений и таким образом обходят проверку Google. Вредонос маскируется под следующие расширения: Nigelify, PwnerLike, Alt-j, Fix-case, Divinity 2 Original Sin: Wiki Skill Popup, Keeprivate и iHabno.

Nigelthorn распространяется через ссылки в Facebook, при переходе по которым пользователи попадают на фальшивую страницу в YouTube, предлагающую загрузить расширения для дальнейшего просмотра видео. После установки вредоносное расширение выполняет скрипт JavaScript, в результате устройство пользователя становится частью ботнета. Основная задача вредоноса заключается в краже учетных данных для аккаунтов жертвы в Facebook и Instagram и хищения содержащейся в них информации. Данные сведения используются для отправки вредоносных ссылок друзьям пользователя.

Кроме прочего, Nigelthorn загружает и устанавливает майнер криптовалюты для добычи цифровых средств, в том числе Monero, Bytecoin или Electroneum. По данным исследователей, за 6 дней операторам вредоноса удалось заработать примерно $1 тыс. в криптовалюте, в основном в Monero.

Вредонос препятствует удалению вредоносного расширения, автоматически закрывая его вкладку. Кроме того, Nigelthorn вносит в черный список все инструменты для очистки, предлагаемые Facebook и Google, а также не позволяет пользователям делать изменения, удалять публикации или оставлять комментарии.

В настоящее время все указанные выше расширения уже удалены из Chrome Web Store. Пользователям, загрузившим какое-либо из расширений, рекомендуется деинсталлировать его и сменить все пароли для Facebook, Instagram и других сервисов, где используются те же учетные данные.

(вгору)

Додаток 12

14.05.2018

Сложный шифровальщик использует новую технику для обхода защиты

Аналитики «Лаборатории Касперского» обнаружили троянца-шифровальщика, который использует новую технику для обхода защитных решений и старательно избегает компьютеров с кириллической раскладкой на клавиатуре. Речь идёт о новой версии уже известного зловреда SynAck. Как выяснили эксперты, он первым из шифровальщиков начал использовать так называемую технику Doppelgänging, которая позволяет вредоносной программе маскироваться под легитимный процесс. Если учесть, что в этом ПО применяются также и другие методы «обмана» антивирусных решений, то

задача обнаружения его присутствия в системе становится довольно сложной (Компьютерное Обозрение).

SynAck известен с осени 2017 г. Тогда он атаковал преимущественно англоговорящих пользователей и задействовал для этого брутфорс-технику (метод перебора пароля) с последующей ручной установкой вредоносного файла. Однако новая версия шифровальщика стала на порядок сложнее. К примеру, используемая в ней техника Doppelgänging эксплуатирует недокументированную возможность загрузки процессов в Windows и позволяет внедрить бесфайловый вредоносный код в легитимные системные процессы. В итоге шифровальщик не оставляет никаких следов в заражённой системе.

Как полагают исследователи, SynAck выбирает своих жертв довольно тщательно, поэтому сейчас атаки шифровальщика носят целевой характер. К настоящему моменту заражения зафиксированы в США, Кувейте, Германии и Иране. Средний размер выкупа, который требует зловред, составляет 3000 долл.

«Игра на опережение между атакующими и защитниками в киберпространстве никогда не останавливается. Новая техника Doppelgänging позволяет вредоносному ПО проскользнуть мимо радаров даже самых современных защитных технологий. Неудивительно, что злоумышленники не замедлили воспользоваться ей. Но к счастью, логика детектирования подобных угроз была добавлена в защитные решения прежде, чем они стали реальностью», – отметил Антон Иванов, антивирусный эксперт «Лаборатории Касперского».

(вгору)

Додаток 13

15.05.2018
«Доктор Веб» выявил автора троянцев-шпионов

В конце марта компания «Доктор Веб» сообщила о распространении троянца, похищающего с зараженных устройств файлы и другую конфиденциальную информацию (ITnews).

Вирусные аналитики исследовали несколько новых модификаций этой вредоносной программы и выявили ее разработчика.

Специалисты компании «Доктор Веб» изучили несколько новых модификаций троянца Trojan.PWS.Stealer.23012, распространявшегося по ссылкам в комментариях к видеороликам на популярном интернет-ресурсе YouTube. Эти ролики были посвящены использованию специальных программ, облегчающих прохождение компьютерных игр, – читов и «трейнеров». Под видом таких приложений злоумышленники и раздавали троянца-шпиона, оставляя с поддельных аккаунтов комментарии к видеороликам со ссылкой на Яндекс.Диск. Также эти вредоносные ссылки злоумышленники активно рекламировали в Twitter.

Все исследованные модификации шпиона написаны на языке Python и преобразованы в исполняемый файл с помощью программы py2exe. Одна из новых версий этой вредоносной программы, получившая наименование Trojan.PWS.Stealer.23370, сканирует диски инфицированного устройства в поисках сохраненных паролей и файлов cookies браузеров, основанных на Chromium. Кроме того, этот троянец ворует информацию из мессенджера Telegram, FTP-клиента FileZilla, а также копирует файлы изображений и офисных документов по заранее заданному списку. Полученные данные троянец упаковывает в архив и сохраняет его на Яндекс.Диск.

Другая модификация этого троянца-шпиона получила наименование Trojan.PWS.Stealer.23700. Эта вредоносная программа крадет пароли и файлы cookies из браузеров Google Chrome, Opera, Яндекс.Браузер, Vivaldi, Kometa, Orbitum, Comodo, Amigo и Torch. Помимо этого, троянец копирует файлы ssfn из подпапки config приложения Steam, а также данные, необходимые для доступа к учетной записи Telegram. Кроме того, шпион создает копии изображений и документов, хранящихся на Рабочем столе Windows. Всю украденную информацию он упаковывает в архив и загружает в облачное хранилище pCloud.

Третья модификация шпиона получила наименование Trojan.PWS.Stealer.23732. Дроппер этого троянца написан на языке Autoit, он сохраняет на диск и запускает несколько приложений, являющихся компонентами вредоносной программы. Один из них представляет собой шпионский модуль, как и его предшественники, написанный на языке Python и преобразованный в исполняемый файл. Он ворует на инфицированном устройстве конфиденциальную информацию. Все остальные компоненты троянца написаны на языке Go. Один из них сканирует диски в поисках папок, в которых установлены браузеры, а еще один упаковывает похищенные данные в архивы и загружает их в хранилище pCloud.

Для распространения этой модификации стилера купившие его у вирусописателя злоумышленники придумали еще один, более оригинальный метод. Киберпреступники связывались с администраторами тематических Telegram-каналов и предлагали им написать пост, посвященный якобы разработанной ими новой программе, и предлагали ее протестировать. По словам злоумышленников, эта программа позволяла одновременно подключаться к нескольким аккаунтам Telegram на одном компьютере. На самом же деле под видом полезного приложения они предлагали потенциальной жертве скачать троянца-шпиона.

В коде этих троянцев-шпионов вирусные аналитики обнаружили информацию, позволившую установить автора вредоносных программ. Вирусописатель скрывается под псевдонимом «Енот Погромист», при этом он не только разрабатывает троянцев, но и продает их на одном популярном сайте.

Создатель троянцев-шпионов также ведет канал на YouTube, посвященный разработке вредоносного ПО, и имеет собственную страницу на GitHub, где выкладывает исходный код своих вредоносных программ.

Специалисты «Доктор Веб» проанализировали данные открытых источников и установили несколько электронных адресов разработчика этих троянцев, а также номер его мобильного телефона, к которому привязан используемый для противоправной деятельности аккаунт Telegram. Кроме того, удалось отыскать ряд доменов, используемых вирусописателем для распространения вредоносных программ, а также определить город его проживания. На представленной ниже схеме показана часть выявленных связей «Енота Погромиста» с используемыми им техническими ресурсами.

Логины и пароли от облачных хранилищ, в которые загружаются архивы с украденными файлами, «зашиты» в тело самих троянцев, что позволяет без особого труда вычислить и всех клиентов «Енота Погромиста», приобретавших у него вредоносное ПО. В основном это граждане России и Украины. Некоторые из них используют адреса электронной почты, по которым нетрудно определить их страницы в социальных сетях и установить их реальную личность. Например, сотрудникам «Доктор Веб» удалось выяснить, что многие клиенты «Енота Погромиста» пользуются и другими троянцами-шпионами, которые продаются на подпольных форумах. Следует отметить, что отдельные покупатели оказались настолько умны и сообразительны, что запускали шпиона на своих собственных компьютерах, вероятно, в попытке оценить его работу. В результате их личные файлы были загружены в облачные хранилища, данные для доступа к которым может без труда извлечь из тела троянца любой исследователь.

(вгору)

Додаток 14

17.05.2018

За вами стежать: чим небезпечні VPN-сервіси

Інтернет-користувачі дедалі частіше намагаються захистити свої персональні дані. Одним із способів є використання VPN. Втім, цього недостатньо (InternetUA).

Спроби зберегти конфіденційність в інтернеті стають дедалі популярнішими.

Користувачі обережніше поводяться з використанням геолокації на телефоні або з реєстрацією на сайтах за допомогою менеджера паролів. Іноді вони заклеюють камери на ноутбуках та обирають для листування приватні месенджери.

Одним із способів убезпечення своєї присутності в мережі є використання VPN. Чи надійний цей інструмент?

Що таке VPN і як він працює

VPN розшифровується як Virtual Private Network – віртуальна приватна мережа. «Віртуальна» – бо для неї не потрібно прокладати фізичне з'єднання, VPN працює на основі всесвітньої мережі. Приватна – бо вона не доступна для сторонніх.

Образно кажучи, VPN – це додатковий «конверт» або «тунель», у який користувач кладе своє повідомлення, щоб ніхто не побачив його зміст.

VPN дозволяє приховати особу і місце розташування в мережі, захищає дані, гарантує безпеку інформації. Користувач може заходити на сайти, заблоковані у його країні. При цьому його майже неможливо вистежити.

Як заробляє безкоштовний VPN

Абсолютно безкоштовних сервісів VPN не існує. Завантажуючи додаток у смартфон, користувач уже сплачує певну ціну. Хтось змушений дивитися рекламу, хтось платить гроші за додаток, хтось повідомляє додатку свої особисті дані.

Перші два способи – це прозора монетизація. Сервіс заробляє або на платі за користування, або на рекламі. Третій варіант – ризикований. Якщо VPN-сервіс не пропонує реклами, а його використання безкоштовне, існує висока ймовірність, що сервіс продає особисту інформацію користувачів рекламодавцям.

Можливий ще гірший варіант. В інформації, якою володіють VPN-сервіси, зазвичай зацікавлена влада, і є ризик тіньової співпраці сервісу з державними органами. Щоб зменшити такий ризик, можна обрати VPN-сервіс іншої країни.

Платні сервіси хоч і зменшують ризики витоку особистої інформації, але їм нічого не заважає використовувати всі способи монетизації, у тому числі продаж даних.

Чим загрожує неперевірений провайдер

VPN-сервіс приховує з'єднання від стороннього ока, але сам він бачить усе. Якщо сервісом володіють зловмисники, вони отримають усю інформацію користувача.

Атаки всередині VPN можна поділити на два види: пасивні та активні.

Пасивні – це збирання даних без втручання в процес передавання інформації. Вони дозволяють бачити історію переглядів сайтів і листи без шифрування. Активні – це викривлення та викрадення даних, що передаються.

«VPN-сервіс передбачає, що весь трафік користувача проходить через третю сторону – комерційну організацію. Вона має повний доступ до вашого трафіку.

Приклад Фейсбуку показує, наскільки низьким може бути рівень відповідальності компаній, які мають доступ до персональних даних. Фейсбук – це великий гравець, до якого прикута увага громадськості. Що вже говорити про маленьку компанію, яка пропонує VPN-сервіс?» – коментує директор з корпоративних сервісів Information Systems Security Partners Артем Михайлов.

Як обрати надійний VPN-сервіс

Відрізнити перевірений додаток від неперевіреного можна кількома способами.

По-перше, потрібно звернути увагу на власника VPN-сервісу.

В описі кожного додатка мусить бути ім'я автора і цифровий підпис перевіреної контрольними органами організації.

Також варто прочитати відгуки користувачів.

По-друге, треба звернути увагу на кількість серверів та країн, які використовує VPN: чим їх більше, тим краще.

«Якщо країн понад 50, компанія зареєстрована в офшорній зоні і присутня на ринку понад десять років, їй можна довіряти», – вважає голова відділу кібербезпеки компанії Hacken Микита Книш.

По-третє, варто уважно прочитати умови конфіденційності. У них вказані підстави, за яких сервер видає персональні дані користувачів, а також інформація про термін їх зберігання. Довіряти можна сервісу, який оприлюднює дані лише за рішенням суду і зберігає інформацію протягом одного-десяти днів.

«Я би радив бути пильними щодо тих VPN, які були створені після обмеження доступу до російських сайтів. Вони можуть бути пасткою», – каже Книш.

Чи можна чимось замінити VPN

Існує багато інструментів, які можуть замінити VPN: TOR Browser, I2P, Freenet, GNUnet, HTTP проксі-сервери, SOCKS проксі-сервери, CGI-проксі або «анонімайзери». Усе залежить від того, для чого потрібен сервіс. Найбільш анонімним є TOR Browser. Його недолік – низька швидкість передавання даних.

VPN-сервіси бувають різними. Є приватні VPN, які можна створити на власному сервері, є VPN, які надає браузер, є автономні VPN, які можна завантажити з інтернету. Найбільш безпечним є VPN-сервіс, створений користувачем самостійно.

Сленговою мовою це називається «підняти свій VPN», тобто орендувати фізичний чи віртуальний сервер і розгорнути на ньому власну інфраструктуру, яка об'єднуватиме певну кількість комп'ютерів. Софт для цього можна налагодити самостійно або завантажити готовий пакет інструментів з мережі.

Втім, одного лише VPN для захисту даних від кібератак недостатньо. VPN-сервер буде безсилим, якщо користувач завантажуватиме неперевірені додатки, використовуватиме однакові паролі та заходитиме на підозрілі інтернет-сторінки.

(вгору)

Додаток 15

17.05.2018

Обнаружены уязвимости нулевого дня в продуктах Adobe и Microsoft

Специалисты ESET обнаружили две новые, ранее неизвестные уязвимости в Adobe Reader и Microsoft Windows. Эксплойты, использующие «двойную уязвимость», были внедрены во вредоносный PDF-файл (Компьютерное Обозрение).

В конце марта внимание специалистов ESET привлек необычный PDF-файл, загруженный в публичный сервис для сканирования вредоносных программ. Изучив образец, эксперты установили, что в нем используются две

0-day бреши: уязвимость удаленного выполнения кода в Adobe Reader и уязвимость повышения привилегий в Microsoft Windows.

Сочетание двух уязвимостей крайне опасно, поскольку позволяет злоумышленникам выполнять произвольный код на компьютере жертвы с максимальными привилегиями и минимальным необходимым участием пользователя.

Файлы в формате PDF нередко используют для распространения вредоносного ПО. Чтобы выполнить вредоносный код на компьютере жертвы, атакующие ищут и используют уязвимости в программах для просмотра PDF, в частности, в Adobe Reader.

В Adobe Reader внедрена технология защиты от вредоносного кода (песочница) – Protected Mode. Песочница усложняет задачу злоумышленников. Чтобы обойти защиту, атакующие, как правило, используют уязвимости в самой операционной системе.

В данном случае злоумышленники нашли уязвимости и написали эксплойты как для Adobe Reader, так и для операционной системы – сравнительно редкий случай, иллюстрирующий высокую квалификацию авторов.

Чтобы сработала «двойная уязвимость», пользователю достаточно открыть вредоносный PDF-файл на компьютере с уязвимой версией Adobe Reader и операционной системы.

Образец PDF, обнаруженный специалистами ESET, не содержал финальной полезной нагрузки – вредоносной программы, установка которой является целью атаки. Возможно, экспертам удалось найти образец на ранних этапах разработки и принять меры, связавшись с Adobe и Microsoft для закрытия уязвимостей.

(вгору)

Додаток 16

17.05.2018
Ирина Фоменко
Распознавание лиц может стать угрозой в руках полиции

Научная фантастика часто является предшественником научного факта. Действие в некоторых из лучших антиутопических романов и фильмов происходит в кошмарном мире, где государство может везде за вами следить, поскольку ваше лицо идентифицируется и сравнивается с базой данных населения (InternetUA).

Теперь распознавание лица стало реальностью, сообщает The Guardian. Полиция сканирует тысячи наших лиц – на протестах, футбольных матчах и музыкальных фестивалях – и сравнивает их с секретными базами данных.

Единственная разница: в книгах и фильмах эта технология всегда работала. 15 мая Big Brother Watch опубликовал результаты своего расследования по использованию программного обеспечения для

распознавания лиц в полиции. Оказалось, что технология Met на 98 % ошибочна.

Это не стало большим сюрпризом для Liberty. В Атлантике алгоритм распознавания лиц ФБР регулярно ошибается на женщинах и представителях других рас. Эта технология может стать серьезным риском в вопросе несправедливости из-за ложной идентификации и делает каждого из нас вечным полицейским.

Распознавание лица существует в регуляторном вакууме. Оно не подпадает под такую же нормативную базу, как наблюдение с помощью камеры и другие биометрические данные, например, отпечатки пальцев и ДНК. Парламент никогда не обсуждал этот вопрос.

И автоматическая технология идентификации лиц не является пассивной, как CCTV. Она загружает камеры наблюдения с помощью биометрического программного обеспечения для создания уникальных характеристик лица в реальном времени. Затем полученные данные измеряются и сопоставляются с изображением.

Несмотря на слова полиции о необходимости внедрения этой технологии для нашей же безопасности, база данных, на которой сравнивались лица тысяч людей на праздновании Дня памяти в ноябре прошлого года, была составлена из продемонстрировавших навязчивое поведение по отношению к конкретным общественным деятелям.

Это лишь маленький пример того, что может произойти, когда существует бесконтрольная и не регулируемая правом технология. Это полицейская деятельность без ограничений.

Без законодательства, руководства, политики или надзора технологию распознавания лиц нельзя использовать, иначе последствия для нашей свободы могут быть крайне негативными. У полиции будет изображение лица каждого человека, прошедшего мимо этих камер. И, если вам не повезет, и вас идентифицируют как преступника (разумеется, ложно), придется доказать свою личность полиции или быть арестованным за несовершенное преступление.

Нетрудно представить, какое негативное влияние будет оказывать неограниченное использование. Постоянное наблюдение приводит к тому, что люди «самоцензурируют» законное поведение. Скрытно эти меры ограничивают наше право на протест, свободу слова и инакомыслие.

Кроме того, эта технология наиболее опасна для людей, которые в ней нуждаются больше всего. Технологии, неправильно идентифицирующие женщин и людей из этнических меньшинств, лишают гражданских прав тех, кто уже столкнулся с неравенством.

В свою очередь, правительство утверждает, что технология только развивается. Но это не оправдывает то, что она оказывает негативное воздействия на людей здесь и сейчас. У британской полиции появилась тенденция – внедрять все новые инструменты и технологии, не одобренные обществом.

14 мая комиссар по вопросам информации Элизабет Денхам заявила, что, если Министерство внутренних дел и полиция не обратит внимание на ее опасения относительно использования технологии распознавания лиц, она рассмотрит вопрос о принятии юридических мер для обеспечения защиты общественности.

(вгору)

Додаток 17

18.05.2018

SAS: только 7 % компаний готовы к новому европейскому регламенту по защите данных

Только 7 % компаний, работающих на международном рынке, полностью готовы к вступлению в силу нового регламента по защите данных General Data Protection Regulation (GDPR), сообщает SAS. Исследование компании, которое проводилось с февраля по апрель, выяснило, с какими вызовами сталкивается бизнес в связи с введением новых правил защиты данных пользователей. В число респондентов вошли представители компаний из разных стран мира, действующих в разных сферах бизнеса (Компьютерное Обозрение).

GDPR начинает действовать на территории Евросоюза уже с 25 мая. Этой дате предшествовал двухлетний переходный период. Действие регламента распространяется на любые организации, которые оперируют персональными данными физических лиц, находящихся на территории Евросоюза, как его граждан, так и резидентов других государств. Это значит, что требования GDPR придется выполнять всем компаниям, которые предоставляют свои услуги на территории Евросоюза.

Несмотря на переходной период, к внедрению новых правил международный бизнес оказался не готов. Как выяснили в SAS, меньше половины респондентов (46 %) уверены, что к 25 мая их компании будут соответствовать требованиям регламента. При этом в самом Евросоюзе ситуация чуть лучше, чем в мире – там этот показатель составил 53 %. Тогда как в США лишь 30 % компаний будут соответствовать новым требованиям.

При этом 68 % респондентов ожидают, что GDPR поможет улучшить имидж их компании, 84 % – что GDPR поможет им эффективнее управлять данными, 63 % ожидают, что правила окажут заметный эффект на бизнес-процессы в целом, а 49 % видят их прямое влияние на проекты, связанные с искусственным интеллектом.

58 % компаний уже разработали структурированный план перехода на новые правила, а еще 35 % компаний собираются это сделать в ближайшее время. Согласно результатам прошлогоднего опроса SAS, еще год назад таких компаний было всего 45 %. Однако для создания подобного плана представителям бизнеса требуется помощь экспертов – 75 % организаций получили или собираются получить ее от консалтинговых компаний или вендоров, обладающих опытом в работе с данными.

(вгору)

Додаток 18

21.05.2018

Михаил Сапитон

Google много обо мне знает. Но почему он не так страшен, как Facebook

В апреле 2018-го журналист The New York Times Брайан Чен провел над собой эксперимент. Он скачал все данные, которые о нем узнала Facebook и детально изучил их. Результаты исследования его удивили и напугали (AIN.UA).

Следом Чен загрузил архив всех данных, которые о нем знаете Google – и написал новую колонку. Несмотря на внушительный объем информации, она оказалась гораздо менее устрашающей. Редактор AIN.UA приводит адаптированный перевод материала.

Чен подмечает парадокс: хотя Google знает о нас гораздо больше, чем Facebook, компания избегает скандалов. У нее на руках – не только данные поисковых запросов, но и почта, календари, карты, фотографии, видео, сведения о мобильных устройствах и данные Chrome. Вместе они гораздо объемнее, чем посты и комментарии на Facebook.

Эта тенденция отразилась на объеме данных. Личный профайл Чена от Google в 12 раз «тяжелее» досье от Facebook. Там были и неприятные неожиданности.

Большую часть того, что я увидел в файле от Google, было знакомо. Я знал, что там окажутся фотографии, документы или письма, в то время как Facebook сохранил список 500 рекламодателей, обладающих моей контактной информацией. И еще – постоянный список друзей, которых я считал «удаленными» годы назад.

Данные, который беспокоили Чена – например, список всех открытых за последние годы Android-приложений – можно было удалить. С Facebook такой возможности часто не было. Журналист рекомендует каждому последовать его примеру и самостоятельно изучить, что же знают о вас крупные компании.

В случае с Google, сделать это несложно. Инструмент для скачивания данных называется Takeout. Его представили в 2008 году. Достаточно перейти на страницу проекта и выбрать тип сведений, который вас интересует. Чен предупреждает – файл со всеми разделами окажется огромным. В его случае – это были 8 Гб. Google потребовалось полдня на подготовку архива. Ссылка на скачивание пришла на почту.

Важнейшая папка называется My Activity – она включает обзор всех ключевых действий с продуктами Google. Автор также рекомендует обратить внимание на вложенную папку с рекламными материалами, Ads. Когда вы посещаете сайты, на которых крутится реклама через сети Google, это учитывается в профайле.

Подпапка Android сфокусирована на мобильной ОС. Там есть записи об дате и времени открытия каждого Android-приложения. Они используются для системных подсказок. Данные напугали Чена. Подумав, он отключил функцию.

Некоторые файлы открыть было непросто – они хранятся в расширениях вроде .JSON. Среди таких, например, данные из приложения Maps. Google оправдывает это тем, что в таком виде их удобно использовать для программных инструментов. Чен жалуется – люди тоже должны иметь возможность открыть файлы.

Журналист советует каждому, кто взялся за такое исследование, задать себе вопрос: «Существование каких данных для меня некомфортно?». Его смутила информация о посещении сайтов, которая собиралась даже без использования Google-продуктов. Также – пункт о приложениях.

Избавиться от поводов для беспокойства можно на myactivity.google.com. Таким образом Чен удалил рекламные данные для трекинга, Android-данные, историю запросов к Google Assistant, историю веб-браузинга в Google News и Chrome. Но действительно ли это значит, что информация пропала? Как объяснил ему пресс-секретарь Google, у разных данных – разный срок окончательной удаления с серверов. Что-то пропадает сразу, что-то со временем.

Возможно, это не покажется таким уж утешением. Но вместо того, чтобы совсем завязать с использованием интернета, лучше иногда поступать с данными, как с домашним мусором – время от времени выбрасывать все ненужное.

(вгору)

Додаток 19

21.05.2018
Владимир Кондрашов
Новая угроза для украинских IT компаний

25 мая начинает действовать Общий регламент Европейского Союза по защите данных (GDPR). Этот документ приходит на замену ныне действующей Директиве ЕС и вносит существенные коррективы в европейскую политику защиты персональных данных (InternetUA).

Как неоднократно отмечалось экспертами, несоблюдение Регламента, благодаря его трансграничным нормам, суровым условиям и драконовским штрафам, может существенно ударить по украинским компаниям, работающим с данными граждан Евросоюза.

InternetUA собрал самые распространенные вопросы о GDPR, и попытался на них ответить.

Что конкретно поменялось

Общий регламент Европейского Союза по защите данных призван гарантировать гражданам ЕС лучшую защиту персональных данных, вне зависимости о того, на какой территории эти данные хранятся.

Регламент, по сравнению с предыдущей Директивой, существенно расширяет понятие персональных данных, уточняет и расширяет понятие чувствительных данных. Как объясняет Сергей Богарада, Head of Personal data practice, Legal IT Group в статье для «Юрист&Закон», теперь персональные данные – это любая информация, относящаяся к идентифицированному физическому лицу или тому лицу, которое может быть идентифицировано («субъект данных»). При этом идентифицированное лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, на основании идентификационной информации, такой как имя, идентификационный номер, данные о местоположении, идентификатор в Интернете (онлайн-идентификатор) или с помощью одного или нескольких показателей, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности физического лица.

Чувствительные данные, согласно Общему Регламенту, определяются по ряду признаков, которые базируются на информации о расовом или этническом происхождении, политическим взглядам, религиозным или философским убеждениям, профессиональном членстве, здоровье или сексуальной жизни, генетических и биометрических данных.

Новый Регламент действует в отношении любой компании, независимо от её расположения, если бизнес работает с персональными данными граждан ЕС.

GDPR существенно расширяет права частных пользователей. Им предоставляются права на перемещение, ограничение обработки, отрицание и удаление данных. Также частным лицам предоставляется право на получение ответа на запрос.

Согласно новым правилам, компании теперь обязаны сообщать об утечках данных и вести журнал учета таких случаев.

Также GDPR устанавливает новые правила получения согласия на обработку персональных данных. В частности, предусматривается два вида согласия: простое согласие и безусловное согласие.

Простое согласие – конкретное и однозначное указание субъекта данных, при помощи заявления или четкого позитивного действия, которым выражается согласие на обработку данных.

Безусловное согласие предоставляется при обработке специальных категорий данных, перемещении данных в третьи страны и т. д.

– Предоставление безусловного согласия предполагает более тщательный подход к организации его получения. Так, например, если вы собираете общие персональные данные о субъекте данных, включая данные о расовом происхождении, то кроме обычного согласия вы также должны получить отдельное безусловное согласие на обработку чувствительных персональных данных, – указывает Сергей Богарада. – Безусловное согласие отличается от обычного согласия тем, что его предоставление требует предоставления значительно большего объема информации физическому лицу, описывающему особенности обработки чувствительных данных. Вместе с тем, физическое

лицо, предоставляя безусловное согласие, должно осуществить дополнительные действия для более четкого подтверждения своего согласия по обработке персональных данных о нем. В таком случае, в частности, может быть применен метод Double opt-in.

На что ещё обратить внимание украинским компаниям

В своей колонке коммерческий директор Information Systems Security Partners (ISSP) Андрей Слободяник обращает внимание на особо важные статьи Регламента, которые необходимо обязательно учитывать украинским компаниям, работающим на рынках Евросоюза.

Помимо обязательного согласия от клиента на обработку его данных (в случае, если речь идет о несовершеннолетнем – ещё и его родителей), своевременных докладов о взломе или компрометации данных и беспрекословного соблюдения прав граждан, у компании, работающей с персональными данными клиентов-граждан Евросоюза, должен быть представитель на территории ЕС для взаимоотношений с местными регуляторами. Также в обязательном порядке в компании назначается ответственное за работу с персональными данными лицо, проводится оценка рисков влияния манипуляций с личными данными на их носителей, учет всех пунктов работы с ПД.

– Немаловажно то, что GDPR не обязывает компании внедрять какие-либо конкретные приемы и методы защиты данных, – отмечает коммерческий директор ISSP . – Организации вправе самостоятельно выбирать систему обеспечения безопасности внутренних данных. Главное – конечный результат — надежная защита персональных данных.

Действительно ли будут драконовские штрафы и как их избежать

Общий регламент Европейского Союза по защите данных устанавливает достаточно серьезные штрафы за нарушение новой европолитики. В частности, компания может заплатить 20 миллионов евро или 4 % от годового дохода за нарушение ключевых положений Регламента, прав субъектов ПД, нормативов передачи личных данных и др. Меньше, 10 миллионов евро или 2 % от годового дохода, сулят нарушения процедуры получения согласия на хранение и обработку ПД несовершеннолетних, несоблюдения технических норм работы с ПД, отсутствие представителя в ЕС и др.

– Регламент накладывает на нарушителей максимальные штрафы, при этом полномочия по назначению конкретных сумм переданы местным органам власти государств-членов Евросоюза, – отмечает Андрей Слободяник. – Смягчающим моментом является тот факт, что в отдельных случаях вместо штрафа дело может ограничиться выговором. Например, когда регулятор признает правонарушение незначительным.

О том, как на практике будет действовать наказание за нарушение GDPR рассказал юрист Европейского суда и бывший руководитель Управления защиты персональных данных Секретариата Уполномоченного Верховной Рады Украины в 2013-2015 гг. Маркиян Бэм. По словам эксперта, постоянным представителем компании на территории ЕС может быть как юридическое, так

и физическое лицо, четко уполномоченное на это отдельным письменным документом. В случае, если орган надзора ЕС обвиняет украинскую компанию в нарушении законодательства о защите персональных данных, тогда компания сама подпадает под юрисдикцию того органа, сама появляется в суды, признает нарушение, если оно действительно было, и выплачивает соответствующую компенсацию.

– Другой случай – это когда компания не является, но отвечает ее представитель. Третий случай – это когда компания игнорирует такие запросы, но, на первый взгляд, многим компаниям кажется, что они могут не назначать представителя, или в случае каких-то проблем не платить штрафы, но тогда применяются другие механизмы воздействия, – рассказывает эксперт. – Наиболее минимальное, что может быть, это если она не будет отвечать на запрос надзорного органа или суда – надзорный орган даст указание компании, расположенной на территории ЕС, приостановить поток или передачу данных в Украине. В случае, когда украинская компания собирается сотрудничать с компанией по территории ЕС, то она обязана придерживаться этих положений. Регламент построен таким образом, чтобы не только заставить к чему компанию на территории Украины, но и заставить компанию с территории ЕС тщательно подбирать своих контрагентов по обработке персональных данных из-за территории Европейского Союза. Скажем, компания-владелец в ЕС поручает обрабатывать персональные данные компании на территории Украины, она понимает, что в случае нарушения регламента первой под удар попадает именно она, ей невыгодно работать с ненадежными компаниями в Украине, которые не соблюдают положений регламента. То есть, это миф, что украинские компании могут не соблюдать регламент. Если они работают с компаниями из ЕС, они должны его придерживаться.

На сегодня, по имеющимся данным, практически все украинские компании, работающие с персональными данными клиентов с ЕС, уже подготовились к приходу GDPR. Смогут ли они удержаться на плаву, учитывая печальный опыт украинских компаний в хранении данных пользователей, эксперты гадать не берутся.

(вгору)

Додаток 20

21.05.2018

Зловред Roaming Mantis атакует пользователей через взломанные роутеры

Аналитики «Лаборатории Каперского» обнаружили зловред Roaming Mantis, который поначалу атаковал преимущественно пользователей азиатско-тихоокеанского региона, однако теперь достаточно быстро стал распространяться по миру (Компьютерное Обозрение).

Зловред использует взломанные Wi-Fi роутеры, чтобы заражать смартфоны и планшеты на Android, перенаправлять устройства на iOS на фишинговый сайт и запускать майнинговый скрипт CoinHive на десктопах и ноутбуках. Для всего этого он применяет DNS hijacking – подмену DNS, поэтому довольно сложно заметить, что что-то идет не так.

Создатели Roaming Mantis прописывают в настройках скомпрометированных роутеров свои адреса DNS-серверов. После этого, что бы пользователь ни набрал в адресной строке браузера на подключенном к данному роутеру устройстве, его перенаправят на вредоносный сайт.

После того как пользователь был перенаправлен на вредоносный сайт, выводится предупреждение о том, что ему следует обновить браузер. После этого начинается загрузка вредоносного приложения с именем chrome.apk (также существует версия с именем facebook.apk).

В процессе установки зловред запрашивает уйму различных разрешений – в том числе на доступ к информации об аккаунтах, получение и отправку SMS и обработку голосовых звонков, запись аудио, доступ к файлам, отображение своего окна поверх других и так далее. Для такого доверенного приложения, как Google Chrome, этот список выглядит не таким уж подозрительным – если уж пользователь поверил, что это легитимный браузер, то разрешения наверняка выдаст, даже не особенно вчитываясь в запрос.

После установки приложения зловред использует право на доступ к списку аккаунтов, чтобы узнать, какая учетная запись используется в данном устройстве. А после этого пользователю выводится сообщение – в окне поверх всех остальных, на это зловред также запрашивал право – о том, что с его аккаунтом что-то не в порядке и надо перелогиниться. Далее открывается страница, на которой пользователь должен ввести свое имя и дату рождения.

По всей видимости, впоследствии эти данные вместе с разрешениями на доступ к SMS, открывающим доступ к одноразовым кодам двухфакторной аутентификации, используются создателем Roaming Mantis для кражи аккаунтов Google.

Кроме того, Roaming Mantis умеет атаковать устройства, работающие под управлением iOS. Тут все происходит иначе, чем на Android. Вместо загрузки приложения вредоносный сайт сразу показывает предупреждение о том, что пользователю следует заново залогиниться в App Store – и показывает соответствующую страницу. При этом в адресной строке отображается вызывающий доверие адрес security.apple.com:

Причем в данном случае злоумышленники не стали ограничиваться кражей логина и пароля от Apple ID, и сразу после ввода этих данных требуют от пользователя ввести еще и номер банковской карты.

(вгору)

Додаток 21

22.05.2018
Владимир Кондрашов

За утечкой данных Запорожской АЭС стоят сотрудники отдела ядерной безопасности

Полиция открыла уголовное дело по факту несанкционированного вмешательства в работу компьютерных сетей ОП «Запорожская АЭС» ГП НАЭК «Энергоатом». Вмешательство повлекло утечку информации с ограниченным доступом ЗАЭС (InternetUA).

Причастными к утечке данных в местном отделении СБУ называют трех сотрудников отдела ядерной безопасности Запорожской АЭС, среди которых и его руководитель.

Информация об этом опубликована в Едином реестре судебных решений, передает InternetUA.

– Из Энергодарской местной прокуратуры в Запорожской области поступило сообщение о том, что неустановленные лица несанкционированно вмешались в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи на ОП «Запорожская АЭС» ГП НАЭК «Энергоатом», чем вызвали утечку информации, ограниченной для общего пользования, что может нанести значительный ущерб интересам указанного предприятия, – говорится в решении суда. – Во исполнение поручения следователя, поступило письмо из отдела в г. Энергодар УСБУ в Запорожской области, в котором указывается, что к указанному уголовному преступлению причастны 2 технолога отдела ядерной безопасности ЗАЭС и технолог – руководитель ОЯБ ОП ЗАЭС.

В апреле следователь 2-го отделения СО Энергодарского ОП ГУНП в Запорожской области, занимающийся расследованием данного дела, пытался получить копии материалов служебного расследования по факту использования несанкционированного созданного небрежными сотрудниками источника доступа к рабочей станции, а также копии приказов на назначение этих сотрудников и их функциональные обязанности. На ЗАЭС следователю отказали, из-за чего последний обратился в суд за разрешением на временный доступ к вещам и документам. Суд просьбу следователя удовлетворил.

Уголовное производство было открыто 19 марта, хотя информацию об утечке данных с Запорожской АЭС в рамках акции #fuckresponsibledisclosure, инициированной Украинским кибералья́нсом, опубликовал в ещё декабре прошлого года хактивист, известный под ником Дмитрий Орлов. Ему, напомним, удалось обнаружить в открытом доступе внутреннюю документацию ЗАЭС, среди которой такие документы как Акт технического состояния объекта ядерной безопасности, служебные записки, Анализ герметичности оболочек ТВЭЛ ТВС и прочее.

Тогда «Энергоатом» в ответ на запрос нашего журналиста признал наличие несанкционированного источника утечки информации – «созданного небрежными сотрудниками источниак доступа к рабочей станции (в составе обособленного сегмента локальной сети) ЗАЭС». В декабре же на Запорожской АЭС была создана комиссия по расследованию данного инцидента, а в пресс-

службе «Энергоатома» подчеркивали, что Госспецсвязи проводила тест на проникновение относительно информационного периметра ЗАЭС, который станция успешно прошла.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

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.