СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(14.03–27.03)

2018 № 6

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(14.03–27.03)
№ 6

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

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 6
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 9
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 13
Інформаційно-психологічний вплив мережевого спілкування на особистість 13
Маніпулятивні технології 15
Спецслужби і технології «соціального контролю» 18
Проблема захисту даних. DDOS та вірусні атаки 21
ДОДАТКИ 39

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

19.03.2018

Skype для Windows 10 подключили к Программе предварительной оценки приложений

Участникам программы Windows Insider, состоящим в круге обновления Skip Ahead, предложена новая версия приложения Skype для Windows 10. С этим обновлением оно было подключено к отдельной программе предварительной оценки приложений и получило новую функцию для Смешанной реальности (InternetUA).

Пользователи Смешанной реальности уже скоро смогут быстро начать звонок часто используемым контактам, разместив их в любом месте своего виртуального дома, что избавит от необходимости сначала открывать Skype. Удобно? Наверное. Жаль скриншотов нет.

Включение Skype для Windows 10 в Программу предварительной оценки позволит оценить новейшие функции приложения инсайдерам из любого круга обновления. Правда толкьо после того, как эта версия Скайпа (12.1811.247.0) до них доберётся.

Немногим ранее пользователи приложения получили возможность ответа на входящие звонки при включённом в Windows 10 режиме «Не беспокоить», получили инструмент для поиска сообщений в текущей беседе, а также избавились от необходимости добавления абонента в список контактов для старта общения с ним.

***

22.03.2018

YouTube разрешил стримить прямо с веб-камеры

Команда видеосервиса YouTube представила новую возможность – теперь можно вести живые трансляции на сайте YouTube прямо с веб-камеры. Вместо того чтобы возиться со специальными приложениями, пользователям достаточно иметь веб-камеру и браузер Chrome (InternetUA).

Для трансляции требуется зайти через Chrome по адресу youtube.com/webcam и нажать кнопку «Начать эфир» (Go live) в шапке сайта. Функция уже доступна в международном масштабе, но для её использования потребуется подтвердить собственный аккаунт с помощью номера телефона. Доступ к функции обычно появляется в течение 24 часов после одобрения. После этого пользователь получает ссылку в стиле youtube.com/c/ВасяПупкин/live, которой он может поделиться с подписчиками для просмотра трансляций.

Также команда YouTube пообещала скорый запуск возможности стриминга прямо с камеры смартфона. Она появится в ближайшие месяцы для «избранных» моделей ASUS, LG, Motorola, Nokia и Samsung.

***

26.03.2018
В WhatsApp появился новый способ отправки денег

WhatsApp тестирует отправку средств с одной банковской карты на другую, и в этом мессенджере появился ещё один способ перевода денег. WhatsApp позволяет осуществлять платежи сканируя QR-код. Это нововведение уже реализовано в бета-версии приложения для Android с номером 2.18.93, но доступно только в тех странах, где работает платёжная система WhatsApp (InternetUA).

Продавец может создать QR-код для оплаты товара, а пользователь, заинтересовавшийся этим товаром, может оплатить его через мессенджер. Для этого нужно включить в WhatsApp опцию платежей, перейти в «Настройки» > «Платежи», прокрутить экран вниз, выбрать «Новый платёж», запустить сканер QR-кодов, отсканировать код и завершить оплату с помощью банковской карты.

***

27.03.2018
Twitter выпустил новое приложение для Windows 10

В Microsoft Store опубликована новая версия приложения Twitter для Windows 10. С этим обновлением приложение стало простым клиентом для веб-версии с поддержкой уведомлений (PWA) (InternetUA).

Перевод приложения на PWA рельсы несёт в себе как очевидные плюсы, так и некоторые минусы для постоянных пользователей Twitter. Из положительного: возможность доступа ко всем новейшим функциям сервиса в день их запуска в веб-версии – ждать редких обновлений больше не придётся. Увеличенный лимит на количество символов в сообщении, закладки, обновлённый алгоритм для ленты, всё это уже доступно здесь и сейчас.

Что там с минусами? Новое PWA приложение вряд ли когда-нибудь будет выглядеть в Windows 10 нативно и естественно, вряд ли получит поддержку живой плитки. Будет показывать рекламу в ленте. Кроме того, как нам кажется, команда Twitter может в ближайшем времени отказаться и от этого приложения. Просто потому, что в нём нет никакого смысла. Уже скоро поддержкой PWA приложений обзаведутся все ведущие браузеры, включая Microsoft Edge. Чтобы пользоваться Twitter в отдельном окне достаточно будет закрепить сайт на панели задач, не устанавливая ничего из Microsoft Store.

Заметим, что от настольного приложения для компьютеров Apple команда Twitter отказалась уже сейчас. Мы совершенно не удивимся, если узнаем – за созданием PWA-версии клиента Twitter стоит Microsoft.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

22.03.2018

Одесский апелляционный административный суд создал чат-бота в Messenger. Его назвали Kurt

За работой Одесского апелляционнаго административного суда теперь можно следить с помощью чат-бота Kurt в Messenger.

Как сообщает пресс-служба суда, Kurt будет отвечать на все распространенные вопросы, которые касаются работы учреждения. В частности, о времени и месте заседаний. В дальнейшем также планируется создать таких ботов в Telegram, Viber и WhatsApp (Oblvesti).

***

22.03.2018

Крах агента 0,7: У соцмережах відреагували на позбавлення Савченко депутатської недоторканності

Користувачі соцмереж відреагували на позбавлення недоторканності і затримання одіозного народного депутата Надії Савченко.

Рішення парламенту викликало схвалення у патріотичної громадськості, однак з огляду на постать головної героїні, основна частина коментарів досить саркастичні (Інфотаб).

Зазначимо, у соцмережах не забули, що Савченко пройшла до Ради завдяки ВО «Батьківщина» Юлії Тимошенко. Коментатори наголошують, що сама Тимошенко має також відповідати за дії свого колишнього депутата.

Сама Тимошенко не прийшла до ВР на розгляд подання щодо зняття недоторканності з Савченко.

***

23.03.2018

Поліцейські Житомирщини долучилися до всеукраїнського флешмобу #КобзарСерцеУкраїни

Захід приурочений 204-ій річниці з Дня народження Тараса Григоровича Шевченка (zhitomirnews.com).

Поетичну естафету учасники флешмобу прийняли від колег з Головного управління Національної поліції в Дніпропетровській області та передали поліції Кіровоградщини.

***

26.03.2018

Французского политика арестовали за радость в Twitter по поводу смерти жандарма

Пуссье был кандидатом в депутаты французского парламента от леворадикальной партии (InternetUA).

Французский политик Стефан Пуссье арестован за размещение в своем микроблоге Twitter радостных сообщений после смерти полицейского в результате теракта в городе Треб. Об этом сообщает BBC.

В своих сообщениях Пуссье радовался смерти подполковника жандармерии Арно Бельтраме, который обменял себя на заложницу, и отметил, что это «прекрасно».

Он добавил, что теперь у президента Франции Эммануэля Макрона «будет на одного избирателя меньше».

Пуссье в своих сообщениях объяснял, что считает французскую полицию виновной в смерти своего друга, экоактивиста Реми Фреса, который погиб во время столкновений с полицейскими в 2014 году в результате взрыва. Сейчас, по сообщениям местных СМИ, политика могут обвинить в публичном оправдании терроризма. По информации Le Monde за это ему грозит наказание в семь лет и 100 тыс. евро штрафа.

Стефан Пуссье был кандидатом в депутаты французского парламента от леворадикальной партии «Строптивая Франция» на парламентских выборах 2017 года. Партия назвала его сообщение «позорными и неприличными» и исключила из своих рядов. Лидер «Непокорный Франции» Меланшон назвал слова Пуссье «отвратительными» и заявил, что подполковник Бельтрам погиб ради других людей.

***

26.03.2018

Крупнейшая в истории Facebook утечка отвернула людей от Цукерберга

Владельцы аккаунтов Facebook перестали доверять социальной сети, а некоторые считают ее угрозой демократическому обществу. Об этом свидетельствуют результаты опросов общественного мнения, опубликованные информационным агентством Reuters и немецким изданием Bild (InternetUA).

Согласно данным исследования Reuters/Ipsos, всего 41 процент американцев продолжают в полной мере доверять Facebook в вопросе обработки данных. Прочие опрошенные сомневаются в том, что корпорация исполняет все требования законов о защите персональной информации.

Эти показатели являются самыми низкими в рейтинге доверия юзеров IT-гигантам: к примеру, 62 процента опрошенных готовы передавать свои личные данные Google Alphabet Inc, примерно столько же – корпорации Microsoft.

Эксперты полагают, что говорить о глобальном исходе пользователей из соцсети пока рано. «Отказаться от такой платформы как Facebook психологически сложно, она плотно укоренилась в жизни людей», – прокомментировала ситуацию интернет-аналитик Дебора Уильямсон (Debra Williamson). По ее мнению, потеря доверия не всегда означает полный отказ аудитории от сервиса.

На прошлой неделе в сети был запущен флешмоб под названием deletefacebook: пользователи удаляли свои профили в социальной сети, обеспокоенные недостаточной безопасностью своих данных. Движение поддержал глава компаний Tesla и Space X Илон Маск. Акции компании на рынке упали на 14 процентов.

***

26.03.2018

Владимир Кондрашов

Документы украинского производителя оружия обнаружены в открытом доступе

Украинский хактивист, известный как Dmitry Orlov, обнаружил в открытом доступе чертежи и документы, используемые украинским заводом «Маяк» для производства оружия. Информацию об этом в рамках акции #FuckResponsibleDisclosure опубликовал на своей странице в Facebook спикер Украинского кибералья́нса, известный под ником Sean Brian Townsend.

Докладніше

***

26.03.2018

«Квітни, а не хворій»: черкаські посадовці долучились до Всеукраїнського флешмобу

До Всесвітнього дня боротьби проти туберкульозу черкаські посадовці долучилися до Всеукраїнського флешмобу «Квітни, а не хворій. #ЗупинимоТуберкульоз». Із букетом білих ромашок, які є символом чистих легень та боротьби із туберкульозом, сфотографувалися заступники голови ЧОДА – Віталій Коваль та Сергій Овчаренко та представники медичної сфери – Олег Стадник, директор департаменту охорони здоров’я та медичних послуг Черкаської міської ради. Віктор Пармонов, голова постійної комісії з питань

охорони здоров'я Черкаської обласної ради директор департаменту охорони здоров'я та медичних послуг Черкаської міської ради, Дар'я Левандовська, головний позаштатний фтизіатр Управління здоров'я ЧОДА, Петро Левченко, головний лікар КЗ «Черкаський обласний центр профілактики та боротьби зі СНІДом». Метою заходу було привернути увагу до проблеми туберкульозу та вчасної діагностики (Прочерк).

Акція відбувається у межах Проекту, який впроваджується БО «Світло надії» за підтримки БО «Всеукраїнська мережа ЛЖВ» та направлений на підтримку та інституційний розвиток ТБ спільноти.

***

27.03.2018

#ямachallenge: Укравтодор разозлился на запущенный в соцсетях флешмоб

«Укравтодор» отреагировал на запущенный шеф-редактором «Обозревателя» Орестом Сохаром и внефракционным нардепом Бориславом Березой флешмоб #ямachallenge, призванный привлечь внимание чиновников к плохому состоянию дорог в Киеве.

Докладніше

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

14.03.2018

Google запретит рекламу криптовалют и ICO

Запрет вступит в силу в июне, отмечает Bloomberg. Ранее такой же шаг предприняла Facebook Inc в январе. После заявления Google цена биткойна упала на 2 %. Интернет-гигант также ограничил рекламу для финансовых продуктов, включая бинарный опцион. В настоящее время запросы с терминами «бинарный опцион» и «купить биткойн» выдает четыре рекламы в топе результатов. После запрета Facebook в январе некоторые компании нашли лазейку и специально делали опечатки в слове «биткойн» в рекламе. Представитель Google отметил, что политика компании постарается просчитать такие обходные пути. Одновременно компания выпустила ежегодный отчет о «плохой рекламе» (Marketing Media Review).

***

14.03.2018

Создатель интернета призвал к революции

Создатель интернета Тим Бернерс-Ли опубликовал открытое письмо, приуроченное к двадцать девятой годовщине появления интернета. По его словам, развитию технологий мешают крупные компании. Они противятся принципиальным изменениям и уничтожают небольшие независимые сайты и сервисы, подобные тем, на которых раньше держался интернет.

Докладніше

***

19.03.2018

Twitter запретит рекламу криптовалют

Twitter намеревается также ввести запрет на рекламу криптовалют и ICO на своей платформе. Об этом сообщает Sky News со ссылкой на свои источники (InternetUA).

По данным телеканала, новая рекламная политика сервиса микроблогов вступит в силу в течение двух недель. Запрет на рекламу криптовалют в Twitter будет действовать во всех странах.

Ранее аналогичный запрет ввели Facebook и Google. Крупные технологические площадки опасаются, что за рекламой криптовалют и ICO могут стоять мошенники, которые намереваются обмануть пользователей.

***

19.03.2018

Knorr предлагает пользователям рецепты исходя из их ленты в Instagram

Производитель приправ и соусов анализирует данные пользователей в Instagram и предлагает им персонализированные рецепты. Если вы проводите отпуск в Греции или прогуливаетесь по Латинской Америке, либо заходите в определенные рестораны, Eat Your Feed предоставит персонализированные рецепты, под стать этим впечатлениям. К примеру, фото из заснеженных Альп может вдохновить бренд на грибное рагу с фузилли и шпинатом. Лондонское digital-агентство AnalogFolk использовали визуальное распознание и данные изображения пользователей для создания AI-алгоритма, чтобы он подбирал идеальные рецепты для постов. Пользователи могут сохранить рецепты и добавить ингредиенты в покупательскую корзину. В рамках кампании бренд откроет pop-up ресторан на один день в Лондоне, где гостям предложат блюда в соответствии с их лентой в Instagram (Marketing Media Review).

***

20.03.2018

Snapchat заработает в Британии больше, чем вся журнальная индустрия

Мобильное приложение обмена сообщениями настолько популярно в Великобритании, что его доходы от рекламы в 2019 году превысят доходы Twitter, а также журнальной индустрии и рекламы в кинотеатрах (Телекритика).

Согласно прогнозам, доход от рекламы в британском сегменте Snapchat в 2019 году составит 181,7 миллиона фунтов ($254,38 млн), а это около десяти процентов от глобальных доходов мессенджера. В 2016-м эта цифра была существенно скромнее: 21,9 миллиона фунтов ($30,66 миллиона).

По прогнозу экспертов, британские рекламные доходы Twitter в 2019 году должны быть в районе 171 миллиона фунтов ($239,4 миллиона).

К 2020 году рекламные доходы Snapchat должны вырости до 310 миллионов фунтов ($434 миллиона), и это будет больше, чем доходы потребительских журналов, как в печатном формате, так и в «цифре».

***

20.03.2018

Цукерберг потерял $5 млрд из-за утечек в Facebook

Основатель Facebook Марк Цукерберг потерял $5 млрд на фоне новостей об утечке данных пользователей соцсети. Об этом сообщает Forbes (InternetUA).

Отмечается, что в ходе торгов 19 марта стоимость акций компании упала на $37 млрд. Цукербергу принадлежит 16 % акций Facebook. В настоящее время его состояние насчитывает $69,6 млрд.

Заместитель главного юридического консультанта Facebook Пол Грюэл назвал произошедшее «надувательством и мошенничеством».

«Мы предпримем любые действия, необходимые для того, чтобы убедиться, что данные, о которых идет речь, были удалены раз и навсегда», – заявил он.

***

21.03.2018

Viber приглашает стартапы принять участие в акселераторе Techstars

Viber приглашает стартапы принять участие в новой международной программе развития бизнеса от Rakuten и Techstars. Данная кураторская программа продолжительностью 3 месяца будет проводиться в Сингапуре. Основной целью является представление инновационных идей по обмену сообщениями, а также поддержка связи между представителями бизнеса и пользователями (Marketing Media Review).

В ходе программы будут изучены все основные функции приложений для общения: обмен сообщениями, покупки, платежи, AR и VR, техническая оптимизация, маркетинг и аналитика. Из всех претендентов будут отобраны 10 стартапов, их представители отправятся в Сингапур.

Кураторы-представители из всех подразделений Rakuten, включая Viber, смогут поработать с отобранными стартапами в формате тесного сотрудничества.

***

21.03.2018
Facebook начинает брать деньги с пользователей

Социальная сеть Facebook в апреле начнет тестировать сервис платных подписок для пользователей, которые хотят поддержать денежной суммой любимых видеоблогеров. Стоимость подписки составит пять долларов в месяц, сообщает Re/code (InternetUA).

Пользователи, оформившие подписку, получат доступ к видеоконтенту, а также специальный значок, который смогут разместить на своей странице.

Авторы видео будут получать около трех с половиной долларов от каждого подписчика, остальную сумму поделят между собой Apple и Google (оплачивать подписку можно будет в мобильных приложениях для iOS и Android).

В Facebook рассчитывают на то, что отсутствие комиссии позволит удержать авторов видео, которые могут перейти на другие платформы, такие как YouTube, полагает Re/code.

***

23.03.2018
YouTube – самое прибыльное приложения в американском App Store

Аналитическая компания Sensor Tower сообщает о том, что приложение YouTube для iOS впервые за все время ведения подобной статистики стало самым прибыльным бесплатным приложением в американском сегменте App Store (IGate).

Ранее YouTube поднимался в этом рейтинге максимум на третье место. Америка стала первой страной, в которой YouTube возглавил рейтинг самых прибыльных бесплатных приложений App Store.

Сервис YouTube стал активно набирать обороты в данном рейтинге после запуска платной подписки YouTube Red, которая дает доступ к музыке и других роликам без рекламы, а также к эксклюзивному контенту. Подписка стоит $9,99 в месяц.

В феврале 2018 году приложение YouTube для iOS только в США принесло создателям 14 млн долларов, на 133 % больше чем годом ранее. В марте приложение уже заработало 12 млн долларов, на 150 % больше, чем в марте 2017.

Эта сумма включает доход только от YouTube Red и Super Chat.

***

25.03.2018

Цукерберг извинился за утечку информации из профилей Facebook, выкупив рекламу в британских газетах

Основатель Facebook Марк Цукерберг извинился перед британцами за утечку личных данных из профилей соцсети, выкупив рекламные полосы в нескольких местных изданиях, сообщает The Mirror, передает 112.ua (InternetUA).

Как отмечает издание, объявление с извинениями Цукерберга появилось на последних полосах сразу в четырех известнейших газетах, в том числе The Observer, принадлежащей The Guardian, которая одной из первых рассказала об утечке данных из Facebook.

Заявление Цукерберга во многом схоже с тем, что было им сделано несколько дней назад в интернет-пространстве. В частности, он вновь признал, что в 2014 году стороннее приложение смогло собрать данные 50 миллионов пользователей, которые затем были использованы для исследования аудитории.

«Это было нарушением доверия, и я сожалею, что в то время мы не сделали больше», – отметил он.

При этом Цукерберг добавил, что на соцсети лежит ответственность по защите личной информации пользователей, поэтому компания будет стараться в дальнейшем его оправдывать.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

15.03.2018

YouTube заборонив своїм модераторам працювати більше 4-х годин на добу

Обмеження торкнулося співробітників, що працюють з фільтрацією підозрілого контенту. На такий крок компанія пішла через турботу про психічне здоров'я модераторів (Espreso.tv).

З відповідною заявою виступила CEO сервісу – Сьюзен Войжітскі, передає The Verge. Вона додала, що навіть 4 години на день багато для такої роботи.

«Це справжня проблема, я сама витратила безліч часу на перегляд цього контенту в минулому році. Це дуже складно», – сказала вона.

Федеральні закони вимагають від технологічний компаній використовувати подвійну модерацію контенту, що включає в себе автоматичні і людські перевірки.

З нещодавніх пір YouTube почала використовувати систему Content ID, яка займається виявленням і усуненням прямих порушень, пов'язаних із захищеним авторським правом, телебаченням, фільмами і музикою.

Але для роликів, на яких відображено насильство, самогубства та інші жорстокі теми сервіс використовує неповний робочий день модераторів, щоб вони змогли підтвердити наявність тривожного контенту на відеозаписах.

Сьюзен повідомила, що дана проблема може посилитися найближчим часом, так як YouTube пообіцяв найняти 10000 нових співробітників, щоб усунути недоліки своїх алгоритмів. І при цьому модератори, які працюють не повний робочий день не мають доступу до посібників з психічного здоров'я, як інші співробітники Google, що працюють повний робочий день.

***

17.03.2018

Выявлена связь между зависимостью от социальных сетей и чертами характера

Компании, управляющие социальными сетями, стремятся создать пользователям наиболее благоприятную обстановку. Исследование, выполненное в Бингамтонском Университете в Нью-Йорке, пробует выяснить как взаимное влияние определённых личностных качеств может быть связано с болезненным пристрастием к социальным сетям.

Докладніше

***

25.03.2018

У школах США штучний інтелект виявляє небезпечних учнів через соцмережі // Програмне забезпечення використовує 450 тисяч різних індикаторів, які вказують на те, що учень може завдати шкоди собі чи оточуючим

Вища техшкола Шошин Веллі (Shawsheen Valley Technical High School) в місті Біллеріка штат Массачусетс запровадила стеження за учнями в соцмережах за допомогою штучного інтелекту, щоб виявляти тих, хто може бути небезпечним для себе і суспільства. Заклад став одним з багатьох шкіл, що почали використовувати цю технологію.

Докладніше

Маніпулятивні технології

14.03.2018

YouTube начнет добавлять к конспирологическим видео ссылки на «Википедию»

Видехостинг YouTube намерен добавлять к видео, которые продвигают конспирологические теории, ссылки на «Википедию» или другие «содержащие достоверную информацию ресурсы». Об этом объявила на конференции South by Southwest (SXSW) в Остине, штат Техас, глава видеосервиса Сьюзен Войжитски, сообщает CNBC (Зеркало недели. Украина).

На такой шаг видеохостинг решился после того, как подвергся критике за то, что в списке рекомендаций и автоматическом списке воспроизведения начали появляться видео, продвигающие теорию заговора, и другой подобный контент.

С помощью ссылок на «Википедию» и другие ресурсы, на которых, предположительно, содержится достоверная информация о событии, YouTube намерен бороться с дезинформацией. По словам Войжитски, ссылки будут сопровождать только самые резонансные конспирологические видео, например, о высадке американцев на Луну.

Вместе с тем, отмечается, что статьи в «Википедии» редактируются множеством авторов, поэтому никто не может гарантировать достоверности размещаемой на ресурсе информации.

***

14.03.2018

В 2020 году нами будут манипулировать при помощи видео, созданных ИИ

Фейковые видеоролики, разработанные технологией Deepfakes, создаются на основе машинного обучения. На протяжении нескольких лет она применялась лишь в лабораториях, но недавно стала доступной для широкой публики. Журналисты британского издания Daily Mail утверждают, что добром это не кончится (Телекритика).

По сути, простое в использовании приложение можно скачать и установить на любой ПК, а затем создавать фейковые видео в любом количестве.

В 2017 пользователь Reddit опубликовал несколько порнофильмов, в которых «засветились» фейковые версии актрис Эммы Уотсон, Дейзи Ридли и Кэти Пэрри. Администрации Reddit, Pornhub и Twitter пытаются остановить этот тренд, но настойчивые юзеры не сдаются. Теперь в поле зрения новоиспеченных монтажеров попали политики.

«Идея о том, что кто-то может наложить лицо одного человека на тело другого, сразу наводит на мысль о попытках вмешаться в естественный ход

жизни, – говорит сенатор от штата Вирджиния Марк Уорнер, возглавивший группу по борьбе с Deepfakes в социальных сетях. – Это новая реальность, с которой нужно бороться, потому что в противном случае к 2020 году последствия могут стать необратимыми».

***

21.03.2018

Цукерберга пригласили в Европарламент в связи со скандалом вокруг Facebook

Основатель социальной сети должен гарантировать, что данные пользователей не использовались для манипуляций (InternetUA).

Европейский парламент пригласил основателя социальной сети Facebook Марка Цукерберга отчитаться перед парламентариями по поводу скандала вокруг утечки данных пользователей, сообщил президент Европарламента Антонио Таяни на своей странице в Twitter.

«Мы пригласили Марка Цукерберга в Европейский парламент. Facebook должен засвидетельствовать перед представителями 500 миллионов европейцев, что личные данные не были использованы для манипулирования демократией», – говорится в сообщении.

***

21.03.2018

Facebook предупредил мексиканцев относительно фейковых новостей

После того как компания навлекла на себя критику за роль в президентских выборах в США в 2016 году, социальная сеть предприняла шаги по предотвращению фейковых новостей во время президентской кампании в Мексике, сообщает Bloomberg. Facebook разместил полностраничную рекламу в ряде крупных изданий, включая El Financiero, под тэглайном: «Советы по определению фейковых новостей». Лого сети разместили в верхнем левом углу объявления. В реклама компания назвала 10 советов, такие как «Не верьте заголовкам», «Проверяйте источник» и «Тщательно проверяйте ссылку». Внизу на испанском оставлено сообщение: «Вместе мы можем ограничить распространение фейковых новостей». По словам Facebook, реклама призвана улучшить digital грамотность и является частью инициативы по борьбе с распространением фейковых новостей и дезинформации. Мексиканцы проголосуют за президента 1 июля (Marketing Media Review).

***

25.03.2018

Google научит детей отличать фейковые новости от настоящих

Компания Google в течение ближайших двух лет намерена вложить 10 миллионов долларов в поддержку медиаграмотности. В частности, компания, владеющая видеохостингом YouTube, будет сотрудничать с детскими образовательными каналами, которым предстоит научить юных пользователей распознавать фейковые новости и отличать их от реальных фактов. Об этом плане Google пишет издание Polygon. В новом проекте примут участие крупные каналы asapSCIENCE и Smarter Every Day, число подписчиков которых составляет 7 и 5,5 млн соответственно. Первые ролики в рамках проекта планируется выпустить в ближайшие месяцы, а при желании к программе сервиса могут присоединиться и другие каналы, посвященные образованию и новостям (InternetUA).

Одной из причин создания программы стал ролик о школьнике, выжившем во время стрельбы во Флориде, пишет TJ. Многие пользователи назвали видео постановочным, а самого юношу сочли актером. Ролик попал в тренды YouTube, и сервису пришлось удалить его вручную.

***

26.03.2018

Украинцы могут не бояться манипуляций с Facebook перед президентскими выборами

Возможно ли использование социальной сети Facebook для манипуляций с общественным мнением накануне украинских президентских выборов-2019? В этом вопросе попытались разобраться ведущие «Громадського радіо» вместе с экспертом по информационной безопасности Николаем Костиняном. И пришли к однозначному выводу: в украинском обществе Facebook не играет столь крупной роли, как в американском (Телекритика).

«Это в Америке все в Facebook. У нас же аудитория была разделена, – заявил Николай Костинян в студии «Громадського радіо». – Кто-то пользовался “ВКонтакте”, кто-то “Одноклассниками”. И после блокировки этих соцсетей не все пользователи перешли в Facebook. У нас не весь электорат сидит в Facebook. И настолько манипулировать, чтобы благодаря приложению кто-то условный выиграл выборы, нельзя».

По словам эксперта, Facebook еще в 2014 году ограничил возможности приложений, и собрать сколь-нибудь большой массив информации о пользователе попросту невозможно.

О создании украинской социальной сети эксперт высказался категорично.

«Технически создать новую платформу можно без проблем, – сказал Костинян. – Самая большая проблема в общности, потому что миллион пользователей не перейдут на другую платформу. Для создания популярной украинской площадки вроде Facebook нет никаких предпосылок».

Спецслужби і технології «соціального контролю»

20.03.2018

СБУ заблокувала спробу популяризувати в мережі інтернет «Житомирську народну республіку»

Оперативники спецслужби встановили, що для створення необхідної «картинки» зловмисники використали реальні персональні дані мешканців Житомирщини, від імені яких зареєстрували фейкові акаунти. Через них вони дистанційно адміністрували сторінки та наповнювали їх антиукраїнською інформацією (InternetUA).

Правоохоронці, зокрема, задокументували, що російські пропагандисти використали особисту інформацію та світлини мешканки одного з райцентрів області для створення спільноти так званої «Житомирської народної республіки». Цей ресурс також використовувався для поширення проросійської пропаганди, підтримки та популяризації терористичних організацій «Д/ЛНР». Жінка навіть не підозрювала про свою «причетність» до створення антиукраїнської сторінки.

Співробітники СБ України також встановили, що більшість облікових записів, з яких підтримували «лайками» антиукраїнські пости, мають явні ознаки «інтернет-ботів», лише деякі з них належать реальним користувачам соцмережі.

Служба у межах чинного законодавства вжила необхідні заходи для блокування Інтернет-спільноти фейкової «ЖНР» та припинення її інформаційного наповнення.

Служба продовжує реалізовувати комплекс заходів із протидії інформаційній агресії спецслужб РФ на шкоду інтересам нашої держави.

***

20.03.2018

Telegram проиграл суд против ФСБ

Верховный суд России отклонил иск Telegram, который просил признать незаконным приказ ФСБ предоставить ключи для расшифровки сообщений пользователей. Об этом пишет «Украинская служба Би-Би-Си» (InternetUA).

После решения суда Роскомнадзор направил Telegram сообщение о необходимости предоставить ФСБ ключи шифрования в течение 15 дней. Если требование Роскомнадзор не выполнят – это может стать поводом для начала блокировки мессенджера на территории России.

Telegram заявил о намерении подать апелляцию на решение Верховного суда.

***

21.03.2018

Власти США проверят Facebook после утечки данных пользователей

Федеральная торговая комиссия США начала проверку Facebook на предмет того, не нарушила ли социальная сеть правила использования персональных данных. Об этом сообщает Bloomberg со ссылкой на источник (InternetUA).

По словам источника, комиссия проверит, давала ли соцсеть компании Cambridge Analytica доступ к личной информации своих пользователей, нарушив соглашение.

***

21.03.2018

Роман Черный

Почему Telegram – самый бескомпромиссный мессенджер современности

Роскомнадзор в очередной раз потребовал от Дурова, чтобы тот предоставлял ФСБ ключи, позволяющие читать частную переписку пользователей Telegram. Дуров же в очередной раз отказался. По его словам, он не намерен ставить под удар неприкосновенность переписки. Да и не смог бы, даже если бы захотел – шифрование обойти не может даже создатель мессенджера.

Докладніше

***

21.03.2018

Google передаст данные о перемещениях своих пользователей полиции

Полицейское управление по городу Роли, Северная Каролина, при участии Google приступило к испытаниям инновационной техники поиска подозреваемых в совершении преступлений. В рамках новой инициативы тестируется возможность использования учетных записей Google для обнаружения всех людей, находившихся вблизи места преступления до, в и после момента его совершения (InternetUA).

Новая техника выявления подозреваемых использовалась полицией Северной Каролины при расследовании как минимум четырех преступлений, совершенных за последний год. Одно из них было раскрыто именно благодаря содействию Google. Единственная причина, почему правоохранители не применяют систему чаще, является необходимость получения санкции, которую вправе выдать только суд.

По своей сути система поиска подозреваемых, которую в англоязычных СМИ почему-то называют инновационной, существует достаточно давно.

Чтобы убедиться в этом, запустите приложение «Google Карты», перейдите в контекстное меню и откройте вкладку «Хронология». Там вы сможете увидеть данные обо всех своих перемещениях по миру за любую дату с момента регистрации учетной записи.

***

23.03.2018
Владимир Кондрашов
СБУ обнаружила в Киеве группу прокремлёвских хакеров

Служба безопасности Украины заявляет о том, что ей удалось блокировать в Киеве офис прокремлёвских хакеров (InternetUA).

Как сообщается, сотрудники Службы безопасности Украины совместно с Генпрокуратурой установили, что подконтрольная ФСБ хакерская группировка организовывала кибератаки, в частности на объекты критической инфраструктуры, государственные и банковские учреждения. Для сокрытия идентификации об атаках злоумышленники использовали сервисы анонимизации сообщений.

– Сотрудники СБ Украины также задокументировали, что злоумышленники по указанию российских спецслужб задействовали так называемые «бот-фермы» для проведения специальных информационных операций против нашей страны, – говорится в сообщении СБУ.

Во время обысков в офисе и по месту жительства фигурантов дела, правоохранители обнаружили программно-аппаратные комплексы, серверное оборудование, компьютерную технику и более пятидесяти тысяч карточек мобильных операторов разных стран, задействованные в хакерских атаках.

Продолжается досудебное расследование в рамках уголовного производства, открытого по ст. 361 Уголовного кодекса Украины.

***

27.03.2018
В ЕС дали Facebook две недели на разъяснение скандала с утечкой данных

Еврокомиссия потребовала от соцсети Facebook ответов относительно скандала с утечкой персональных данных пользователей (InternetUA).

Об этом говорится в письме еврокомиссара по вопросам правосудия Веры Юровой к главному операционному директору Facebook Шерил Сандберг, сообщает Reuters.

Юрова пояснила, что предыдущие заявления руководителей Facebook относительно скандала не смягчили ее беспокойство.

«Это особенно разочаровывает, учитывая наши усилия по построению отношений, основанных на доверии с вами и вашими коллегами ... теперь это доверие уменьшилось», – заявила еврокомиссар.

В письме Юрова интересуется, захватил ли недавний скандал любые данные граждан ЕС. Если да, намерен Facebook информировать об этом власти стран Евросоюза и ее граждан.

Еврокомиссар также спрашивает, может ли социальная сеть Facebook быть уверенной, что такая ситуация больше не повторится. Юрова хочет услышать ответы на свои вопросы в течение двух недель.

***

27.03.2018

Viber, как и Telegram, может быть заблокирован в России

Мессенджер Viber может ждать блокировка на территории России по тем же основаниям, что и Telegram. Это следует из заявления операционного директора компании Viber Media S.a.r.I. Майкла Шмилова РБК. По его словам, руководство сервиса при всем желании не сможет предоставить властям ключи для дешифровки сообщений из-за отсутствия технической возможности (Центр информационной безопасности).

Несмотря на то что в распоряжении компании действительно отсутствуют ключи шифрования, в Viber считают, что сотрудничество с властями пойдет на пользу обеим сторонам. «Разыскать спамеров, задержать злоумышленников, которые используют подобные нашей платформы для нелегальной активности и т. д. Работать с [властями] для нас обязательно», – говорит Шмилов.

При этом дать спецслужбам то, чего просто не существует, нельзя, уточняет топ-менеджер. В данном случае речь идет о ключах шифрования, которые хранятся исключительно на устройствах клиентов Viber и невидимы для руководства сервиса. В теории, говорит Шмилов, можно попросить ключи у самих пользователей, но такая перспектива едва ли устроит сотрудников правоохранительных органов.

Проблема захисту даних. DDOS та вірусні атаки

14.03.2018

Fujitsu предложила технологию обнаружения уязвимостей в блокчейн-системах

Компания Fujitsu объявила о создании технологии, которая в проактивном режиме способна обнаруживать уязвимости в смарт-контрактах, а также в программах, выполняющих транзакции на основе блокчейн-платформ. Новая разработка автоматически определяет подозрительные места в исходном коде смарт-контракта.

Докладніше

***

14.03.2018

Сотрудники «Лаборатории Касперского» нашли неубиваемый компьютерный вирус

Вирусное ПО получило название Slingshot и используется для точечной слежки за пользователями. Вирус может сохранять нажатия клавиш, отправлять скриншоты, перехватывать трафик, пароли и все данные до того, как они будут зашифрованы.

Докладніше

***

14.03.2018

Уязвимости В SecurMail позволяют читать чужие сообщения

Пользователям почтового сервиса SecurEnvoy SecurMail настоятельно рекомендуется установить последнее обновление, в противном случае злоумышленники могут расшифровать их зашифрованные электронные письма. Как сообщают исследователи из SEC Consult, сервис подвержен ряду уязвимостей, из-за которых он не выполняет обещанные функции по защите конфиденциальности (Центр информационной безопасности).

В общей сложности исследователи обнаружили в SecurMail семь уязвимостей, в том числе уязвимость обхода каталога и небезопасные прямые ссылки на объект, позволяющие одним получателям читать электронные письма, отправленные другим получателям. Еще одна уязвимость связана с отсутствием механизмов аутентификации и авторизации и позволяет злоумышленникам перехватывать или модифицировать хранящиеся на сервере электронные письма, а также переписывать или удалять письма в папке «Входящие».

Исследователи обнаружили уязвимости за короткий промежуток времени и допускают возможность существования и других проблем с безопасностью, ускользнувших от их взгляда. Уязвимости были обнаружены во время проведения небольшого краш-теста, и эксперты рекомендуют воздержаться от использования сервиса до тех пор, пока не будет проведен комплексный аудит безопасности и приняты соответствующие меры. Если отказаться от использования сервиса не представляется возможным, рекомендуется установить патч 1_012018 для семи уязвимостей, обнаруженных SEC Consult, или обновиться до версии 9.2.501.

***

14.03.2018

Взломавшие CCleaner хакеры готовили третий этап вредоносной кампании

Исследователи компании Avast сообщили новые сведения о нашумевшем прошлогоднем инциденте с CCleaner. Согласно представленному на конференции SAS в Мексике докладу, хакеры, атаковавшие инфраструктуру CCleaner и внедрившие в утилиту бэкдор, готовились к заражению инфицированных компьютеров третьим вариантом вредоносного ПО, сообщает Bleeping Computer.

Докладніше

***

14.03.2018

Найден способ взломать компьютер через наушники

Исследовательская группа из университета имени Давида Бен-Гуриона в Негеве (Израиль) провела эксперимент по захвату данных с помощью наушников и динамиков компьютера. О новом методе сообщило издание Bleeping Computer.

Докладніше

***

14.03.2018

Хакеры научили роботов показывать порно и вымогать биткоины

Мошенники давно используют вредоносное ПО для вымогательства денег – файлы на электронном устройстве шифруются, а за возможность вернуть доступ к ним нужно заплатить (однако оплата не является гарантией). Как выяснили специалисты из компании IOActive, под ударом оказываются не только компьютеры или смартфоны – новой целью могут стать роботы.

Докладніше

***

14.03.2018

Украинский метеоцентр майнит криптовалюту на официальном сайте

Скрытый майнинг с помощью сервиса CoinHive стал настолько распространенным, что добрался уже и до государственных сайтов (InternetUA).

JavaScript-майнер, который можно установить в код сайта, чтобы добывать криптовалюту незаметно для посетителей, был обнаружен на сайте Украинского Гидрометцентра.

Примечательно, что его существование никаким образом не скрывается, скрипт установлен в самом начале HTML-кода и не спрятан в других файлах, не обфусцирован и не маскируется другими методами.

Возможно, сайт стал жертвой взломщиков, как, например, сайты государственных органов Великобритании и Австралии, но есть и вероятность того, что скрытым майнингом занимаются технические специалисты Украинского Гидрометцентра.

Скрипты для скрытого майнинга определяются большинством антивирусных программ, как вредоносные. Их работа в браузере может приводить к 100 % загруженности компьютера и его зависанию, что чревато потерей данных и другими неприятными последствиями.

С октября 2017 года скрипт CoinHive занимает 6 место в списке самых распространенных вредоносных программ.

***

14.03.2018

Вредонос Slingshot занимается кибершпионажем как минимум с 2012 г.

Исследователи «Лаборатории Касперского» обнаружили сложную киберугрозу, которая используется для шпионажа в странах Ближнего Востока и Африки по меньшей мере с 2012 г. Вредоносное ПО получило название Slingshot.

Докладніше

***

18.03.2018

Сайт ЦИК России подвергся атакам хакеров

Сайт Центральной избирательной комиссии России в день выборов президента подвергся хакерской атаке из 15 стран. Об этом сообщила председатель ЦИК Элла Памфилова, передает ТАСС (InternetUA).

«18 марта у нас с двух до пяти часов ночи была отражена компьютерная атака на сайт, типа “отказ на обслуживание”. Пик атаки пришелся на 02:20 по московскому времени. Источники атаки были расположены в 15 странах», – сказала она.

***

18.03.2018

Как защитить аккаунт в соцсетях от собственного любопытства

Кем ты был в прошлой жизни? Что о тебе говорит твоя аватарка? Как ты записан в телефоне у своих друзей? Эти вопросы выманивают персональные данные, которые мы зачастую бездумно дарим мошенникам.

Докладніше

***

19.03.2018

Facebook уличили в сливе данных 50 миллионов пользователей

Социальная сеть Facebook проводит собственное расследование относительно связи своих сотрудников со сторонней компанией, которая завладела данными 50 миллионов пользователей. Предполагается, что они использовали личную информацию юзеров для поддержки штаба нынешнего президента США Дональда Трампа.

Докладніше

***

19.03.2018

На телефонах с Android найден вирус, ворующий деньги через телефонные звонки

Специалисты в области кибербезопасности обнаружили обновленный вариант опасного программного обеспечения FakeBank, которое способно перехватывать телефонные звонки жертв. Об этом сообщается в отчете компании Symantec (InternetUA).

Новая конфигурация вредного ПО переключает телефонные звонки пользователей по номерам банков на мошенников. Злоумышленники собирают информацию о финансах жертвы и далее используют ее по своему усмотрению. При этом FakeBank может внедряться в смартфон жертвы и, анализируя данные о банковских приложениях пользователя, совершать любые операции под видом финансовой организации.

Более ранние модификации вредного ПО подделывали изображения входа в мобильное приложение той или иной организации. Помимо этого, FakeBank мог сохранять дееспособность даже на неактивном гаджете. Эту Android-угрозу не раз называли самой «креативной» на рынке вирусов.

Согласно наблюдениям экспертов, пока обновленный вариант трояна активен только на территории азиатского региона. Он распространяется через сторонние магазины приложений и ссылки в социальных сетях.

***

19.03.2018

Теория заговора или обычная паранойя: не прослушивает ли нас Facebook?

Среди пользователей Facebook и Instagram ходит теория о том, что их телефоны прослушиваются, и рекламодатели знают, что говорят их владельцы.

Докладніше

***

19.03.2018

Avast обнаружила скрытый майнер в нескольких приложениях из Google Play

Исследователи Avast обнаружили скрытые вредоносные программы в составе нескольких приложений из каталога Google Play. Еще в ноябре 2017 г. специалисты компании начали обнаруживать штампы вредоносной программы, известной как JSMiner, в Google Play. Возможности майнить криптовалюту Monero были обнаружены внутри игрового приложения Cooee. На этой неделе найдены еще два приложения для добычи криптовалюты в Google Play: SP Browser и Mr. MineRusher с совокупной абонентской базой в тысячи пользователей (Компьютерное Обозрение).

Подобно кампании в конце прошлого года, процесс мобильного майнинга начинается, как только пользователь загружает приложение и открывает его. При этом происходит автоматическое соединение с веб-сайтом apptrackers.org, где размещается майнер CoinHive Java Script для Monero. Как только соединение с доменом будет выполнено, начинается процесс майнинга. Вредонос делает это незаметно в фоновом режиме, когда экран выключен, и устройство подключено к мобильному Интернету или Wi-Fi.

Хорошей новостью для пользователей этих приложений является то, что они вряд ли вызовут проблемы с безопасностью или конфиденциальностью. При этом для хакеров вознаграждение за их усилия невелико, так как майнинг на мобильных устройствах практически не приносит прибыли из-за их относительно невысокой вычислительной мощности.

***

18.03.2018

Ваш смартфон постоянно слушает и смотрит в камеру на вас – даже когда выключен

Эксперт в сфере информационных технологий, искусственного интеллекта и ИТ-безопасности Игорь Ашманов посоветовал заклеивать камеры смартфонов и планшетов. В интервью «АиФ» специалист рассказал, как спецслужбы следят через смартфон, почему опасно проходить тесты в соцсетях, а также поделился мыслями о безопасности мессенджеров.

Докладніше

***

18.03.2018

Google избавилась от 3,2 млрд вредоносных рекламных объявлений в 2017 году

Google рассказала, что в 2017 году удалила 3,2 млрд так называемых плохих рекламных объявлений – в 2016 году компании удалось избавиться от 1,7 млрд таких объявлений, что на 88 % меньше. Таким образом, в прошлом году калифорнийский гигант избавлялся от 100 единиц вредоносной рекламы в секунду (InternetUA).

Плохая реклама – любые объявления, которые нарушают правила Google. Это могут быть мошеннические, фишинговые и вредоносные сообщения. Компания говорит, что большинство таких объявлений она блокирует ещё до того, как злоумышленникам удаётся осуществить свой замысел. Google удалила из своей рекламной сети за нарушения 320 тысяч издателей, а также добавила в чёрный список примерно 90 тысяч сайтов и 700 тысяч мобильных приложений.

Google добавила, что каждый месяц в 2017 году удаляла за нарушение правил 2 млн интернет-страниц. Этого удалось достичь отчасти благодаря новой технологии, которая позволяет компании убирать рекламу с отдельных страниц сайтов-нарушителей.

За прошедший год Google добавила 28 новых правил для рекламодателей и 20 правил для издателей. В этом году компания уже успела обновить ряд политик, связанных с бинарными опционами, криптовалютами, зарубежными валютными биржами и контрактами на разницу цен. Издателям-партнёрам Google выплатила за 2017 год $12,6 млрд.

***

19.03.2018

Уязвимость в функции «мастер-пароль» в течение 9 лет ставит под угрозу пользователей Mozilla

На протяжении последних девяти лет Mozilla использовала в своей функции «мастер-пароль» недостаточно надежное шифрование.

Докладніше

***

19.03.2018

Новый вирус крадет деньги через телефонные звонки

Вирус распространяется в соцсетях и сторонних магазинах приложений (U-News). Вирус способен работать только на операционке Android, а распространяется он посредством социальных сетей и сторонних магазинов приложений.

Специалисты считают, что FakeBank обладает возможностью внедрения в смартфоны. Также вирус анализирует сведения о банковских приложениях и совершает любые операции под видом кредитного учреждения.

Однако пока деятельность вредоносного софта распространяется исключительно в среднеазиатском регионе.

Помимо этого, в начале марта 2018 года пользователи услышали о новом вирусе, атакующем их девайсы на Android. Это программа RedDrop, похищающая аудиофайлы и размещающая их в Сети в облачных хранилищах. Также вирус подписывает владельцев смартфонов на SMS-сервисы с премиальным доступом.

При этом вирусная программа скрывает все признаки установки на гаджет и производит маскировку вредоносных приманок под разнообразные инструменты, такие как графические редакторы или калькуляторы.

Сообщается, что к настоящему моменту методов борьбы с RedDrop пока не нашли.

***

20.03.2018

Что скрывается за красочными фасадами Facebook и Google

Всем известные внешние атрибуты корпораций Кремниевой Долины: красочные велосипеды, настольный теннис, кресла-мешки и бесплатная еда – лишь рисованный фасад, за которым скрывается жесткий кодекс секретности.

Докладніше

***

19.03.2018

Атаки вымогателей становятся все более разрушительными и направлены в основном на бизнес-сегмент

Microsoft выпустила глобальный отчет по информационной безопасности Microsoft Security Intelligence Report volume 23. Свежий выпуск включает данные, собранные с февраля 2017 г по январь 2018 г. Эксперты проанализировали миллиарды анонимных сигналов об угрозах безопасности сервисов и продуктов Microsoft, включая Windows, Bing, Office 365 и Azure.

Докладніше

***

19.03.2018

Как отличить бота от человека?

Интернет превратился в огромную коммуналку, где с одного адреса может писать и человек, и бот, мечтающий заразить сервис. Решение проблемы – сервис IPv6, но он имеет свои недостатки.

Докладніше

***

19.03.2018

Хакерская группировка Fancy Bear провела новую шпионскую кампанию

Исследователи безопасности из компании Palo Alto Networks сообщили о новой фишинговой кампании, за которой стоит хакерская группировка Fancy Bear, предположительно связанная с властями РФ.

Докладніше

***

20.03.2018

Новый вид мошенничества: хакеры начали продавать селфи своих жертв

Согласно отчету в NextWeb, израильская компания Sixgill, занимающаяся веб-исследованиями Даркнета, обнаружила большой объем сомнительного контента, среди которого были селфи пользователей.

Докладніше

***

20.03.2018

Как Facebook отреагировал на скандал с утечкой данных

Facebook поделился первой реакцией на скандал с утечкой данных, согласно которому лондонская аналитическая компания Cambridge Analytica, которая работала над избирательной кампанией Трампа и кампанией «Брекзит», анализировала и хранила данные о 50 млн американских пользователях сети. Вице-президент по маркетингу Кэролин Эверсон признала, что была «разгневана и встревожена» отчетами, выступая на конференции по ритейлу ShopTalk. «Если подозрения верны, это невероятное нарушение всего, что мы отстаиваем», – добавила она. Эверсон первой из топ-руководителей Facebook ответила на вопросы относительно подозрений, что Cambridge Analytica никогда не удалял нелегально полученные данные о пользователях, которые он получал от российско-американского исследователя в 2015 году. Тем временем медиа и пользователи раскритиковали Facebook за небрежность по отношению к защите данных и за то, что топ-менеджера не прокомментировали ситуацию публично. Глава безопасности Алекс Стамос предварительно разметил серию твитов о том, что инцидент нельзя считать «взломом данных» и затем удалил их. Отметим, в связи со скандалом акции компании упали на 8 % (Marketing Media Review).

***

20.03.2018

Беззащитные данные: как Facebook оказалась в центре самого большого скандала в истории

Cambridge Analytica придумывала, как высасывать из пользователей Facebook максимальное количество информации: она делала всевозможные веселые приложения и тесты, а потом составляла профили, помогающие манипулировать людьми.

Докладніше

***

20.03.2018

В 2017 году ИИ помог выявить 60,3 % вредоносных Android-приложений

На днях Google обнародовала отчёт о безопасности Android за 2017 год в рамках своих постоянных усилий по информированию пользователей о различных уровнях безопасности мобильной ОС. Одним из ключевых моментов отчёта является тот факт, что встроенные функции безопасности Android в Google Play предотвратили установку 60,3 % потенциально вредоносных приложений (PHA, Potentially Harmful Apps) (IGate).

В значительной степени выявление такого ПО осуществляется службой Google Play Protect, которая теперь включена на более чем 2 миллиардах устройств. Google Play Protect работает на Android 4.3 или выше и постоянно сканирует приложения на предмет злонамеренной активности. Служба использует преимущественно машинное обучение для повышения эффективности борьбы с установкой PHA, но также применяет множество других методов и тактик, чтобы обеспечить безопасность пользователей и их данных.

Компания также рассказала, что в рамках мер по повышению безопасности и качества ПО в 2017 году из магазина Play было удалено более 700 000 приложений за нарушение правил, что на 70 % больше, чем в 2016 году. Google упомянула также использование машинного обучения для обнаружения ПО, имитирующего популярные приложения, использующего неприемлемый контент или имеющего вредоносную направленность.

***

20.03.2018

Украинские хакеры начали вымогать выкупы в биткоинах

В Украине киберпреступления все чаще совершают при помощи самых обычных устройств. На днях полицейские в Хмельницком поймали злоумышленника, который обворовал нескольких граждан с помощью их же мобильных телефонов.

Докладніше

***

20.03.2018
Смартфоны на Android атакует новый банковский троян

Эксперты антивирусной компании Symantec узнали о существовании нового банковского трояна Fakebank, способного перехватывать сообщения и звонки банка (Украинский телекоммуникационный портал).

Таким образом, мошенники могут выдавать себя за представителей банковской организации, препятствуя установлению связи с реальной службой технической поддержки.

Попадая на устройства, троян подменяет телефонные номера банков, клиентами которых являются жертвы, чтобы иметь возможность связываться с ними от имени реально существующих организаций.

В результате на экране смартфона жертвы будет отображаться знакомый телефонный номер, за которым на самом деле скрываются злоумышленники.

По данным Symantec, троян, распространяемый посредством социальных сетей и скомпрометированных сайтов, содержится в более чем 20 приложениях.

Несмотря на то что в настоящее время злоумышленники ориентируются на рынок Южной Кореи, есть все основания полагать, что география их деятельности может быть расширена

***

21.03.2018
Ваш гаджет захватили майнеры. Что делать?

Майнеры атакуют! В последнее время они стали самым активным типом вирусов. Даже красть данные с серверов крупных корпораций сегодня не так выгодно, как скрыто майнить на этих мощностях.

Докладніше

***

22.03.2018
Мошенники научились манипулировать поисковыми подсказками

Исследователи из трех американских университетов определили, что каждая 200-я ссылка в поисковых подсказках Google связана с мошеннической активностью. «Черные SEO-шники» используют функцию автозаполнения, чтобы привлекать трафик на свои сайты, продвигать зловредное ПО и прочий вредоносный контент (Центр информационной безопасности).

В своей работе ученые применяли специальный инструмент Sacabuche (Search Autocomplete Abuse Checking – «проверка на манипулирование поисковыми подсказками»; слово также означает «ручной насос, помпа» по-испански). Объектом исследования стали 117 млн подсказок, которые Google, Yahoo! и Bing предлагают пользователю по мере ввода запроса. Вредоносный характер был выявлен у 0,48 % позиций в этом массиве.

За подменой подсказок стоит множество компаний, которые предлагают свои услуги по цене от 1 до 20 долларов в день. Одни используют ручной труд операторов, другие автоматизируют процесс с помощью набора браузеров, отправляющих запросы с разных IP-адресов. Авторы исследования описали двухступенчатый механизм атак: сначала вредоносная подсказка внедряется в список автозаполнений, потом злоумышленники продвигают свою страницу в соответствующей выдаче.

Ученые установили более 3 тыс. сайтов, появляющихся среди результатов поиска после подмены подсказки, из чего сделали вывод о работоспособности этой стратегии. По их словам, значительную роль в ее популярности сыграла растущая доля мобильных устройств в веб-трафике. Пользователи смартфонов часто кликают по подсказкам, чтобы сэкономить время и избежать опечаток.

Схема работает не только в трех поисковиках, которые вошли в исследование, но и любых других сервисах с функцией автозаполнения, в частности в Yandex и китайском Baidu. Ученые донесли информацию об уязвимости до всех этих компаний и уже получили ответ от Google, содержание которого не раскрывается.

***

21.03.2018

На украинский бизнес осуществляется новая массированная вирусная атака

Украинский бизнес предупреждают о новых волне хакерских-атак. Вирусные письма рассылаются на электронные почтовые ящики предприятий от имени Национального агентства по предупреждению коррупции (НАПК), а также Государственной фискальной службы (ГФС). Об опасности друг друга предупреждают бухгалтера украинских предприятий в тематических пабликах в соцсети Facebook (InternetUA).

От псевдо-ГФС письма приходят с темой «Обращение руководителю предприятия» о том, что компания якобы уклонялась от уплаты налогов. От липового НАПК приходит опрос с темой «Уважаемый гражданин!». Письма присылают с обратными адресами в Японии r.oodaira@nishikawa-kogu.co.jp, product@vousetes.co.jp, mrc@x-make.sky-office.jp и пр.

Также вредоносные письма могут приходить от имени Исполнительной службы или гласить о каком-то виде административного правонарушения, предупреждают пользователи.

Эксперты призывают ни в коем случае не открывать подобные письма – все они содержат вредоносные прикрепленные файлы. А в случае получения отправлений с сомнительных адресов, немедленно их удалять.

***

22.03.2018

Обнаружена связь американских военных со шпионским ПО Slingshot

На минувшей неделе SecurityLab сообщал о хакерской группировке, использующей шпионское ПО Slingshot для заражения сотен тысяч маршрутизаторов Mikrotik в странах Ближнего Востока и в Африки. Жертвами хакеров стали отдельные лица и ряд правительственных организаций в различных странах, включая Кению, Йемен, Ливию, Афганистан, Ирак, Танзанию, Иорданию, Маврикий, Сомали, Демократическую Республику Конго, Турцию, Судан и Объединенные Арабские Эмираты (Центр информационной безопасности).

Как сообщило издание CyberScoop со ссылкой на анонимный источник и бывших сотрудников разведки США, Slingshot фактически является операцией Совместного командования специальных операций США (JSOC), входящего в состав Командования специальных операций (SOCOM), против членов террористических организаций, таких как ДАИШ и «Аль-Каида» (обе запрещены в РФ). SOCOM хорошо известна своими контртеррористическими операциями, которые иногда могут включать в себя кибератаки.

Источники CyberScoop выразили обеспокоенность тем, публикация информации о кампании может привести к провалу операции и даже подвергнуть опасности жизни солдат. Инфраструктура Slingshot, вероятно, была уничтожена после раскрытия информации, предположил один из бывших сотрудников разведки.

***

22.03.2018

Шесть способов увидеть, что интернет знает о вас всё

В середине марта компания Facebook оказалась в центре скандала из-за использования личных данных пользователей без их ведома. Мы собрали несколько примеров того, как крупные сервисы открыто рассказывают о собранных персональных данных – но это все равно может вызвать тревогу.

Докладніше

***

23.03.2018

Дмитрий Демченко

В Facebook вирусятся посты с призывом оставлять комментарии BFF, чтобы проверить безопасность аккаунта. Это фейк

В последние несколько дней в Facebook появляются публикации с призывом оставить комментарий BFF якобы для того, чтобы проверить безопасность аккаунта. Это неправда – таким образом невозможно определить, достаточно ли защищен профиль (AIN.UA).

Авторы публикаций пишут, что Марк Цукерберг придумал слово BFF (в другом посте – число 28/33), которое поможет определить защищенность аккаунта. По условиям, если аббревиатура отображается зеленым – то профиль в безопасности. Если же нет, авторы призывают немедленно сменить пароль.

Дело в том, что BFF всегда будет высвечиваться зеленым, кроме тех случаев, когда слово написано со смартфона с не самой свежей версией Facebook. BFF – одно из слов, которое включает специальную анимацию. Аббревиатура расшифровывается как Best Friend Forever, «Лучшие друзья навсегда». Если нажать на нее, включится анимация ладоней, дающих друг другу «пять». Среди других таких слов – «Поздравляю», «Я люблю тебя» и так далее.

Эти слова не показывают, защищен аккаунт или нет. Они сделаны для красоты и вау-эффекта. В Facebook не существует инструмента, который поможет проверить уровень защищенности аккаунта. Чтобы обезопасить себя от возможного взлома – используйте уникальный пароль и двухфакторную аутентификацию.

***

24.03.2018

Вирус в сервисе YouTube ворует логины и пароли пользователей

Видеохостинг YouTube является крайне популярным сервисом среди жителей всех стран мира, где он не заблокирован в силу каких-то причин. Хоть компания Google и ведет постоянную работу над расширением его функциональных возможностей, однако иногда ее трудов недостаточно. Сегодня, 24 марта 2018 года, компания «Доктор Веб» объявила об обнаружении опасного вируса, который ворует личные данные всех пользователей – логины, пароли и прочие (Украинский телекоммуникационный портал).

Злоумышленники используют недостатки YouTube для того, чтобы заражать компьютеры на базе Windows опасным вредоносным ПО. Речь идет о трояне Trojan.PWS.Stealer.23012, который также иногда встречается для устройств под управлением macOS и Linux. Он, попав на компьютер, крадет всю личную информацию, которая может представлять хоть какую-то ценность. Это сохраненные логины и пароли из всех веб-браузеров, а также файлы Cookie из браузеров Chrome, Яндекс. Браузер, Opera, Vivaldi, Kometa, Orbitum, Dragon, Amigo и Torch.

Ссылки с сайта YouTube на загрузку чита ведут на «Яндекс.Диск» и другие сервисы. Чтобы еще больше убедить пользователей, злоумышленники в комментариях к файлу с различных аккаунтов пишут положительные отзывы. В итоге, жертва, сама того не зная, скачивает на свой компьютер самораспаковывающийся RAR-архив, которые содержит в себе троян.

Эксперты по безопасности рекомендуют не скачивать никакое ПО подозрительного происхождения, а если очень хочется, то использовать специальную «безопасную зону» в антивирусах, при которой файл открывается

и проверяется в ее рамках. Ранее Google благодаря YouTube установила мировой рекорд, заработав рекордную сумму денег.

***

26.03.2018
Facebook подтвердила слежку за звонками и SMS пользователей

Команда социальной сети Facebook отреагировала на обвинения в слежке за звонками и SMS пользователей Android-устройств. С одной стороны, Facebook подтвердила сбор истории звонков и сообщений, но при этом подчеркнула, что «слежка» является опциональной и ведётся исключительно с согласия самих пользователей (InternetUA).

В конце прошлой недели ресурс Ars Technica опубликовал внушительную заметку о том, что Facebook без разрешения пользователей годами собирала историю звонков и текстовых сообщений с Android-устройств, на которые установлены фирменные приложения. Теперь компания опровергла это обвинение.

Как отмечается в официальном заявлении Facebook, при авторизации в Messenger или Facebook Lite на Android-устройстве, у пользователя запрашивается разрешение на постоянную загрузку информации о контактах, а также истории звонков и текстовых сообщений. Таким образом, пользователи сами разрешают «следить» за собой, хотя мало кто обращает внимание на такие предупреждения и многие отвечают «да» просто на автомате.

Интересно, что подобная функциональность не разрешена на iOS, таким образом, пользователи iPhone не подвергаются сбору именно этих данных со стороны Facebook.

***

26.03.2018
Facebook знает о вас всё

Facebook получает 98,5 % выручки от показа рекламы, и в этом нет ничего плохого. Другое дело, что для того, чтобы показывать вам максимально подходящие объявления, Facebook лезет в вашу жизнь.

Докладніше

***

26.03.2018
Пользователям Youtube грозит новый вирус

В описаниях к видео на Youtube обнаружили вирус, который похищает из зараженного устройства файлы и персональную информацию (U-News).

Вредоносную программу назвали Trojan.PWS.Stealer.23012. Она заражает устройства под управлением Microsoft Windows.

«Чтобы убедить посетителя сайта нажать на ссылку, на страницах роликов публикуют комментарии. Их написали с поддельных аккаунтов. При попытке перейти по такой ссылке, потенциальная жертва загружает на свой компьютер самораспаковывающийся RAR-архив. Он содержит троянца», – сообщают инженеры Dr. Web.

Ролики, которые заразил вирус, посвящены использованию мошеннических методов прохождения игр с применением специальных приложений. На зараженном компьютере программы собирает файлы Cookies браузеров Vivaldi, Chrome, Opera, Kometa, Orbitum, Dragon, Amigo, Torch, сохраненные логины и пароли с этих ж браузеров. Также вирус копирует с рабочего стола Windows файлы с расширениями .txt, .pdf, .jpg, .png, .xls, .doc, .docx, .sqlite, .db, .sqlite3, .bak, .sql, .xml.

Полученную информацию Trojan.PWS.Stealer.23012 сохраняет в папке C: / PG148892HQ8. Вирус упаковывает файлы в архив spam.zip. Затем он поступает на сервер злоумышленников.

***

26.03.2018

Ирина Фоменко

Офицер российской разведки взломал сервера Национального комитета Демократической партии США

Guccifer 2.0, взломавший сервера Национального комитета Демократической партии США накануне выборов 2016 года, оказался служащим российской военной разведки. Это открытие повлечет за собой серьезные последствия для продолжающегося расследования специальным советником Робертом Мюллером вмешательства России в президентские выборы США в 2016 году. Об этом сообщает The Fortune (InternetUA).

Во время выборов в США Guccifer 2.0 представлялся как независимый румынский хакер. Предполагалось, что имя он взял в честь румынского киберпреступника, взломавшего почтовый сервер Хилари Клинтон. Guccifer 2.0 получил архивы электронной почты Национального комитета Демократической партии США, а затем обнародовал их, в том числе и в WikiLeaks. Эти электронные письма стали доказательством, как Клинтон пыталась помешать своему главному конкуренту Берни Сандерсу.

Отношение к Guccifer 2.0 изначально было весьма скептичным, поэтому разведывательные органы США сразу заявили, что взлом, вероятно, является российской операцией. Однако доказать это было сложно, поскольку хакер выходил в сеть через VPN. Согласно данным The Daily Beast, Guccifer 2.0 идентифицировали как офицера ГРУ только после того, как один раз хакеру не удалось активировать VPN.

Отметим, что Guccifer 2.0 напрямую общался с приближенными Дональда Трампа. Один из союзников Трампа и советник по кампании Роджер Стоун признал в марте, что он обменивался поздравлениями с Guccifer 2.0 в

Twitter во время выборов. Стоун переписывался с Guccifer 2.0 уже после взлома Национального комитета Демократической партии США. Агенты ФБР, которые следили за Guccifer 2.0, теперь стали частью команды Мюллера.

***

26.03.2018

Самым эффективным методом социальной инженерии оказался фишинг

Специалисты Positive Technologies собрали статистику эффективности атак с применением методов социальной инженерии.

Докладніше

***

26.03.2018

Кіберполіція викрила українського хакера, який працював на міжнародне угруповання Cobalt

Чоловік входив до міжнародного хакерського угрупування «Cobalt», члени якого причетні до масових атак на різноманітні світові банки. Наразі оперативники з кіберполіції встановили всіх учасників цього угрупування. Всі вони перебувають на території Російської Федерації (InternetUA).

Працівники Київського управління кіберполіції Департаменту кіберполіції спільно зі слідчими Голосіївського управління поліції Києва, під процесуальним керівництвом Київської міської прокуратури №1, встановили причетність 30-річного мешканця Києва до розробки вірусів, кібершпигунства та продажу персональних даних громадян з усього світу. Хакер також збував різноманітне шкідливе програмне забезпечення, а його віруси використовувалися для отримання віддаленого доступу до комп'ютерів жертв та подальшого повного контролю над ними.

Поліцейські встановили, що чоловік з 2016 року є учасником хакерського угрупування, відомого під назвою «Cobalt», члени якого причетні до масових атак на різноманітні світові банки. До його обов'язків входили розробка та підтримка належної роботи «експлойтів», які використовували вразливості у найбільш розповсюджених серед користувачів програмних продуктах.

***

26.03.2018

Депутати хочуть запровадити мільйонні штрафи за умисний спам

Народні депутати пропонують ввести зміни до законодавства України щодо протидії спаму, зокрема за умисне розповсюдження спаму штрафувати від 850 тисяч гривень до 1,7 мільйона гривень (InternetUA).

Про це йдеться у порівняльній таблиці до проекту Закону, який направили на розгляд Комітету Ради, передає Depo.ua.

Пропозиції депутатів містять визначення спаму та визначають покарання за його розповсюдження.

Умисне розповсюдження спаму, яке не призвело до порушення роботи комп'ютерів, пропонується карати штрафом від 500 до тисячі прожиткових мінімумів – тобто від 850 тисяч гривень до майже 2 млн гривень.

За організацію чи сприяння розсилки спаму пропонують штрафувати на таку ж суму.

Умисна масова розсилка спаму без попередньої згоди отримувачів, що призвела до припинення роботи комп'ютерів, каратиметься штрафом від 500 до 1000 мінімальних зарплат – це від 1,8 мільйона гривень до 3,7 млн гривень. Або можуть обмежити волі на термін до 3 років.

У законопроекті пропонується також, аби ті, хто розсилає спам, протягом 3 місяців після набуття чинності цього законопроекту, повідомили отримувачів про їхні підписки на розсилки. У цьому повідомленні мають міститися дані про те, як споживач може відмовитись від розсилки.

***

27.03.2018

В YouTube появился новый троян

Эксперты по кибербезопасности из компании Dr.Web сообщают о новейшем опасном вирусе на популярном видеохостинге YouTube. Основной целью мошенников стали компьютеры с операционной системой Microsoft Windows (Центр информационной безопасности).

Распространение вируса под названием Trojan.PWS.Stealer.23012 происходит через облачный сервис Яндекс.Диск. Мошенники оставляют под видео ссылки на скачивание приложений, которые якобы помогут взломать популярную компьютерную игру или получить виртуальную игровую валюту. Однако при открытии ссылки начинается загрузка самораспаковывающегося RAR-архива с трояном.

Как только вирус попадает на компьютер, он собирает всю личную информацию:

– пароли с браузеров, включая файлы Cookies из Vivaldi, Chrome, Яндекс.Браузер, Opera, Kometa, Orbitum, Dragon, Amigo, Torch;

– документы с Рабочего стола с расширениями ".txt", ".pdf", ".jpg", ".png", ".xls", ".doc", ".docx", ".sqlite", ".db", ".sqlite3", ".bak", ".sql", ".xml";

– данные о местоположении зараженного устройства;

– скриншот рабочего стола и т.д.

Все полученные сведения Trojan.PWS.Stealer.23012 сохраняет в папке C:/PG148892HQ8, после чего запаковывает в архив spam.zip и отправляет на сервер злоумышленников. Злоумышленники таким образом получают доступ к

конфиденциальной информации, в том числе к соцсетям и могут как украсть денежные средства со счетов, так и шантажировать владельца.

Основная мера безопасности все та же – не скачивать неизвестные файлы от малознакомых людей. В тоже время, аналитики из «Доктор Веб» заверяют, что их продукт успешно определяет вредоноса и его модификации, поэтому троянец не представляет угрозы для пользователей Dr.Web.

ДОДАТКИ

Додаток 1

26.03.2018

Владимир Кондрашов

Документы украинского производителя оружия обнаружены в открытом доступе

Украинский хактивист, известный как Dmitry Orlov, обнаружил в открытом доступе чертежи и документы, используемые украинским заводом «Маяк» для производства оружия (InternetUA).

Информацию об этом в рамках акции #FuckResponsibleDisclosure опубликовал на своей странице в Facebook спикер Украинского кибералъянса, известный под ником Sean Brian Townsend.

ПАО «Завод «Маяк» входит в государственный концерн «Укрборонпром». Согласно официальному сайту завода, основными направлениями его деятельности являются разработка и производство стрелкового оружия (снайперских винтовок, пехотных и танковых пулемётов), артиллерийского оружия, модернизация и ремонт колесной бронетехники, экспорт и импорт продукции военного и специального назначения.

– Дмитрий Орлов прислал свежую порцию «открытых данных» для вечно неунывающей рубрики #FuckResponsibleDisclosure. В этот раз попался ПАО «Завод Маяк». Там делают стрелковое оружие, завод входит в «Державний концерн «Укроборонпром». И что тут такого? Всего-то чертежи новых оборонных разработок, заказы, договора на поставку комплектующих. Листайте дальше, – написал спикер УКА. – Особого цинизма добавляет то, что «Укроборонпром» является инициатором амбициозных проектов в области безопасности – киберцентра и баг-баунти программы, которая ещё не взлетела. Хотел бы попросить господ советников уделить немного внимания собственному концерну, а то и, чем черт не шутит, потратить пару монеток. Примеры документов, обнаруженных в открытом доступе/ San Brian Townsend, Facebook

Как уточнил Sean Brian Townsend в комментарии для нашего издания, в общем доступе различные чертежи оказались благодаря открытому для всех желающих сетевому диску с данными.

В ПАО «Завод «Маяк» нашему изданию сообщили, что обнародованные хактивистами данные не являются секретными:

– Это обычная рабочая информация, никаких секретных данных там нет, – отметили в ПАО «Завод «Маяк».

В то же время ответить на вопрос, закрыта ли уязвимость на данный момент и обнаружен ли вообще источник утечки нашему журналисту не смогли, попросив предоставить письменный запрос.

Флешмоб #FuckResponsibleDisclosure – акция, инициированная Украинским кибералъянсом. Она направлена на выявление уязвимостей государственных электронных ресурсов и публичное информирование о найденном с целью обратить внимание на проблему соответствующих служб. По словам самих представителей УКА, такой подход к раскрытию информации оказался в разы эффективней классического Responsible Disclosure (ответственного раскрытия) – уязвимости во многих случаях закрывались за считанные часы.

Информация о найденных данных хактивистами передана в Службу безопасности Украины.

(вгору)

Додаток 2

27.03.2018

#ямachallenge: Укравтодор разозлился на запущенный в соцсетях флешмоб

«Укравтодор» отреагировал на запущенный шеф-редактором «Обозревателя» Орестом Сохаром и внефракционным нардепом Бориславом Березой флешмоб #ямachallenge, призванный привлечь внимание чиновников к плохому состоянию дорог в Киеве (Экономические известия).

В ведомстве признали, что дороги Украины находятся в не самом лучшем состоянии, однако при этом обвинили Березу в манипуляциях и популизме, информирует news.eizvestia.com.

«Укравтодор» не отвечает за все дороги в стране. «Укравтодор» отвечает только за дороги государственного значения. Дороги и улицы в городах, селах – ответственность органов местного самоуправления. Областные и районные дороги – сфера ответственности областных государственных администраций. Просим не манипулировать информацией и не вводить людей в заблуждение», – сказано в сообщении агентства.

В ответ нардеп также обвинил «Укравтодор» в манипуляции и пиаре.

«Укравтодор, вы не пиаром занимайтесь, а дороги ремонтируйте. Так ремонтируйте, чтоб люди довольны были, а не проклинали бы вас. И не надо начинать петь песни о том, что за год вы не можете все исправить. Вы все эти

годы не можете исправить. Не стоните о тяжелом климате или погодных условиях. Посмотрите на Беларусь или Швецию. Климат там схож с нашим, а дороги… Ну, вы сами в курсе. И последнее. Качество вашей работы – это отсутствие ям на дорогах государственного значения. А с этим у вас пока все плохо. Не верите?» – написал он, призвав автолюбителей публиковать в сети фото и видео реального состояния дорог в Украине.

Кроме того Береза добавил, что все вышеуказанные претензии также относятся и к «Киевавтодору».

(вгору)

Додаток 3

14.03.2018

Создатель интернета призвал к революции

Создатель интернета Тим Бернерс-Ли опубликовал открытое письмо, приуроченное к двадцать девятой годовщине появления интернета. По его словам, развитию технологий мешают крупные компании. Они противятся принципиальным изменениям и уничтожают небольшие независимые сайты и сервисы, подобные тем, на которых раньше держался интернет (InternetUA).

Бернерс-Ли считает, что интернет мог бы стать намного лучше, если правительства разных стран, учёные, бизнесмены, инженеры, программисты, художники и гражданские активисты начнут сотрудничать друг с другом и выработают новые принципы взаимодействия. Наибольшей критике изобретателя подверглись такие гиганты, как Facebook и Google – именно эти компании, по его мнению, контролируют, какие идеи воплощаются в реальность, а какие умирают нереализованными. Они нанимают самых талантливых разработчиков и скупают наиболее перспективные инновации, но используют полученные преимущества не во благо обществу, а для увеличения собственных доходов. Наиболее ярким примером того, какую роль эти компании играют в мире, можно считать скандал перед выборами президента США. Американские соцсети оказывают настолько сильно влияние на умы и настроение людей, что публикации провокационных вбросов с фейковых аккаунтов якобы определили результаты голосования.

Бернерс-Ли уверен, что интернет не безнадёжен и его ещё можно спасти. На это способно общество, которое отвергнет монополистическую власть интернет-корпораций и начнёт само решать, что именно ему нужно. Кроме того, потребуются новые законодательные инициативы, которые ограничат гегемонию крупнейших компаний и создадут равные условия для всех.

(вгору)

Додаток 4

17.03.2018

Выявлена связь между зависимостью от социальных сетей и чертами характера

Компании, управляющие социальными сетями, стремятся создать пользователям наиболее благоприятную обстановку. Исследование, выполненное в Бингамтонском Университете в Нью-Йорке, пробует выяснить как взаимное влияние определённых личностных качеств может быть связано с болезненным пристрастием к социальным сетям (InternetUA).

«Было проведено множество исследований с целью выяснить, как сочетание определённых личностных черт может быть связано с болезненным пристрастием к алкоголю и наркотикам, – рассказывает профессор Школы менеджмента Бингамтонского Университета Исаак Вагефи. – Мы решили применить аналогичную методику к зависимости от социальных сетей».

Трёмстам студентам было предложено ответить на ряд вопросов, и в результате были выявлены три личностных особенности, наиболее связанные с увлечением социальными сетями – нейротизм, добросовестность (сознательность) и доброжелательность (конформность).

Эти три черты характера являются частью пятифакторной личностной модели, принятой в психологии. Установлено, что остальные две черты в этой модели – экстравертность и открытость опыту – не играют заметной роли в склонности к зависимости от социальных сетей.

Дополнительно к проверке влияния отдельных черт, исследователи рассмотрели и взаимное их влияние. «Это сложная, многосторонняя тема. Здесь неприемлем упрощающий подход», – говорит Вагефи.

Невротизм и добросовестность

Сами по себе невротизм и совестливость имеют прямое влияние, как положительное так и отрицательное, на склонность к развитию зависимости от социальных сетей.

Исследователи обнаружили, что невротизм (показатель глубины переживания отрицательных эмоций, таких как стресс и беспокойство) увеличивает вероятность зависимости от социальных сетей.

С другой стороны, большая добросовестность (самоконтроль и стремление к достижению поставленных целей) снижают вероятность развития зависимости.

Но, будучи рассмотренными совместно, невротизм показал ослабляющее влияние на добросовестности в отношении пристрастия к социальным сетям.

Так как личность может быть очень невротичной и одновременно обладать высоким самоконтролем, исследователи обнаружили, что даже способные к самодисциплине и целенаправленным усилиям люди в состоянии стресса и беспокойства могут потерять контроль над тягой к социальным сетям.

Ослабляющее влияние нейротизма на сознательность (самоконтроль) делает более вероятным развитие зависимости от социальных сетей.

Добросовестность и конформность

Установлено, что конформность (степень дружелюбия, сопереживания и отзывчивости) сама по себе не имеет значительного влияния на пристрастие к

социальным сетям, но такое влияние проявляется, если рассматривать конформность совместно с сознательностью.

Сочетание низких добросовестности и конформности (человек может быть одновременно неотзывчивым и безответственным) часто связано с большей склонностью к сетевой зависимости – но, как это ни странно, точно так же влияет на зависимость одновременно повышенные конформность и сознательность.

Вагефи объясняет этот неожиданный результат в свете «рациональной зависимости», когда человек намеренно проводит больше времени в социальных сетях для расширения дружеских отношений.

Такой результат необычен, так как не является следствием иррациональности или отсутствия самоконтроля, которые часто связаны с зависимостями. Здесь же зависимость развивается в ходе рационального процесса с благими намерениями.

Вагефи выразил надежду, что это исследование заставит рассматривать «картину в целом» при выяснении того, как личностные черты влияют на зависимость от социальных сетей. Вместо того, чтобы обращать внимание на какой-то одной черте личности, оно обращает внимание на личностный профиль в целом.

(вгору)

Додаток 5

25.03.2018

У школах США штучний інтелект виявляє небезпечних учнів через соцмережі // Програмне забезпечення використовує 450 тисяч різних індикаторів, які вказують на те, що учень може завдати шкоди собі чи оточуючим

Вища техшкола Шошин Веллі (Shawsheen Valley Technical High School) в місті Біллеріка штат Массачусетс запровадила стеження за учнями в соцмережах за допомогою штучного інтелекту, щоб виявляти тих, хто може бути небезпечним для себе і суспільства. Заклад став одним з багатьох шкіл, що почали використовувати цю технологію (ipress.ua).

Про це пише видання WBUR.

Систему стеження розробила для школи аналітична компанія Social Sentinel. Гендиректор фірми Гері Марголіс розповів, що Social Sentinel працює з лінгвістами та психологами, щоб натренувати свій штучний інтелект.

Компанія використовує власну «бібліотеку загроз», що складається з 450 тис. різних індикаторів, які вказують на те, що учень може завдати шкоди собі чи оточуючим. Штучний інтелект маркує потенційно проблемних учнів і має допомогти школі запобігти трагедіям.

«Ми зробили крок назад і подивилися на мову, яку використовували стрілки у школах у своїх маніфестах, опублікованих у соцмережах. І ми

спробували виявити патерни і подібності. Ми можемо навчити комп'ютери ідентифікувати такі нюанси», – розповів гендиректор Social Sentinel.

За інформацією WBUR, учні школи «навіть не здогадувалися», що їх навчальний заклад використовує такі технології. Марголіс заявив журналістам, що компанія вважає себе не «інструментом спостереження, моніторингу або розслідування», а «системою попередження загроз».

Social Sentinel працювала над системою спільно з поліцейськими, до того як дала доступ школам. Послуги компанії коштують Шошин Веллі 10 тис. доларів на рік, однак фірма відмовилася розкривати, наскільки успішно працює її штучний інтелект.

У місті Арлінгтон систему впровадили на рівні поліцейського управління: вона аналізує повідомлення від учнів відразу у всіх школах міста. За словами начальника поліції Фреда Райана, завдяки Social Sentinel співробітники вже змогли врятувати учня, який планував накласти на себе руки.

Шошин Веллі не єдина школа, яка почала практикувати такий підхід до безпеки на тлі випадків масової стрілянини. Як повідомляє WUSF News, школа Майамі-Дейд запросила 30 млн з бюджету штату на посилення системи безпеки, зокрема оплату послуг співробітників, які відстежуватимуть соцмережі.

Школи в техаському окрузі Вілсон і у штаті Теннессі також використовують системи моніторингу соціальних мереж, пише Tennessean. Навчальні заклади в Нью-Йорку і Флоріді витратили мільйони доларів на створення цілодобового спостереження, яке здатне розпізнавати осіб і має біометричні сенсори, інформує Gizmodo.

(вгору)

Додаток 6

21.03.2018

Роман Черный

Почему Telegram – самый бескомпромиссный мессенджер современности

На днях мы стали свидетелями очередного обострения в противостоянии Павла Дурова и российских спецслужб. Роскомнадзор в очередной раз потребовал от Дурова, чтобы тот предоставлял ФСБ ключи, позволяющие читать частную переписку пользователей Telegram. Дуров же в очередной раз отказался. По его словам, он не намерен ставить под удар неприкосновенность переписки. Да и не смог бы, даже если бы захотел – шифрование обойти не может даже создатель мессенджера (IGate).

Давайте же разберемся, почему именно Telegram настолько надежен.

Секретные и несекретные чаты

Первое, что следует понимать – к некоторой части переписки Дуров все же мог бы получить доступ, если бы захотел. В Telegram имеются секретные и

несекретные (обычные) чаты. По-умолчанию вся переписка, которую вы ведете в мессенджере, ведется через обычный чат.

Почему Дуров сразу не сделал все чаты секретными? Потому что такое решение ограничило бы функциональность мессенджера. В частности, это привело бы к потере всей истории переписок.

Представьте, что вы купили новый смартфон. Вы вставляете в него свою карточку, устанавливаете приложение Telegram и получаете доступ ко всей истории своих старых переписок. Возникает вопрос: где же хранилась эта история? Она хранилась на облачном сервере Telegram. А значит, в теории, компания могла бы в нее заглянуть.

Так работают обычные несекретные чаты Telegram, и так же работают все популярные мессенджеры вроде WhatsApp или Viber. Запомните простое правило: если мессенджер сохраняет переписку в облаке, о стопроцентной надежности речь не идет. Даже если вы удалите сообщения у себя в смартфоне, они останутся в облаке до тех пор, пока их не удалят все участники беседы.

Но если так работают все мессенджеры, почему российские спецслужбы взъелись именно на Telegram? Всё дело в секретных чатах.

Сундук с двумя замками

Секретные чаты Telegram абсолютно надежны. Все потому, что общение в них защищено так называемым шифрованием End-to-End. Простым языком эту систему можно описать так.

Представьте, что у вас есть неразрушимый сундук. Вы пишете письмо другу, кладете его в сундук и закрываете навесным замком. Ключ от этого замка существует в единственном экземпляре, и вы оставляете его при себе.

Сундук доставляется вашему другу, но тот не может его просто открыть. Вместо этого он берет еще один навесной замок, вешает его рядом с первым и закрывает на собственный уникальный ключ. Свой ключ он также оставляет при себе.

Сундук, закрытый уже двумя замками, отправляется обратно. Вы получаете его, снимаете свой первый замок, и снова отправляете сундук другу. В этот раз сундук закрыт на единственный замок, принадлежащий вашему другу, так что он без проблем снимает этот второй замок и наконец-то получает доступ к письму.

Таким образом, сундук трижды курсировал между отправителем и получателем в запечатанном виде. А что же Telegram? Telegram в этом случае – всего лишь курьер, который бегает с сундуком туда и обратно. Возможности заглянуть внутрь у него нет.

Всякий раз, когда вы в секретном чате Telegram отправляете сообщение другому пользователю, мессенджер за доли секунды выполняет все вышеописанные операции. При этом переписка хранится только у вас в смартфоне. Удалите ее – и никаких следов не останется. О надежности ключей шифрования, которые находятся у пользователей, тоже не приходится волноваться. Чтобы взломать один такой ключ, всем компьютерам планеты

придется работать несколько лет. А индивидуальные ключи сменяются раз в несколько дней.

Проще говоря, когда Павел Дуров говорит, что *не может* предоставить никому ключей от секретной переписки, он говорит чистую правду. Шифрование End-to-End взломать невозможно.

Справедливости ради, стоит отметить, что End-to-End-шифрование понемногу внедряют и другие мессенджеры. Правда, часто они ставят под удар безопасность переписки в угоду комфорту пользователей.

Так, в 2016 году на конференции Google I/O представители WhatsApp признались, что их мессенджер сохраняет в облако копии чатов, которые шифруются через End-to-End. Дескать, это делается для того, чтобы пользователи имели доступ к истории переписки.

Ситуация получается довольно абсурдной. Система WhatsApp проделывает все вышеописанные операции с сундуком и двумя замками только для того, чтобы потом, когда сундук будет открыт, курьер подсмотрел через плечо пользователя и скопировал письма в свой архив. Конечно, разработчики клянутся, что облачное хранилище истории абсолютно надежно. Хакеры его, может быть, и не взломают. Но как быть с запросами от правительства? Вообще, весьма показательным кажется тот факт, что у ФСБ не возникло никаких претензий к администрации WhatsApp.

Бескомпромиссный мессенджер

Если секретные чаты Telegram абсолютно надежны, то и за обычную переписку можно не беспокоиться. Как бы сильно Роскомнадзор не угрожал Дурову, тот не сможет выполнить требований российских властей. А потому у него нет причин идти даже на маленькие уступки.

На данный момент Роскомнадзор дал Telegram 15 дней на размышления. Но этот срок – условность. Учитывая вектор движения РФ, блокировка Telegram, да и вообще всего, что имеет отношение к свободе слова, просто неизбежна. Если этого не случится через 15 дней, это случится через месяц, полгода, год.

Конечно, Дуров уже подготовился к «светлому будущему». Еще прошлым летом Telegram получил обновление, добавляющее в мессенджер функцию с крамольным названием «Свобода Слова». Функция должна позволить мессенджеру обходить возможные блокировки не только на территории РФ, но и ускользать из-под колпака других диктатур. Вероятно, у россиян будет повод опробовать ее в действии.

В целом же, пользоваться Telegram имеет смысл всем, кто уважает приватность и личное пространство. Возможно, Telegram не самый яркий и богатый на функции мессенджер, но он, определенно, один из самых надежных и безопасных. А его создатель – один из самых бескомпромиссных людей в современном IT-пространстве. Павел Дуров хорошо известен своими либертарианскими взглядами. И пока он контролирует Telegram, ни киберпреступники, ни правительства, ни спецслужбы не смогут заглядывать вам через плечо.

(вгору)

Додаток 7

14.03.2018

Fujitsu предложила технологию обнаружения уязвимостей в блокчейн-системах

Компания Fujitsu объявила о создании технологии, которая в проактивном режиме способна обнаруживать уязвимости в смарт-контрактах, а также в программах, выполняющих транзакции на основе блокчейн-платформ. Новая разработка автоматически определяет подозрительные места в исходном коде смарт-контракта (Компьютерное Обозрение).

Технология блокчейн гарантирует, что данные не будут изменены в процессе передачи. Поэтому она может найти применение не только в сфере финансов, но и в других областях, включая недвижимость и здравоохранение. Блокчейн предлагает особые функции, которые получили название смарт-контракты. Смарт-контракты автоматически создаются в системе, копируются в разные хранилища и исполняются с помощью распределенных вычислений. Поэтому после исполнения смарт-контракта его нельзя исправить, даже если позже в нем обнаружатся уязвимости.

С помощью Ethereum, единой платформы для блокчейн-приложений, смарт-контракты объединяются в 6 категорий. В ходе идентификации начального вызова к исполнению транзакции с помощью непрямых вызов через несколько смарт-контрактов возникали изменения данных о начальном вызове транзакции из-за определенных особенностей платформы Ethereum. Это свойство системы можно использовать для обхода процедуры аутентификации. Предыдущие разработки не позволяли обнаруживать подобного рода риски, т.к. они не могли отследить внутреннюю информацию блокчейн-платформы о транзакции.

Специалисты Fujitsu разработали специальные алгоритмы для определения подвергающихся рискам последовательностей транзакций в Ethereum. Для защиты используется технология символьного выполнения. С помощью особых алгоритмов разработка Fujitsu может обнаруживать риски, которые могут быть пропущены при проверке корректности смарт-контрактов всех 6 категорий в ручном режиме, и определять соответствующие места в их исходном коде.

Разработанная технология с высокой точностью определяет, к какой части исходного кода относится обнаруженная уязвимость смарт-контракта. Она позволяет осуществлять символьное выполнение за счет удаления неиспользуемых команд.

Компании-разработчики установили, что ранее используемые инструменты проверки обнаруживают только порядка 67 % рисков, тогда как новая технология Fujitsu обнаруживает до 100 % (за исключением отдельных случаев). Показатели точности обнаружения уязвимостей достигают 88 %, что

гарантирует защиту от всех типов уязвимостей и выявление их точного положения в исходном коде.

Новая технология улучшит эффективность разработки новых типов смарт-контрактов. Совместно с технологией обнаружения расположения рисков, она будет способствовать значительному уменьшению объема работ по анализу спецификации, оценке и исправлению кода.

Отмечается, что компания Fujitsu продолжит разработку технологий проверки надежности смарт-контрактов не только на базе платформы Ethereum, но и для проектов Hyperledger Fabric и Hyperledger, реализуемых некоммерческим консорциумом Linux Foundation.

(вгору)

Додаток 8

14.03.2018

Сотрудники «Лаборатории Касперского» нашли неубиваемый компьютерный вирус

Чуть ли не каждый день во Всемирной паутине обнаруживают несколько новых компьютерных вирусов. И очень редко бывает так, что вирусы невозможно уничтожить. Более того, редкий вирус способен скрываться годами от разработчиков антивирусного ПО. Но, согласно недавнему сообщению специалистов «Лаборатории Касперского», им удалось обнаружить именно такой вирус: его почти невозможно уничтожить, а «работал» он с 2012 года (Центр информационной безопасности).

Вирусное ПО получило название Slingshot и используется для точечной слежки за пользователями. Вирус может сохранять нажатия клавиш, отправлять скриншоты, перехватывать трафик, пароли и все данные до того, как они будут зашифрованы. Более того, работа вируса не вызывает никаких ошибок в ядре системы. Также удалось выяснить, как вирус внедрялся в систему: происходило это через уязвимость маршрутизаторов MikroTik. Производители уже выпустили новую прошивку, однако в «Лаборатории Касперского» допускают, что вирус может использовать и другие пути внедрения. Проникнув на маршрутизатор, вирус заменяет одну из DDL-библиотек вредоносной, загружая ее в память компьютера при запуске. Таким образом, вредоносная DLL-библиотека запускается на компьютере и подключается к удаленному серверу для загрузки самой программы Slingshot. Как отметили эксперты, вредоносное ПО включает в себя две части: Cahnadr (модуль режима ядра) и GollumApp (модуль пользовательского режима), предназначенные для сбора информации, сохранения присутствия на системе и хищения данных. Как заявили сотрудники «Лаборатории Касперского», «Модуль Cahnadr, также известный как NDriver, имеет функции антиотладки, руткита и анализа трафика, установки других модулей и многое другое. Написанный на языке программирования C, Canhadr обеспечивает полный доступ к жесткому диску и оперативной памяти, несмотря на ограничения безопасности устройства, и выполняет контроль

целостности различных компонентов системы, чтобы избежать обнаружения системами безопасности».

Высокий уровень защиты самого вируса от обнаружения также заслуживает отдельного упоминания. Например, еще один из его модулей называется Spork. Он собирает информацию об ОС и о том, какие антивирусы на ней установлены. В зависимости от этого, вирус использует разные способы заражения.

«Например, вирус использовал зашифрованную виртуальную файловую систему, которая создавалась в неиспользуемой части жесткого диска. Это решение очень сложное, и Slingshot – чуть ли единственный вирус, который оснащен такой технологией. Более того, каждая текстовая строка в модулях вируса зашифрована».

Кто является автором вируса, на данный момент выяснить не удалось, но, как пишет издание Engadget, исходя из анализа кода, можно сделать вывод, что вредоносное ПО создали, скорее всего, англоязычные программисты. Также сообщается, что основными жертвами хакеров стал ряд правительственных организаций Кении, Йемена, Ливии, Афганистана, Ирака, Танзании, Иордании, Маврикия, Сомали, Демократической Республики Конго, Турции, Судана и Объединенных Арабских Эмиратов.

(вгору)

Додаток 9

14.03.2018

Взломавшие CCleaner хакеры готовили третий этап вредоносной кампании

Исследователи компании Avast сообщили новые сведения о нашумевшем прошлогоднем инциденте с CCleaner. Согласно представленному на конференции SAS в Мексике докладу, хакеры, атаковавшие инфраструктуру CCleaner и внедрившие в утилиту бэкдор, готовились к заражению инфицированных компьютеров третьим вариантом вредоносного ПО, сообщает Bleeping Computer (Центр информационной безопасности).

Напомним, инцидент имел место в сентябре 2017 года, когда исследователи Avast обнаружили , что в 32-разрядные версии CCleaner v5.33.6162 и CCleaner Cloud v1.07.3191 был внедрен инфостилер. По словам экспертов, вредонос инфицировал порядка 2,7 млн компьютеров, однако похищал только базовую информацию, такую как имя компьютера и данные о домене.

Как выяснилось позднее, внедрение инфостилера было лишь первым этапом масштабной кампании, предназначенным для выявления компьютеров, относящихся к внутренним сетям крупных технологических компаний, таких как Google, Cisco, Oracle, Intel, Akamai, Microsoft и пр. В ходе второго этапа злоумышленники заразили вредоносным ПО только 40 компьютеров, обнаруженных в этих сетях. По мнению экспертов Avast, Cisco Talos и

«Лаборатории Касперского», ответственность за атаки лежит на киберпреступной группировке Axiom, предположительно имеющей китайское происхождение.

Согласно представленному на конференции в Мексике докладу, злоумышленники также готовили третий этап своей кампании. На компьютерах сотрудников Piriform (компании-разработчика CCleaner, приобретенной Avast в июле 2017 года) был обнаружен образец третьего вредоносного ПО, присутствующий там еще с 12 апреля 2017 года. Хакеры использовали сети Piriform для подготовки основного взлома, считают эксперты.

Речь идет о многофункциональном модульном фреймворке ShadowPad. Вредонос оснащен целым набором плагинов, предназначенных для самых разных целей. В частности, они выполняют функции бэкдора, кейлоггера и инфостилера. Судя по лог-файлам на зараженных компьютерах Piriform, в данном случае хакеры намеревались применять ShadowPad в качестве кейлоггера.

По мнению специалистов Avast, ShadowPad должен был использоваться на третьем этапе вредоносной кампании. Тем не менее, исследователи безопасности выявили зараженную версию CCleaner до запуска третьего этапа, и планы злоумышленников были расстроены.

(вгору)

Додаток 10

14.03.2018

Найден способ взломать компьютер через наушники

Исследовательская группа из университета имени Давида Бен-Гуриона в Негеве (Израиль) провела эксперимент по захвату данных с помощью наушников и динамиков компьютера. О новом методе сообщило издание Bleeping Computer (InternetUA).

Способ проведения атаки, названный специалистами MOSQUITO, предполагает заражение компьютера специальным вирусом, который производит реверсию выходных аудиоразъемов. Инфицированная машина по сути превращает динамики и наушники одновременно и в передатчики звуковой информации, и в некое подобие микрофонов.

Вредоносное программное обеспечение способно преобразовывать локальные сохраненные на компьютере файлы в аудиосигналы и передавать их злоумышленникам. Принимающая машина, используя тот же вирус, принимает информацию через динамик или наушник, а затем преобразует его обратно в файл.

В проведенном эксперименте участвовал массив двоичных данных, который передавался на расстоянии от одного до девяти метров. Скорость обмена достигала 1800 бит в секунду. При этом шум окружающей среды,

звучащая человеческая речь или музыка не внесли существенных помех в зловредные действия вируса.

По данным исследователей, скорость передачи информации резко падает, когда динамики двух компьютеров не обращены друг к другу или при обмене данными изменяется звуковая частота. Исследователи объясняют это изначальной оптимизацией аудиосигналов компьютера под слух человека, а не под машинное восприятие.

Эксперты отмечают, что вряд ли подобные проблемы для злоумышленников станут критичными. Каким образом можно избежать подобной атаки, пока неизвестно.

(вгору)

Додаток 11

14.03.2018

Хакеры научили роботов показывать порно и вымогать биткоины

Мошенники давно используют вредоносное ПО для вымогательства денег – файлы на электронном устройстве шифруются, а за возможность вернуть доступ к ним нужно заплатить (однако оплата не является гарантией). Как выяснили специалисты из компании IOActive, под ударом оказываются не только компьютеры или смартфоны – новой целью могут стать роботы (InternetUA).

В качестве доказательства эксперты взломали гуманоидного робота NAO компании SoftBank. Он является «близнецом» более известного робота Pepper, который также уязвим для хакеров. Эти устройства работают в качестве помощников продавцов, их можно встретить в учреждениях образования. NAO оборудован крупным дисплеем, размещенным в районе груди, микрофоном и динамиками.

Об уязвимости специалисты IOActive сообщили производителю роботов около года назад, однако информации о том, что дыра в безопасности закрыта, нет.

Как продемонстрировали в компании, зараженного робота можно полностью вывести из строя, научить показывать на цветном экране порнографию (или любой другой контент), проклинать клиентов и атаковать человека. От лица злоумышленников робот за возврат контроля может требовать выкуп в криптовалюте. Сложностей добавляет то, что починка или замена устройства может занять недели. Так, в общем-то, и случилось с роботом в распоряжении IOActive – вернуть его в строй может только производитель, а клиент оплачивает все сопутствующие расходы.

(вгору)

Додаток 12

14.03.2018

Вредонос Slingshot занимается кибершпионажем как минимум с 2012 г.

Исследователи «Лаборатории Касперского» обнаружили сложную киберугрозу, которая используется для шпионажа в странах Ближнего Востока и Африки по меньшей мере с 2012 г. Вредоносное ПО получило название Slingshot (Компьютерное Обозрение).

Одна из самых примечательных особенностей Slingshot – необычный вектор атак. Многие жертвы зловреда были заражены через роутер. В ходе атак группировка, стоящая за Slingshot, взламывает устройство и помещает в него компоненты вредоносного ПО, в том числе динамически загружаемую библиотеку ipv4.dll. Когда администратор подключается к роутеру для его настройки или диагностики, прошивка устройства загружает и запускает на компьютере администратора этот модуль, который, в свою очередь, скачивает остальные модули этой вредоносной программы с роутера. Один из этих компонентов может работать в режиме ядра (kernel mode), что даёт ему полный контроль над компьютером жертвы.

Метод взлома самого роутера пока остаётся неясным, возможно, злоумышленники использовали для этого один из известных эксплойтов.

После заражения Slingshot загружает несколько дополнительных модулей, включая два больших и мощных: Cahnadr и GollumApp. Они работают в связке и «помогают» друг другу в сборе информации, защите от обнаружения и фильтрации данных.

Судя по всему, главное предназначение Slingshot – кибершпионаж. Программа собирает и передаёт злоумышленникам скриншоты, вводимые с клавиатуры символы, сетевую информацию, пароли, подключения к USB, данные из буфера обмена и многое другое. Доступ зловреда к ядру означает, что в теории Slingshot может украсть всё что угодно.

Slingshot включает и ряд техник, помогающих ему оставаться незамеченным. Среди них шифрование всех модулей, вызов системных служб напрямую, минуя защитные решения, ряд антиотладочных приёмов, а также гибкие сценарии поведения в зависимости от того, какое защитное решение используется в устройстве.

Образцы вредоносного кода, которые анализировали эксперты, были помечены как «версия 6.x». Судя по этой метке, угроза существует уже довольно давно. В совокупности эти улики позволяют сделать вывод, что группировка, стоящая за Slingshot, высокоорганизованна, профессиональна и, возможно, спонсируется государством. Текстовые артефакты в коде говорят о предположительно англоязычном происхождении разработчиков.

На данный момент эксперты обнаружили около 100 жертв Slingshot. Большинство из них расположены в Кении и Йемене, также есть жертвы в Афганистане, Ливии, Конго, Иордании, Турции, Ираке, Судане, Сомали и Танзании. Значительная часть атакованных – физические лица, однако встречаются и государственные органы.

(вгору)

Додаток 13

18.03.2018
Как защитить аккаунт в соцсетях от собственного любопытства

Кем ты был в прошлой жизни? Что о тебе говорит твоя аватарка? Как ты записан в телефоне у своих друзей? Эти вопросы выманивают персональные данные, которые мы зачастую бездумно дарим мошенникам (InternetUA).

В начале марта администраторы нескольких телеграм-каналов пожаловались на взломы, а самым популярным приложением в российском AppStore стало GetContact, которое позволяет узнать, как ты записан в телефонах друзей. Эксперты не видят прямой связи между этими событиями, но не исключают, что данные из приложения упростят подобные атаки в будущем, ведь приложение собирает в одной базе информацию, которая необходима для взлома аккаунта.

В соглашении (которое мы все, разумеется, читали) говорится, что данные могут быть переданы третьим лицам, коими могут оказаться банки, мошенники или спамеры.

Лишняя информация

«Полное имя, дружеские прозвища, номер телефона, адрес электронной почты, пол, аккаунты в социальной сети, место работы, фотография, адрес – такого набора данных о человеке достаточно для того чтобы провести очень хорошо подготовленную целевую атаку и получить доступ не только к социальным сетям, но и к деньгам жертвы, если эти данные окажутся в руках злоумышленников», – предупреждает ведущий контент-аналитик «Лаборатории Касперского» Надежда Демидова.

Она добавляет, что стоит обратить внимание на права, которые предоставляются приложению: доступ к контактам, телефону, памяти телефона или камере открывают излишний простор владельцам приложения. Например, позволяют просматривать и модифицировать историю вызовов, менять контакты в адресной книге, делать снимки, а также совершать звонки.

GetContact как инструмент хакера

Например, GetContact в качестве «вступительного взноса» предлагает пользователю предоставить доступ к данным о городе и стране проживания, а также запрашивает фото, пол, место работы, аккаунты в социальных сетях. Кроме того, «новобранец» GetContact должен поделиться с приложением своей телефонной книгой. Таким образом, в базу попадают не только данные пользователя, но и номера его контактов, которые вовсе не планировали в ней оказываться.

«GetContact получает данные зарегистрированных пользователей, они попадают в их публичную базу. Приложение позволяет найти номер администратора телеграм-канала, если, конечно, это человек публичный (многие телеграм-каналы анонимны: их администратор не известен). Зная

номер телефона, вы можете пытаться привязать его к аккаунту в телеграме. Зная, что этот аккаунт является создателем канала, вы уже получаете вектор, понятный для взлома», – считает эксперт по информационной безопасности Group-IB Илья Обушенко.

Безнадежная защита

По его словам, даже двухфакторная аутентификация не гарантирует безопасность, если пользователь легкомысленно относится к защите своей почты и аккаунтов в соцсетях. «Сбросить» один этап аутентификации можно, зная почту администратора канала и имея к ней доступ.

Люди часто привязывают к одному почтовому ящику много аккаунтов в различных сервисах, а также используют для них один и тот же пароль, который зачастую подходит и для почты: знаешь его – знаешь все.

Таким образом, злоумышленнику достаточно взломать какой-то из аккаунтов пользователя, и он получит доступ к почтовому ящику.

«Самое трудоемкое – это получить код из SMS. Как правило, для этого используются два способа. Первый – это возможность с помощью социальной инженерии, фишинга получить этот код. Например, вам звонят, говорят: «Вы выиграли миллион, сейчас вам придет код подтверждения, мы точно должны знать, что это вы, скажите нам его, пожалуйста». А это был код для идентификации в телеграме. Злоумышленник получает доступ к телеграму, там производит изменение номера телефона и удаление аккаунта или очищение его от всего контента. Вторая история – клонирование сим-карты. Это дело затратное, но возможное. С помощью клонирования SIM-карты злоумышленник получает доступ к телефону, SMS и доступ к аккаунту в телеграме», – поясняет Обушенко.

GetContact вроде бы даже предлагает пользователям возможность удалить себя из базы. Однако эксперты заметили, что вместе с номером телефона приложение запрашивает и IMEI (международный идентификатор мобильного оборудования – Forbes) устройства, который из базы никуда не исчезает, да и номер на практике удаляется не сразу.

«Вы меняете номер, вставляете в телефон SIM-карту с новым номером, но кто-то уже знает ваш IMEI, привязанный к другому номеру телефона. И ему не составит труда привязать ваш новый номер телефона к старому. Таким образом, появляется понимание, с кем связан номер, и вас снова нашли», – добавляет Обушенко.

Слишком любопытные тесты в соцсетях

Но GetContact – не единственное приложение, которое собирает наши персональные данные. Тесты, которые запрашивают доступ к соцсетям, чтобы проанализировать их или дать вам возможность поделиться результатом с друзьями, тоже пополняют таким образом чьи-то базы данных, а иногда могут направлять на фишинговый сайт или давать ссылку на скачивание вредоносного ПО.

Правда, их аппетиты, как правило, скромнее: они запрашивают доступ к списку друзей, открытому профилю и электронной почте. Но есть и более

любопытные, которым нужен доступ ко всем постам, место жительства, работы, фотографии и дата рождения.

«На Facebook, например, есть возможность восстановить пароль, опознав людей на фотографиях, а если вы уже предоставили эту информацию каким-то приложениям, мошенники могут сделать это за вас», – описывает потенциальную атаку Демидова. Она добавляет, что сейчас данные стоят «действительно много» и напоминает, что в соглашении GetContact прямо указано, что они могут быть переданы третьим лицам.

«И кем окажутся эти третьи лица, банком или мошенником – большой вопрос», – заключает эксперт «Лаборатории Касперского».

Исправление ошибок

Пройдена ли точка невозврата, если страница пестрит результатами тестов, да и GetContact уже установлен? Скорее всего, да. Но на будущее все равно нужно сменить все пароли, причем важно, чтобы они были разными. Для каждого аккаунта. И для почты тоже.

Двухфакторная аутентификация – must have. Здесь компромиссов быть не может. И, конечно, нужно следить за тем, какие ссылки вы открываете и на каких сайтах вводите свои данные.

Обушенко рекомендует владельцам каналов в телеграме, групп «Вконтакте» или Facebook не привязывать их к личному аккаунту, с которого ведется общение. По мнению эксперта, безопаснее купить отдельную SIM-карту и использовать ее. Лучше не применять публичные беспроводные сети или выходить в них только через VPN.

«Это обеспечит шифрованное соединение. Даже если кто-то будет пытаться вас прослушать или паразитировать, ничего не выйдет... И почаще менять пароли – раз в месяц-три», – рекомендует эксперт Group IB.

Демидова советует также зайти в настройки социальной сети и посмотреть, каким приложениям даны разрешения, и ограничить их при необходимости.

«Тесты, популярные в социальных сетях, часто запрашивают доступ на размещение контента в социальной сети от вашего имени, то есть, без вашего ведома они могут разместить любой контент на вашей странице, например, фишинговую ссылку», – предупреждает она. Демидова добавляет, что такие приложения запрашивают доступ к адресу электронной почты, контактам пользователя и его фото. Даже если владелец потом удалит приложение или отзовет право на использование своих фотографий, нет гарантий, что приложение выполнит его пожелание. «Информация, которую вы уже предоставили этим приложениям, может остаться у них, и ей могут воспользоваться злоумышленники», – опасается Демидова.

Информационная гигиена

Каждый раз, когда пользователи думают, что вот теперь-то они видели все, появляется новый способ отвлечь внимание и выманить персональные данные. Вот только основные правила безопасности не меняются, и их стоит помнить.

«Сколько бы людям ни говорили, что нужно беречь свои персональные данные, сколько бы таких историй ни происходило, все равно они повторяют свои ошибки»? – печалится Обушенко.

Он сокрушается, что многие пользователи беспорядочно раздают свой номер телефона различным сайтам, а потом понимают, что надо бы перестать и поменять SIM-карту. Но поезд уже ушел: из Интернета нельзя ничего стереть. Если задаться целью, то все равно можно найти и сопоставить все аккаунты, которые были привязаны к одному номеру.

«Такой сейчас мир: начать жизнь с чистого листа так, чтобы нельзя было связать вас с вашим прошлым – уже практически невозможно», – заключает эксперт.

(вгору)

Додаток 14

19.03.2018

Facebook уличили в сливе данных 50 миллионов пользователей

Социальная сеть Facebook проводит собственное расследование относительно связи своих сотрудников со сторонней компанией, которая завладела данными 50 миллионов пользователей. Предполагается, что они использовали личную информацию юзеров для поддержки штаба нынешнего президента США Дональда Трампа, сообщает CNN (InternetUA).

Руководство корпорации выяснило, что сотрудники Facebook Джозеф Канселлор (Joseph Chancellor) и Александр Коган (Aleksandr Kogan) являются создателями фирмы Global Science Research, которая предоставляла данные платформе Cambridge Analytica. Последняя была тесно связана с предвыборным штабом Трампа. Как сообщает ряд зарубежных СМИ, фирма обладает информацией о нескольких десятках миллионов аккаунтов, собранной с помощью приложения для опросов под названием thisisyourdigitallife. Юзерам оно преподносилось как составитель «психологического портрета».

Недавно в блоге Facebook появилось сообщение о приостановке работы лаборатории стратегических коммуникаций, в том числе сбора аналитических данных о пользователях, до выяснения обстоятельств. Канселлор и Коган являются сотрудниками этого подразделения. Также компания временно прервала сотрудничество с Cambridge Analytica.

Позднее компания дополнила эту новость информацией о том, что Коган якобы не нарушал соглашение о конфиденциальности, так как пользователи сами соглашались на обработку данных, регистрируясь в приложении. Однако насколько двое сотрудников корпорации злоупотребили своим служебным положением, пока неясно.

На сайте Cambridge Analytica указано, что компания занимается аналитикой данных, в том числе для политических проектов. В 2016 году разработанное сотрудниками приложение thisisyourdigitallife было заблокировано на Facebook, соцсеть потребовала удалить информацию. Однако

несколько дней назад руководству компании стало известно, что Cambridge Analytica не выполнила свои обещания.

(вгору)

Додаток 15

19.03.2018

Теория заговора или обычная паранойя: не прослушивает ли нас Facebook?

Краткая инструкция для параноиков, как выключить «прослушку» гаджета через социальную сеть (InternetUA).

Среди пользователей Facebook и Instagram ходит теория о том, что их телефоны прослушиваются, и рекламодатели знают, что говорят их владельцы. В магазине обуви вы просите принести вам ботинки от одного бренда вашего размера. В тот же вечер Facebook показывает вам рекламу обуви, которую вы примеряли. «Должно быть, совпадение», – думаете вы. «Какие весы сейчас самые продвинутые?», – спрашивает вслух ваша жена. Через пять минут в Instagram-ленте появляется реклама весов. Вы чихаете, и мать советует принять таблетки от простуды, а через некоторое время вы видите ее рекламу. Неужели компании и правда прослушивают телефоны?

Сотрудники Facebook всячески опровергают эту теорию. Вот какие факторы действительно влияют на рекламные рекомендации, и как их можно ограничить.

Ваша история покупок

Лекарство от простуды вам порекомендовали потому, что до этого вы покупали салфетки и спрей для носа. При этом вы пользовались карточкой аптеки, при регистрации которой вводили свой электронный адрес, номер телефона или другую информацию. Благодаря ей брокеры данных могут составить вашу историю покупок.

Информация о содержимом вашей корзины начала распространяться между участниками партнерской сети. Производитель лекарства выкупил ее у брокеров и с помощью данных вашей дисконтной карты нашел ваш аккаунт в Facebook (по словам компании, брокеры шифруют личную информацию, но все равно ее можно сопоставить с тем, что указано в вашем профиле). Затем производитель лекарства решил запустить рекламу для аудитории конкретного возраста, которая покупала ее медикаменты или средства конкурентов. Так вы и увидели эту рекламу.

Как это ограничить: откажитесь от использования дисконтных карты или указывайте при регистрации почту и номер телефона, которыми вы не пользуетесь.

Где вы были

Что может быть лучше вашей истории покупок? Разумеется, ваши геоданные. Вы недавно заходили в какой-то магазин? Реклама напомнит вам, что нужно будет туда вернуться. Вы находитесь рядом с каким-то заведением?

Держите купон на скидку! Рекламодатели узнают о ваших перемещениях с помощью GPS, точек Wi-Fi рядом с вами, IP-адресов и многого другого.

Как это ограничить: ограничение можно установить в настройках мобильного приложения Facebook. Зайдите в Настройки > Настройки аккаунта > Местоположение и запретите отслеживание геолокации. Отключите также историю перемещения.

Другие приложения тоже могут определять ваше положение. Чтобы это запретить, зайдите в настройки телефона и выберите «Конфиденциальность», а затем «Службы геолокации». Проверьте, какие настройки стоят в приложениях из списка (везде должно быть «Никогда» или «При использовании программы», но не «Всегда»).

Какие приложения вы используете

Разбираем случай с весами. Их реклама могла появиться у вас в ленте, потому что до этого вы скачивали приложение для здорового питания. Скорее всего, это приложение показывает рекламу из сети для аудитории Facebook. Даже если вы не авторизовались в нем через Facebook, оно все равно может найти вас по рекламному идентификатору, который есть у вашего телефона. После запуска приложения идентификатор отнес вас к аудитории, которая заботится о здоровом питании и поддержании нормального веса.

Как это ограничить: если у вас iOS, зайдите в Настройки > Конфиденциальность > Реклама и включите «Ограничение трекинга». Вы можете также сбросить идентификатор. Если у вас Android, зайдите в Настройки > Google > Реклама > Отключить персонализацию рекламы.

Ваши клики все расскажут

Благодаря истории вашего браузера Facebook может узнать о вас все. Плагин Facebook Pixel установлен на миллионах сайтов и приложений и позволяет рекламодателям и Facebook определять, что вы там делаете.

Как это ограничить: таргетированную рекламу используют такие крупные технологические компании, как Facebook, Amazon, Google и другие. В некоторых случаях ее можно отключить. На Facebook вы можете зайти в Настройки > Настройки аккаунта > Реклама > Настройки рекламы и отключить все опции на этой странице. Можете также удалить все интересы, которые указал за вас Facebook.

Поставьте плагины для браузера Ghostery или Privacy Badger. С их помощью вы увидите все отслеживающие плагины на сайтах и сможете их отключить.

Кем вы являетесь

Вся эта информация плюс ваши действия в Facebook и Instagram – какие страницы и публикации вы лайкали, кто у вас в друзья и так далее – позволяет составить ваш четкий портрет.

Брокеры данных могут сделать его еще точнее – какая у вас зарплата, какие автомобили вы любите, какого размера ваш дом, ваши политические взгляды, как вы тратите деньги и так далее.

Эти данные позволяют любому рекламодателю зайти в Менеджер рекламы Facebook и настроить таргетирование. Любой желающий может найти в настройках нужную аудиторию, например, тех, кто проживает в определенном районе, купили мебель и собираются скоро переезжать.

Как это ограничить: удалите Facebook и поселитесь в бункере. На самом деле ничто не поможет полностью остановить эту рекламу.

«Когда таргетирование используется правильно, реклама становится лучше, – считает представитель Facebook Джо Осборн. – Поэтому мы разрабатываем инструменты таргетирования так, чтобы они не сообщали рекламодателям личную информацию о пользователях, из-за чего люди могут контролировать, какую рекламу они видят».

Но проблема в том, что до конца непонятно, как именно эта реклама доходит до нас. Если вы верите, что Facebook все-таки прослушивает ваш телефон, вы можете всегда отключить микрофон. Если у вас iOS, зайдите в Настройки > Конфиденциальность > Микрофон > Facebook. Для Android нужно зайти в Настройки > Приложения > Facebook > Разрешения > Отключить микрофон.

(вгору)

Додаток 16

18.03.2018

Ваш смартфон постоянно слушает и смотрит в камеру на вас – даже когда выключен

Эксперт в сфере информационных технологий, искусственного интеллекта и ИТ-безопасности Игорь Ашманов посоветовал заклеивать камеры смартфонов и планшетов. В интервью «АиФ» специалист рассказал, как спецслужбы следят через смартфон, почему опасно проходить тесты в соцсетях, а также поделился мыслями о безопасности мессенджеров (InternetUA).

АиФ: Говорят, что вся техника с камерами – ноутбуки, планшеты, телефоны – следит за нами, снимает фото и видео, когда ей вздумается. Это правда?

Игорь Ашманов: Да. Не зря Марк Цукерберг, основатель Facebook, технически очень продвинутый человек, заклеивает камеру своем ноутбуке – и начал делать это еще 7 лет назад! Ваш телефон всегда вас «слушает», всегда определяет ваше местоположение, и постоянно смотрит в камеру на вас – даже когда, казалось бы, не активен. При этом телефон понимает, если снимок сделан в кармане, и на экране темно. Снимки же с лицами, людьми, какие-то ситуациями аппараты отправляют на «центральные сервера» – кто выгодоприобретатели этой информации, можно только предполагать... К данным с аппаратов с Android имеют доступ не только производители телефона, но и АНБ, которому владелец ОС обязан отдавать данные по закону.

АиФ: Выходит, нужно выключать телефон, когда им не пользуешься?

Игорь Ашманов: Это не поможет. Надо понимать, что каналов слежки много. Надо стараться не совершать ничего компрометирующего. Потому что даже если вы считаете, что телефон выключен, далеко не факт, что это так. Гарантия отключения – съем батареи с аппарата. Почти все современные телефоны имеют несъёмную батарею. С выключением тоже не всё просто: аппарат может проигрывать вам анимацию выключения и гасить экран – но оставаться активным. Есть другой вариант, как осложнить слежку – купить «бабушкофон» вроде Nokia 6610 и не пользоваться смартфонами.

Сам Ашманов пользуется одним из последних смартфонов Galaxy, но камеры нам нем не заклеивает. Специалист считает, что ему это не нужно: прослушка и слежка несет непосредственный риск для людей, которые имеют дело с какими-то тайнами. Это чиновники, представители спецслужб, крупные бизнесмены и преступники. Сервера же собирают массивы данных, не выделяя из них конкретно вас как личность.

Игорь Ашманов: В любом случае я стараюсь не использовать смартфон в специфических ситуациях: на переговорах, в сауне, спальне и т. п.

АиФ: Говорят, мессенджеры (Telegram, WhatsApp, Viber) шифруют информацию – и в отличие от смс и электронной почты они безопаснее. Это так?

Игорь Ашманов: Не уверен. Этого никто не может знать доподлинно. Это же маркетинг. Надежный ли алгоритм шифрования, на чьих серверах и в каком виде хранится ваша переписка? Простой пример: знаете, что публичная почта (например, Google) «читает» содержимое ваших писем? Она предлагает вам рекламу того, о чём шел разговор в письмах. А Google по закону обязан отдавать данные разведке. Аналогично устроены все коммуникационные сервисы: конечно, читают не живые люди, а искусственный интеллект с лингвистическим анализом. А операционная система Windows-10 в изначальной поставке имеет встроенного клавиатурного шпиона, который все ваши нажатия клавиш отправляет в Microsoft.

АиФ: В соцсетях постоянно расшаривают тесты: каким вы будете в старости, какая вы собака... При этом для получения результата нужно предоставить доступ к данным профиля. Это безопасно?

Игорь Ашманов: Выкачать публичный профиль можно и внешними программами. Опасность тестов, на мой взгляд, в другом. Это массовая дрессировка людей, натаскивание их на выполнение чего-то по команде. Механизм прост: большинству людей не хватает внимания к себе, а тут из говорят, что ты талантливый кулинар или похож на знаменитость. Приятно! Какое ты животное, кем ты был в прошлой жизни – миллион идиотских результатов, которыми все делятся с друзьями. Дрессировка состоит именно в «поделиться». Такой же смысл несут флэшмобы: облей себя водой, или напиши, как тебя изнасиловали. Так тренируют бездумное массовое поведение, как у леммингов. Мне говорят – я делаю: все побежали, и я побежал. Тот, кто собирает массовые данные, ставит пометку: вот эти пользователи склонны вестись на массовые действия. Работа такая же, по сути, как в «группах смерти»

(которые далеко не самое страшное, что сейчас есть в сети). Дрессированным массам людей можно подкидывать задания всё сложнее, и они охотно их выполнят.

АиФ: Вы сказали, есть что-то страшнее «групп смерти». Что?

Игорь Ашманов: группы блатной романтики АУЕ, группы романтизации школьных расстрелов (по-английски «скулшутинга»). На самом деле, вот такая кибербезопасность должна волновать и семью, и государство в первую очередь. Когда пароль украли – это полбеды. А вот когда украли мозги – это гораздо хуже. Манипуляторов в сети сейчас тысячи, и они становятся все изощреннее. Проверяйте, чем занимаются в интернете ваши дети, в каких группах с кем они общаются, какие задания выполняют – это может спасти им жизнь.

В свою очередь мы хотим напомнить вам о важности сохранения конфиденциальности и личных данных. Нужно внимательно следить за тем, в какие сервисы и системы вы «выкидываете» информацию о себе. Хороший пример – история с приложением GetContact, которое хранит на своих сервера собранную информацию о пользователях (данные телефонной книги, аккаунтов в соцсетях, должностях и местах работы, фотографии, IP-адреса и записи телефонных разговоров) и оставляет за собой право передавать эти данные третьим лицам.

Это же касается и правил безопасности в магазинах приложений. Никогда не устанавливайте сомнительные программы, обещающие волшебные функции и возможности, недоступные в официальных клиентах каких-либо сервисов. На этот счет у нас тоже есть хороший пример: недавно в Google Play появилось приложение «Все банки в одном месте». Как выяснилось, это вирус, который крадет данные для доступа к банковским счетам жертв. В описании программы сказано, что оно избавляет пользователей от необходимости устанавливать несколько программ и позволяет управлять всеми финансами с помощью единого интерфейса. Оценки и отзывы к приложению были накручены, и за несколько дней его успели установить около 500 человек.

(вгору)

Додаток 17

19.03.2018

Уязвимость в функции «мастер-пароль» в течение 9 лет ставит под угрозу пользователей Mozilla

На протяжении последних девяти лет Mozilla использовала в своей функции «мастер-пароль» недостаточно надежное шифрование (InternetUA).

В Firefox и Thunderbird предусмотрена функция, позволяющая пользователям устанавливать мастер-пароль, играющий роль криптографического ключа для шифрования каждого пароля, сохраненного в браузере или почтовом клиенте. Данная функция получила хорошие отзывы ИБ-экспертов, поскольку без нее браузеры сохраняют пароли локально в незашифрованном виде, оставляя их уязвимыми для вредоносного ПО или

хакеров с физическим доступом к компьютерам жертв. Однако по словам создателя AdBlock Plus Владимира Паланта (Wladimir Palant), используемый функцией механизм шифрования ненадежен и может быть легко взломан с помощью брутфорса.

В ходе анализа исходного кода Палант обнаружил функцию sftkdb_passwordToKey(), преобразовывающую пароли в ключи шифрования, применяя хеширование SHA-1 к строке, состоящей из самого мастер-пароля и произвольных символов (соли). По словам исследователя, здесь и кроется проблема.

Счетчик цикла функции SHA-1 равен единице. Это значит, что она применяется только один раз, тогда как рекомендованным значением является 10000 (к примеру, в LastPass счетчик цикла равен 100000). Столь низкое значение существенно облегчает работу хакерам, которые могут осуществить брутфорс-атаку, расшифровать мастер-пароль, а затем и все зашифрованные с его помощью пароли.

Палант – не первый исследователь, обнаруживший данную проблему. Еще девять лет назад о ней сообщил Джастин Долске (Justin Dolske) сразу же после появления функции «мастер-пароль». Тем не менее, Mozilla не исправляла уязвимость до тех пор, пока недавно о ней снова не напомнил Палант. Как сообщили в компании, проблема будет исправлена с выходом нового компонента для функции «мастер-пароль» под кодовым названием Lockbox.

Счетчик цикла – термин, часто использующийся для обозначения переменной, контролирующей повторы выполнения циклов (конструкции языков программирования). Свое название термин получил благодаря тому, что в большинстве случаев использования этой конструкции ее результат записывается в некоторую переменную, принимающую в качестве значения набор целых чисел в определенной последовательности (например, начиная с 0 и заканчивая 10 с шагом приращения 1). Счетчики циклов изменяют свое значение при каждом прохождении цикла, подставляя уникальное значение для каждой отдельной итерации.

(вгору)

Додаток 18

20.03.2018

Что скрывается за красочными фасадами Facebook и Google

Как-то раз Джон Эванс (имя изменено) получил сообщение от своей начальницы в Facebook с новостью о грядущем повышении по службе. На следующий день они встретились, и по дороге в кабинет начальница нахваливала его работу. Однако когда молодой человек зашел в переговорную, куда его привели, он оказался лицом к лицу с «крысоловами» – сотрудниками секретной службы Facebook по борьбе с утечками и руководителем внутренних расследований Соней Ахуджа (Украинский телекоммуникационный портал).

Допрос был формальностью.

«Мы знаем, что это ты слил информацию прессе», – сказали ему.

В качестве доказательства Эвансу предъявили сделанные им снимки с экрана и ссылки, которые он просматривал. Также ему дали понять, что в курсе его переписки с журналистом, начатой еще до прихода на работу в Facebook.

«Какой-то ужас, сколько им известно. Попав в Facebook, ты сначала оказываешься в теплой, уютной атмосфере. Тебе говорят: “мы меняем мир к лучшему” и “нам не все равно”. Но стоит отношениям испортиться, как все моментально меняется, и вот ты уже перед “охранкой” Марка Цукерберга», – говорит молодой человек. На интервью The Guardian он согласился лишь на условиях анонимности.

Всем известные внешние атрибуты корпораций Кремниевой Долины: красочные велосипеды, настольный теннис, кресла-мешки и бесплатная еда – лишь рисованный фасад, за которым скрывается жесткий кодекс секретности. Чтобы не допустить краж интеллектуальной собственности или других преступлений, в ход идет целый арсенал – от поощрения фанатичной преданности до слежки, цифровой и физической, угроз юридической ответственности и выплат в виде акции с ограничениями (Прим. пер.:Restricted Stock Units (RSU) – схема поощрения, дающая сотруднику право на акции при выполнении определенных условий).

Между тем, эти же средства используются, чтобы пресечь публичные высказывания о компании штатных или контрактных сотрудников, пусть даже речь идет о них лично – об условиях работы, проступках или культурных противоречиях, с которыми они сталкиваются.

Пожалуй, больше других секретностью славится Apple. «Яблочная» корпорация тщательно скрывает грядущие новинки, а ее сотрудники подписывают специальные соглашения о неразглашении.

Google и Facebook, напротив, всячески подчеркивают свою открытость и прозрачность. Основатель и глава крупнейшей в мире соцсети Марк Цукерберг каждую неделю проводит собрания, на которых рассказывает тысячам сотрудников о планах корпорации и еще не представленных продуктах. К тому же, пользуясь внутренней версией Facebook, даже сотрудники младшего звена и контрактники могут видеть, над чем работают другие отделы.

«Когда ты попадаешь в Facebook, такая прозрачность просто шокирует. Тебе доступно столько всего, даже то, что тебе не нужно по работе», – рассказывает Эванс.

С одной стороны – колоссальное доверие, а с другой – расплата, грозящая тем, кто нарушит правила.

«Стоит только выйти за рамки дозволенного, и тебя раздавят, как букашку», – добавляет собеседник.

В 2015 году, после того, как в СМИ просочились слухи о новом интеллектуальном помощнике «М» для мессенджера Facebook Messenger, Марк Цукерберг на одном из еженедельных собраний оставил свою обычную любезность и пообещал многотысячной аудитории: того, кто допустил утечку,

найдут и выгонят. Неделю спустя на очередной встрече глава корпорации объявил: виновного поймали и уволили. Новость встретили аплодисментами.

А что же Google? Похожая история. Персонал пользуется внутренней версией соцсети Google Plus, а в обширной внутрикорпоративной рассылке обсуждаются самые разнообразные вопросы, от бытовых до социальных. По большей части сотрудники ведутся на лозунги о корпоративной миссии в атмосфере показного энтузиазма, царящей в кампусе, которая помогает воспитывать фанатичную приверженность и не допускает предательства. Также персонал поощряется годовыми бонусами в виде акции с ограничениями, что позволяет купить их молчание на годы вперед после ухода из компании.

«Ты никогда не сделаешь чего-то, что может помешать успеху компании, ведь это напрямую коснется и тебя», – говорил о существующем в Google давлении следовать определенным правилам бывший сотрудник корпорации Джастин Максвелл.

На принятый в Google уклад проливает свет и внутреннее письмо Брайана Катца, который ранее руководил в корпорации группой по расследованиям и борьбе с утечками. С декабря 2017-го он покинул Google и возглавил собственную компанию Lighthouse Global Solutions, специализирующуюся на расследованиях, защите интеллектуальной собственности и информационной безопасности.

«Прошу, помните: утечки, неважно, умышленные или непреднамеренные, подрывают нашу корпоративную культуру. Отдавайте себе отчет, с кем и какими сведениями о компании вы делитесь. Если вы думаете о том, чтобы раскрыть конфиденциальную информацию репортеру или кому-то за пределами компании – во имя всего, что ценно для Google, передумайте! Это не только может стоить вам работы, этим вы предадите ценности, делающие нас единым сообществом», – писал Брайана Катц в мае 2016 года.

Текст письма в 2017-м опубликовал портал The Verge в связи с судебным иском, в котором один из бывших гугловцев заявил, что был несправедливо уволен из-за подозрений в «сливе» информации, и обвинил Google в создании атмосферы чрезмерной секретности, страха и доносительства. Также в заявлении говорилось, что политика Google противоречит трудовому законодательству, согласно которому сотрудники имеют право обсуждать условия работы, уровень зарплаты и возможные правонарушения внутри компании.

На слуху и недавний скандал вокруг бывшего программиста Google Джеймса Деймора из-за разосланного им по внутрикорпоративной почте письма, суть которого сводилась к тому, что невысокая доля женщин среди руководства технологических компаний объясняется биологическими различиями между полами. За это письмо Деймор был немедленно уволен. В январе 2018-го вместе с другим экс-сотрудником Google Дэвидом Гудманом он подал на компанию в суд за дискриминацию приверженцев консервативных политических взглядов и мужчин европеоидной расы.

Еще один бывший гугловец, теперь управляющий собственным стартапом, в беседе с The Guardian заявил, что руководство Google годами мирилось со скрытыми сексизмом, предрассудками и другими проблемами. По признанию собеседника, лично ему пришлось испытать на себе крутой нрав вспыльчивого менеджера.

«Никто и пальцем не шевелил до тех пор, пока однажды вице-президент не увидел, как этот парень орет на меня в коридоре. Люди годами терпят подобное, пока им не приходит в голову мысль: “Если Google ничего не собирается предпринимать, мы расскажем об этом”».

Контрактников, на которых ИТ-гиганты сгружают низкооплачиваемую рутину, держать язык за зубами принуждают чаще кнутом, чем пряником. Отсутствие опционов на акции и корпоративного духа с лихвой компенсирует страх потерять работу.

Журналисты The Guardian ознакомились с договором одного из европейских контрактных служащих Facebook, занятых в модерации контента. Согласно документу, корпорация вправе следить за его активностью в социальных сетях, включая личный аккаунт в Facebook, а также контролировать его переписку по электронной почте, телефонные звонки и действия в интернете. Кроме того, контрактник согласился на досмотр своих личных вещей, сумок, портфелей и салона автомобиля, пока он находится на территории компании. Отказ от обыска считается грубым нарушением контракта.

Контроль за тем, что фотографируют контрактники и какие документы распечатывают, тоже обычная практика. Еще один распространенный прием проверки лояльности – подкинутые службой безопасности «мышеловки» в виде USB-накопителей, будто бы случайно забытых.

«Если попадается флэшка или нечто подобное, надо ее сразу отдать. Стоит подключить накопитель к компьютеру, об этом сразу же узнают и тут же выпроводят вон. Доходило до паранойи: мы использовали код в сообщениях, если нужно было обсудить что-то по работе и говорили на эту тему только при личной встрече», – рассказал Guardian один из бывших контрактников Facebook.

Некоторые из работников Facebook опасаются слежки. В феврале 2018-го интернет-издание Wired опубликовало статью по материалам интервью с бывшими и действующими сотрудниками соцсети, и один из собеседников попросил журналиста выключить смартфон перед разговором, чтобы компания не узнала о встрече с репортером.

В Facebook, конечно, заверяют, что не используют таких методов.

«Мы не отслеживаем местонахождение наших сотрудников по их мобильным телефонам. Также мы не следим за репортерами или другими людьми, не работающими в Facebook», – заявил пресс-секретарь корпорации Берти Томсон.

Между тем, The Guardian утверждает, что ИТ-гиганты устраивают негласное наблюдение за сотрудниками с помощью детективных агентств, и

даже называет одну из таких фирм под названием Pinkerton, в списке клиентуры которой числятся Google и Facebook.

Наряду с прочим, агенты Pinkerton посещают кафе и рестораны поблизости с кампусами корпораций, чтобы подслушивать разговоры сотрудников.

«Если мы слышим разговоры о готовящихся к выходу продуктах, новых направлениях бизнеса или акциях, мы передаем эту информацию службе безопасности компании», – рассказал управляющий директор Pinkerton Дэвид Давари. Он также добавил, что основной упор делается на то, чтобы не допустить кражу интеллектуальной собственности и инсайдерской торговли.

Facebook и Google отрицают подобную практику.

Что интересно, просмотрев профили LinkedIn, журналисты выяснили: несколько бывших агентов Pinkerton впоследствии перешли на работу в Facebook, Google и Apple.

В качестве резюме в статье приводится комментарий директора по вопросам неприкосновенности частной жизни Стэнфордского центра Интернета и общества (Stanford Center for Internet and Society) Альберта Джидари. Специалист назвал типичными и распространенными методы корпораций, отметив, что они вполне легальны, хотя и вторгаются в частную жизнь.

«Компании обязаны предпринимать меры для выявления и предотвращения преступлений, и нет ничего удивительного в том, что они используют такие способы для контроля за соблюдением сотрудниками контрактных обязательств», – добавил эксперт.

(вгору)

Додаток 19

19.03.2018

Атаки вымогателей становятся все более разрушительными и направлены в основном на бизнес-сегмент

Microsoft выпустила глобальный отчет по информационной безопасности Microsoft Security Intelligence Report volume 23. Свежий выпуск включает данные, собранные с февраля 2017 г по январь 2018 г. Эксперты проанализировали миллиарды анонимных сигналов об угрозах безопасности сервисов и продуктов Microsoft, включая Windows, Bing, Office 365 и Azure. Эти сервисы ежемесячно сканируют 400 млрд электронных писем на фишинг и вредоносное ПО, обрабатывают 450 млрд аутентификаций, проверяют более 18 млрд веб-страниц (Компьютерное Обозрение).

Судя по собранным данным, бот-сети продолжают воздействовать на миллионы компьютеров по всему миру, заражая их вредоносными программами. Боты используются в качестве инфраструктуры распространения таких программ с бизнес-моделью «оплата за установку». В ноябре Microsoft обнаружила крупнейшую в мире бот-сеть Gamarue, которая распространяла

более 80 различных семейств вредоносных программ. После разоблачения число заражений уменьшилось на 30% всего за три месяца.

Хакеры предпочитают простые и недорогие методы атак, такие как социальная инженерия, – в противовес более дорогостоящим попыткам обойти меры безопасности жертвы. Выявив точку опоры, злоумышленники разворачивают специальные вредоносные программы, адаптированные к целевому устройству. В период с июня по декабрь 2017 г. именно фишинг составил более 50 % всех атак, нацеленных на Office 365. С октября 2017 г. по январь 2018 г. было выявлено, что 79 % облачных приложений для хранения данных и 86 % облачных приложений для совместной работы не шифруют информацию.

Вымогатели проводят все более стремительные и разрушительные атаки, направленные главным образом на бизнес-сегмент. Наибольшее количество таких случаев – в Мьянме, Бангладеш, Венесуэле, Пакистане, Индонезии и Украине. При выборе страны злоумышленники оценивают разные факторы, такие как уровень ВВП, средний возраст пользователей интернета, доступные в регионе платежные средства. WannaCrypt, Petya/NotPetya и BadRabit – недавние примеры того, как вымогатели приобретают влияние над своими жертвами не только в рамках цифрового мира.

Подводя итог, в компании отмечают, что все эти угрозы – взаимосвязаны. К примеру, именно вымогательство было одним из самых известных типов вредоносных программ, распространяемых бот-сетью Gamarue. Другой пример: киберпреступники используют законные возможности платформы, чтобы прикрепить документ (например, документ Microsoft Office), содержащий вымогательство в фишинговом электронном письме.

(вгору)

Додаток 20

19.03.2018
Как отличить бота от человека?

Интернет превратился в огромную коммуналку, где с одного адреса может писать и человек, и бот, мечтающий заразить сервис. Решение проблемы – сервис IPv6, но он имеет свои недостатки (InternetUA).

«Докажите, что вы не робот». Уверен, многим из вас порядком надоело назойливое предложение Google, «Яндекса» или другого интернет-ресурса подтвердить, что вы человек. Многие пользователи, жалующиеся на появление так называемой «капчи» (CAPTCHA, Completely Automated Public Turing test to tell Computers and Humans Apart), считают, что виноваты в появлении этих сообщений сами интернет-сервисы, которые только усложняют жизнь простых посетителей. На самом деле это не так: Google, «Яндекс» и другие ресурсы, использующие CAPTCHA, не виновники, а пострадавшие, и ответственность за происходящее здесь полностью лежит на операторе связи, который

предоставляет пользователям услугу доступа в интернет. Казалось бы, какая связь между интернет-провайдером и веб-страницей?

Коллективная ответственность

Использование теста CAPTCHA необходимо, чтобы защитить ресурсы поисковиков и других интернет-компаний от недружественных ботов, которые процветают в сетях операторов связи. Помимо сервисных программ, посещающих сайт, например, с исследовательскими целями, многих ботов создают злоумышленники, чтобы похищать контент интернет-компаний или организовать DDoS-атаку, при которой сервер перестает работать. Веб-ресурсы умеют обнаруживать такую атаку и, чтобы защититься, заблокировать передачу данных с определенных IP-адресов. Но когда их не хватает, операторы за одним IP скрывают несколько пользователей одновременно, среди которых могут находиться и вредоносные боты, и добропорядочные пользователи. Чтобы не отрубать всех, приходится раз за разом просить разгадать непонятно написанную комбинацию букв и цифр.

IP-адрес – это максимально точный адрес в сети, а значит, все сущности, «живущие» за этим адресом, для веб-ресурсов не различимы. Отсюда оборонительные действия со стороны поставщиков контента.

Почему же не выдать каждому пользователю по своему IP-адресу, чтобы ресурсы могли оценивать деятельность каждого пользователя, не заставляя его отвечать за «соседа»? Когда интернет только задумывался, в текущем его виде под адресацию было выделено 32 бита, ограничивающих адресное пространство 4 294 967 296 возможными уникальными IP-адресами. Казалось бы, очень много, но это даже меньше, чем живет на Земле людей. А учитывая, что на одного человека сегодня приходится как минимум три-четыре подключенных к сети устройства, то становится очевидно, что в интернете уже давно кончились адреса. Поэтому все операторы связи вынуждены использовать механизм NAT (Network Address Translation), который позволяет одним IP-адресом или пулом адресов пользоваться нескольким десяткам тысяч конечных пользователей одновременно.

IPv6 для улучшения жилищных условий

О том, что адреса в Глобальной сети закончатся, было понятно еще в момент зарождения коммерческого интернета в девыностые годы прошлого столетия. В тот момент стало ясно, что интернет – это коммерчески успешный проект и пользоваться им будут не только университеты, военные и исследовательские учреждения, как это изначально задумывалось, но и бизнес и обычные пользователи. А значит, адресного пространства на всех явно не хватит. Чтобы решить эту проблему, было принято решение заменить основной и обслуживавший большую часть сети интернет-протокол IPv4 (Internet Protocol version 4) на новую версию. Изначально она называлась IPng (Internet Protocol next generation) и была утверждена в 1995 году, впоследствии став современным IPv6 – интернет-протоколом версии 6 (так случилось, что цифра 5 была уже занята).

Новая версия протокола IP была призвана решить проблемы, с которыми столкнулась предыдущая – IPv4, то есть расширить адресное пространство, чтобы IP-адресов хватило на всех. Эта задача была решена триумфальным образом. Вместо длины адреса в 32 бита IPv6 предлагает 128 бит, а значит, новый протокол может обеспечить до 340 282 366 920 938 463 463 374 607 431 768 211 456 адресов. На самом деле не все из них могут использоваться («всего» 4,2×1037), но можно с уверенностью утверждать, что адресов теперь хватит на всех.

Помимо расширения адресного пространства, IPv6 обладает еще несколькими улучшениями по сравнению с IPv4, которые сделают логику маршрутизации проще. К тому же он улучшает совместимость с мобильными сетями, например, избавит от использования технологии NAT.

Трудности переходного этапа

Невооруженным глазом видны значительные преимущества нового протокола, однако статистика говорит нам следующее: по состоянию на конец 2017 года, согласно данным APNIC, доля IPv6 в общем сетевом трафике составляет лишь 14 %. Что же препятствует массовому использованию новой версии протокола, если она столь хороша?

Замена базового протокола сети IPv4 в тот момент, когда он находится в фазе активной эксплуатации, без остановки сервисов – совсем не тривиальная задача. Много времени и сил инженерного сообщества тратится на разработку стандартов и обдумывание процесса перехода с IPv4 на IPv6, что может занять годы.

С точки зрения бизнеса, переход на IPv6 – весьма дорогостоящий процесс, он требует значительных инвестиций, отдача от которых неочевидна. Потому не все компании поддерживают идею миграции на новый протокол, ведь зачем тратить силы и средства на модернизацию, если IPv4 пока еще работает?

Но долго откладывать переход не удастся: адресное пространство IPv4 закончилось еще в 2012 году, и сейчас оно продается на биржах. Если еще в начале 2017 года стоимость одного IP-адреса составляла порядка $10, то сейчас возросла в 2,4 раза – цена за IP-адрес превышает $24. Напомню, что всего адресов IPv4 4,3 млрд, а значит, это потенциально рынок в миллиарды долларов, фактически основывающийся на продаже «воздуха». Например, Microsoft приобрела в компании Nortel 666 000 IPv4-адресов за $7,5 млн. По сравнению с торговлей адресным пространством биткоин становится куда менее абстрактным предметом.

В результате закончившееся адресное пространство и растущая стоимость IP-адресов все-таки вынуждают операторов связи, в особенности мобильных, чья аудитория растет рекордными темпами, постепенно мигрировать на IPv6. В Северной Америке, например, этот процесс не просто запущен, а уже находится в стадии активного развертывания: уже 12 крупнейших операторов полностью перешли на IPv6. От Америки не сильно отстает Китай, где адресное пространство IPv4 закончилось раньше всего.

Согласно плану Коммунистической партии, к 2025 году должна произойти полная миграция на новый протокол: все сети, приложения и терминальные устройства Китая должны будут полностью поддерживать IPv6.

IPv6 – не панацея

Казалось бы, вот оно счастье, скоро IPv6 придет в каждый дом, решив кризис адресного пространства и принеся благо даже конечным пользователям. Но не тут-то было. Как любая новая технология, решая одни проблемы, она неизбежно создает другие. Достаточное количество IP-адресов будет означать, что все устройства, подключенные к домашнему роутеру или к сети мобильного оператора, будут иметь выход в интернет и смогут инициировать «общение» с сетью по своему усмотрению. Следовательно, пакет, посланный холодильнику, чайнику, телевизору, будет обработан сетью и передан на это устройство, и при наличии уязвимостей в прошивке (а их в «умных» гаджетах масса) хакеры смогут использовать их для вредоносной активности.

Если в 2016 году первый ботнет интернета вещей работал преимущественно на камерах видеонаблюдения, число которых достигало 25 000, то теперь к ним добавятся и другие устройства, подключенные к интернету. По факту они лишаются уровня защиты, который давал им механизм Network Address Translation: NAT работал как диод, то есть выпускал исходящий трафик, но не впускал входящий. Теперь такая «подушка безопасности» отсутствует, и операторам связи, как и простым пользователям, придется осваивать новые правила цифровой «гигиены» при работе с новым протоколом IPv6.

Пользователям необходимо всерьез задуматься о безопасности своих «умных» вещей: обязательно изменять установленные по умолчанию пароли (по данным компании Trustlook, более трети (35 %) владельцев устройств не меняют пароли по умолчанию, а 54 % пользователей не устанавливают никакое программное обеспечение для защиты устройств от кибератак), регулярно устанавливать обновления прошивок и приобретать устройства только у проверенных производителей. В свою очередь, операторы, если они хотят позаботиться о своих пользователях, должны производить фильтрацию всех входящих соединений, чтобы отсеивать нелегитимный трафик.

Наблюдая за развитием современных технологий и техник кибератак, можно сказать, что цифровой апокалипсис надвигается неумолимо и неизбежно. Сети, в которые входят миллионы зараженных устройств, становятся поистине разрушительной силой. Небезопасные устройства интернета вещей, подключенные к IPv6, и соединенные по высокоскоростным мобильным сетям передачи данных, выглядят как идеальный шторм для нового интернета версии 6.

(вгору)

Додаток 21

19.03.2018

Хакерская группировка Fancy Bear провела новую шпионскую кампанию

Исследователи безопасности из компании Palo Alto Networks сообщили о новой фишинговой кампании, за которой стоит хакерская группировка Fancy Bear, предположительно связанная с властями РФ (InternetUA).

По словам исследователей, активность хакеров была зафиксирована дважды, 12 и 14 марта 2018 года. Для осуществления атак группировка использует обновленную версию платформы DealersChoice, которая эксплуатирует уязвимость в Adobe Flash для скрытой доставки вредоносного ПО.

Обновленная версия DealersChoice использует новую технику ухода от обнаружения. В частности, вредоносный модуль загружается только тогда, когда просматривается конкретная страница вредоносного документа, содержащегося в фишинговых письмах.

Жертвой фишинга стала некая европейская правительственная организация (название не раскрывается). Сотрудники организации получили письма с темой «Оборона и безопасность 2018». Письма содержат документ MS Word, озаглавленный «Defence & Security 2018 Conference Agenda.docx».

Как отметили исследователи, атакующие полностью скопировали повестку дня реальной конференции, которая состоится в Великобритании. Если пользователь открывает вложение Microsoft Word, объект Flash, содержащий вредоносный скрипт, пытается установить полезную нагрузку, однако скрипт запускается только в том случае, если жертва прокрутит документ до третьей страницы.

«Судя по всему хакеры уверены в том, что их цели будут достаточно заинтересованы в содержании, чтобы прокрутить документ до 3 страницы», – отметили эксперты.

По словам специалистов, вредоносный Flash-объект не запускается до тех пор, пока пользователь не дойдет до третьей страницы, поскольку SWF-загрузчик DealersChoice не активируется до тех пор, пока не появится на экране. Данная тактика помогает вредоносу избежать обнаружения. Вредоносный Flash-объект отображается как маленькая черная точка, которую многие пользователи могут просто не заметить.

После активации Flash-объект связывается с C&C-сервером для загрузки дополнительного вредоносного ПО, которое содержит код эксплоита.

Исследователи связали данную кампанию с Fancy Bear, поскольку в свойствах документа имя пользователя, в последний раз вносившего изменения, было обозначено как Nick Daemoji. Данное имя пользователя фигурировало в предыдущих кампаниях Fancy Bear.

(вгору)

Додаток 22

20.03.2018

Новый вид мошенничества: хакеры начали продавать селфи своих жертв

Согласно отчету в NextWeb, израильская компания Sixgill, занимающаяся веб-исследованиями Даркнета, обнаружила большой объем сомнительного контента, среди которого были селфи пользователей. Алекс Карлински из Sixgill заявил, что компания столкнулась с рекламой на форуме с закрытым доступом, в которой преобладает русский язык. Кто-то продавал 100 тыс документов за $50 тыс. В сообщении было указано, что пакет документов включал удостоверение личности или паспорт, подтверждение адреса и селфи, что достаточно необычно для подобных объявлений (InternetUA).

Это, по-видимому, является одним из первых случаев, когда в набор данных было включено личное фото жертвы. С одной стороны селфи, сами по себе, не несут большой ценности для хакеров. Но с другой стороны, в сочетании с другой идентифицирующей информацией, эти безобидные на первый взгляд фото могут позволить хакерам открывать банковские счета и получать кредиты под именем жертвы. Это обусловлено тем, что некоторые банки позволяют клиентам открывать учетную запись с помощью загруженных документов онлайн. В таком случае селфи может использоваться как средство проверки и подтверждения личности.

Продавцы Даркнета, по словам экспертов Sixgill, зачастую выставляют не очень высокую цену на подобный вид данных – идентификационные документы человека и селфи можно приобрести всего за $70. На вопрос, как частные фото попадают в руки преступников, Алекс Карлински ответил, что самый простой способ получить селфи – украсть их из телефонов, заразив их вредоносным ПО. Также он добавил, что современные хакеры не ограничиваются каким-то одним способом кражи информации, и есть еще много вариантов незаконно завладеть личными данными.

(вгору)

Додаток 23

20.03.2018

Беззащитные данные: как Facebook оказалась в центре самого большого скандала в истории

Cambridge Analytica придумывала, как высасывать из пользователей Facebook максимальное количество информации: она делала всевозможные веселые приложения и тесты, а потом составляла профили, помогающие манипулировать людьми (InternetUA).

Акции Facebook падают – с 19 марта капитализация компании «провалилась» на $40 млрд. Причина – масштабный и нехорошо пахнущий скандал: бывший сотрудник компании Cambridge Analytica (далее CA) Крис Уайли (Chris Wylie) дал интервью The Guardian, в котором признался, что

компания использовала данные пользователей Facebook без их ведома, для профилирования и «промывания мозгов».

А конкретно – для активной доставки контента, влияющего на решения людей, в том числе во время выборов президента США. Крис признался, что покровителем затеи был не кто иной, как Стив Бенон, доверенный советник Трампа, и именно он придумал проекту название «psychological-warfare mindfu@k tool» (если смягчить перевод – «инструмент для запудривания мозгов»). Об этой истории на данный момент написала практически вся западная пресса: The Guardian, NY Times, Observer, и маятник только начинает раскачиваться, ибо все вопросы, которые витали в воздухе относительно понятия «приватность» внезапно стали как никогда актуальными и наглядными. Оказалось, что как минимум одна коммерческая компания может влиять на то, кто будет президентом любой развитой страны.

Ситуация очень сложная с технической точки зрения, поэтому большинство спикеров не комментируют, что, собственно, произошло и почему это настолько важно, что инвесторы сбрасывают акции Facebook. Мне кажется, важно объяснить суть, а для этого вспомним порядок событий. Изложение сознательно упрощено, чтобы не уходить в технические дебри:

1) Компания Cambridge Analytica во главе с CEO Александром Никсом (Alexander Nix) понимает, что данные о человеке можно использовать для манипуляции общественным мнением.

2) Компания поднимает инвестиции, нанимает инженеров, чтобы сделать программное обеспечение, способное анализировать поведенческие данные человека: что пользователь пишет в интернете, с кем общается, его лексикон, маршруты движения, предпочтения в литературе, фильмах и музыке и т. д. На основании этих данных делаются конкретные заключения: что надо сказать человеку и в каких выражениях/форме, чтобы он поверил и отреагировал предсказуемо – так, как надо заказчику.

3) Компания проводит тесты своего софта и понимает, что она не ошиблась: условно, если холерикам и сангвиникам, собирателям и революционерам давать разный контент и упаковывать одни идеи в разные сообщения – кому-то видео чиновника со скрытой камеры, кому-то скриншот почтового ящика Хилари Клинтон, кому-то подкаст никому не известного блогера, – люди реагируют с потрясающим уровнем конверсии (соотношение кликов к количеству показанной рекламы).

В CA понимают – это золотая жила, но для того, чтобы развернуться, им нужно еще больше данных о людях.

4) Cambridge Analytica придумывает ход конем, чтобы высасывать из пользователей Facebook максимальное количество информации: о них, их друзьях и знакомых, а главное – дополнительную личную информацию для составления психологического портрета пользователей. Они своими руками и руками внешних подрядчиков начинают делать всевозможные веселые приложения и онлайн-тесты, пройдя которые, можно узнать, условно, «кто ты

во «Властелине колец» и «кто ты на самом деле по гороскопу», и поделиться смешным рейтингом с друзьями.

Затея срабатывает – люди не чуют подвоха, соглашаются на любые условия работы приложения и начинают отдавать кучу личной информации о себе и своих друзьях. Эти приложения по сути представляют собой психологическое анкетирование (до 2015 года это было возможно в космических масштабах и почти без ограничений, в 2015-м Facebook изменил свой API и запретил приложениям собирать большую часть информации о «друзьях друзей», но это драматично не повлияло на бизнес CA, ибо их главный конек был и остается в социальном инжиниринге).

5) Помимо FB компания Cambridge Analitica покупает данные у дата-брокеров (на рынке более 2000 компаний, в том или ином виде специализирующихся на перепродаже наших данных – истории покупок, истории поиска и веб-серфинга и т. д.). Сопоставляя данные профилей FB, покупную информацию и данные из «веселых» приложений и «даркнета», где публикуют, например, украденные хакерами базы данных, они получают возможность делать предсказания о конкретных людях с колоссальной точностью.

По исследованиям компании Biolink, всего можно выделить 14 типов данных. Например, чтобы вы понимали возможности: с высокой достоверностью даже по анонимным данным можно определить пол человека, расу, профессию, социальный статус и примерный уровень доходов. А также личные качества: гей или натурал, изменят жене/мужу или нет, за кого будет голосовать из списка кандидатов, шовинист или нет, расист или нет, правые или левые взгляды – список классификаций почти бесконечный.

Как писал Джордж Оруэлл, «кто контролирует прошлое, контролирует будущее». И тут это как нельзя точно описывает суть – если ты знаешь, что делал человек последние 10 лет, ты почти гарантированно сможешь сказать, что он будет делать завтра.

6) CA убедилась, что машинка по поиску целей работает. С каналами доставки мозговых бомб тоже все было понятно – социальные сети. Осталось решить простую проблему – контент. Они начали в прямом смысле планировать кампании по изменению общественного мнения через компромат, настоящий и выдуманный контент, компрометирующий или, наоборот, выставляющий в хорошем свете конкретного человека или фракцию. Гендиректор компании открыто признался в одном из своих интервью – «не важно, правдива новость или нет, если в нее поверят». Это в сути своей отражает бизнес-модель CA: собрать базу из 50 млн человек, разбить их по типам, понять цель заказчика и начать одним людям скармливать одно, другим – другое, третьим – третье, чтобы все начали ругаться друг с другом, но в сухом остатке была достигнута цель – победа кандидата X на выборах или принятие решения на референдуме по выходу Англии из Евросоюза. Автор не утверждает, что в CA это сделали, лишь указывает, что у них могла быть такая возможность, компания открыто продавала свои услуги на рынке.

The Guardian упоминает о том, что они делали питч даже компании «Лукойл», которая не совсем поняла, как их возможности связаны с нефтяным бизнесом, и якобы на этом разговор и закончился. Зная косность и консервативность нефтянки и то, как «быстро» они принимают стратегические решения вне своей прямой экспертизы, полагаю, что «Лукойл» – ложный след. Это лишь пример разнообразия клиентской базы CA.

7) Facebook напряглись, что у них в пуле есть партнер, который высасывает из их абонентской базы столько данных. По заявлению вице-президента Facebook Пола Греваля (Paul Grewal), FB отрезал CA доступ к данным после изменения правил в 2015-м. Он четко обозначил позицию: мол, они нарушили наше лицензионное соглашение, и мы потребовали письменных доказательств, что данные, полученные о наших пользователях, уничтожены. Были ли они уничтожены на самом деле – неизвестно, но в этом сейчас будет разбираться экспертная группа, автор уверен, что власти UK и EU выдадут соответствующий ордер.

8) Отписавшись в Facebook, мол, все окей, не переживайте, Cambridge Analytica не просто не прекратила своей деятельности, она, наоборот, ее стала наращивать и применять новые инструменты сбора данных, часто противоречащие политике самой Facebook. Крис Уайли признался:

«Мы использовали несовершенство программного обеспечения Facebook для сбора миллионов пользовательских профилей и построения моделей, которые позволяли нам узнавать о людях и применять эти знания для активации их внутренних демонов».

Бесплатные соцсети. Дорого

В сухом остатке совершенно неважно, докажет расследование, что CA нарушили правила работы Facebook, или окажется, что Facebook, например, не просто не мешала, но и помогала их деятельности. Существует одна компания, которая сосредоточила в своих руках знания о поведении 2 млрд человек.

Эти знания компания, ее легальные партнеры и не ограниченные законом хакеры и преступные группировки могут использовать для изменения исхода любого голосования, отношения к совершенно любому тезису, человеку или компании.

Мы видим, что социальные сети совсем не бесплатные. Наши данные стоят денег, и немалых: Facebook зарабатывала на рекламе около $40 млрд в год, а сколько заработала CA на выборных кампаниях – страшно подумать (только на предвыборную компанию в интернете штаб Трампа затратил $58,6 млн).

Монополия Facebook на наши «цифровые ДНК» (следы, которые пользователь оставляет в интернете) стоит поперек горла всем. Бизнесы подсаживаются на рекламные ковровые бомбардировки, как на героин, люди устают смотреть рекламу вещей, которые им не нужны, государства в силу своей природы ищут баланса сил на уровне ООН, а FB очевидным образом придает больше силы США. И не все в США этому рады: в Америке живет и работает огромное количество блестящих специалистов и потрясающих,

добрых, открытых людей, реально ставящих нужды планеты выше своих собственных. Не надо судить о США по поведению политиков, так же, как многие американцы не судят о России по передачам российского телевидения.

На данный момент Марк Цукерберг не дал ни одного комментария о ситуации, что выглядит крайне странно, особенно на фоне пикирующего курса акций. Как сообщил Marketwatch, оказывается, Марк в последние дни активно распродавал собственные акции, полагаю, он это делает осознанно, понимая будущую силу только начинающегося скандала.

Осенью 2016 года автор этого текста выступал на TEDx с темой важности «цифрового ДНК» и опасности управления с его помощью общественным мнением. По итогам в числе прочего пришлось выслушать массу критики в духе «не надо выдумывать проблему там, где ее нет. Не существует такой проблемы, как приватность, потому что данные – это собственность бизнесов».

Надеюсь, теперь многие увидят, как жестоко ошибались. Рад, что эта ситуация стала публичной и вопрос прав человека на владение своими данными неизбежно будет обсуждаться на уровне глав государств.

И о важном. Заявление, что данные применялись «без ведома пользователей», технически не соответствует действительности.

Пользовательское соглашение Facebook устроено таким образом, что единожды кликнув «я согласен», вы навсегда прощаетесь со всеми (!) правами на свои посты, фото, поведенческие данные, историю маршрутов и все косвенные заключения, которые можно сделать на основе этих данных.

Например, не удивляйтесь, если Facebook соберет из ваших данных бота с вашим лицом и начнет вашим друзьям продавать что-то. Это не будет нелегальным. Уверен, сложившаяся ситуация наконец всех отрезвит и подходы к данным в мире начнут меняться.

(вгору)

Додаток 24

20.03.2018

Украинские хакеры начали вымогать выкупы в биткоинах

В Украине киберпреступления все чаще совершают при помощи самых обычных устройств. На днях полицейские в Хмельницком поймали злоумышленника, который обворовал нескольких граждан с помощью их же мобильных телефонов. Как рассказала спикер хмельницких копов Инна Глега, 24-летний подозреваемый обогатился как минимум на 30 тыс. грн (InternetUA).

«Этот парень, ранее уже судимый за кражи, пользовался доверием случайных людей. Он просил у них мобильный телефон якобы для того, чтобы сделать срочный звонок. Взяв телефон, он заходил в мобильное банковское приложение (если номер, конечно, был привязан к банковской карте. – Авт.), менял пароль доступа и быстро перечислял деньги с чужого счета на свою карту. После этого возвращал телефон ничего не подозревающей жертве», – рассказала «Сегодня» Инна Глега.

К этому полицейские добавили, что вычислили подозреваемого, отследив похищенные средства. Парень задержан, ведется следствие, подозреваемого проверяют на причастность к подобным преступлениям. Ему грозит до 5 лет тюрьмы.

Впрочем, это еще мелочь.

«На протяжении нескольких месяцев в киберполицию с жалобами на хакеров-вымогателей обращаются представители государственных и частных финансовых учреждений, транспортных компаний, госучреждений и интернет-провайдеров», – заявил департамент киберполиции Нацполиции.

И добавляют:

«Жертвам, от имени так называемой хакерской группы LizardSquad, на электронные почтовые ящики приходят письма с сообщением, что их предприятие выбрано для следующей DDoS-атаки. Для того чтобы избежать блокирования работы, жертвы должны заплатить хакерам 3 биткоина».

Курс биткоина сегодня составляет $7818, то есть хакеры требуют со своих жертв почти $24 тыс. (около 600 тыс. грн).

В киберполиции пытаются установить личности шантажом. При этом копы обращают внимание, что, если предприниматели и заплатят хакерам выкуп, то все равно не получат полной гарантии того, что избегут их атаки.

«Уплата этих денег лишь финансирует дальнейшую деятельность злоумышленников и подтверждает правильность выбранной схемы шантажа», – говорят полицейские.

А в Полтаве на днях пытался выйти на свободу 35-летний подозреваемый в хакерстве Геннадий К., за которым охотились полицейские сразу 30 стран и который был арестован в конце февраля. Он обжаловал решение об аресте в Апелляционном суде. Впрочем, суд отказал ему в этом и оставил на время следствия за решеткой. Напомним, полицейские подозревают его в том, что мужчина якобы является организатором интернет-платформы, которая могла за один день заразить вирусами до 500 тыс. компьютеров. Украинские силовики инкриминируют ему покушение на убийство правоохранителя в момент задержания.

(вгору)

Додаток 25

21.03.2018

Ваш гаджет захватили майнеры. Что делать?

Майнеры атакуют! В последнее время они стали самым активным типом вирусов. Даже красть данные с серверов крупных корпораций сегодня не так выгодно, как скрыто майнить на этих мощностях (InternetUA).

Впрочем, компьютерам и смартфонам рядовых пользователей тоже достаётся. Рассказываем, как не стать жертвой скрытого майнера.

Майнер в браузере

Бывает, заходишь на сайт, а он «вешает» весь компьютер. Что происходит? Есть вероятность, что на сайте запущен особый скрипт, который жрёт ресурсы вашего компьютера ради пары монет для «дяди».

Майнят чаще всего Monero (XMR), реже – Zcash и другие анонимные криптовалюты.

Майнеры могут внедрить хакеры или же сами владельцы сайта. Таким не побрезговала даже The Pirate Bay. Правда, вскоре майнер «бухта» всё же убрала.

Вирусы для майнинга на компьютерах

Цель вредоносов такого рода – сделать ваш компьютер частью ботнета, который объединяет мощности сравнительно слабых устройств для майнинга и решения других задач. Это вдвойне выгодно: во-первых, злоумышленникам не нужно покупать дорогие майнеры или видеокарты, во-вторых – платить за электричество тоже не придётся.

Часто злоумышленники используют легальные майнеры. Но устанавливают их без ведома владельца устройства, скрывают работу майнера и указывают свой кошелёк для добытых монет.

Обычно майнер попадает на компьютер с помощью дроппера. Этот вредонос нередко кладут в состав пиратских версий популярных программ или генераторов ключей активации. После запуска файла на компьютер жертвы ставится установщик, который непосредственно скачивает майнер и утилиту для его маскировки в системе.

Часто в комплект кладут инструменты для автозапуска вредоноса и настройки его работы. Эти сервисы могут приостанавливать работу майнера, когда пользователь запускает игру или другое ресурсоёмкое приложение. Так майнер не выдаст себя и проведёт на компьютере жертвы максимум времени.

Современные майнеры способны самовосстанавливаться, останавливать работу антивируса, мониторить активность системы и майнить только в периоды низкой нагрузки.

Устранение конкурентов

Майнеры обычно запускают в оперативной памяти процессы с именами вроде как Silence, Carbon, xmrig32, nscpucnminer64, mrservicehost, service, svchosts3, svhosts, system64 и др. Но найти незащищенный компьютер, который ещё не заражен, всё сложнее. Так что майнерам приходится эволюционировать.

Одна из недавних находок – майнер с функцией kill list. Когда он попадает в компьютер, то анализирует список процессов. Если майнер находит процессы, которые запущены другими майнерами, то принудительно останавливает их. И сам захватывает все доступные ресурсы.

Майнеры в официальных магазинах приложений

И такое бывает! Например, с сентября 2017 года в Google Play можно было скачать Monero Miner (XMR) разработчика My Portable Software.

Формально приложение было предназначено для майнинга и ничего не нарушало. Но вот незадача: какой бы адрес кошелька вы ни вводили,

намайненное на вашем смартфоне всё равно отправлялось бы на кошелек разработчиков вредоноса.

Владельцам техники Apple «повезло» не меньше. В Mac App Store появилось приложение Calendar 2, которое скрыто майнило Monero. Правда, приложение достаточно быстро удалили. Но осадочек остался.

Сколько зарабатывают на майнерах

Ботнет с майнером Minergate, обнаруженный экспертами, приносил владельцам 30 тыс. долларов в месяц. Через кошелёк, в который отправлялись добытые монеты, прошло свыше 200 тыс. долларов.

Компания Qbix, разработчик Calendar 2, за три дня заработала 2 тыс. долларов на скрытом майнинге Monero.

А разработчик из Камбоджи Макс Корнет рассказал, что получил всего 0,89 доллара за 60 часов от установки скрытого майнера на сайте с посещаемостью около 1 тыс. пользователей в сутки. То есть он зарабатывал 36 центов в день или около 10 долларов в месяц. Конечно, больше посещаемость – выше заработки. Но платные статьи или другую рекламу владельцам сайтов и в этом случае размещать выгоднее.

Как бороться с майнерами

В браузере

1.Перейти на сайт https://cryptojackingtest.com/, который проверит, защищен ли ваш браузер. Проверка бесплатная, но результаты не всегда верны.

•Зеленая надпись YOU’RE PROTECTED – ваш браузер защищен.

•Красная надпись YOU’RE NOT PROTECTED – ваш браузер уязвим.

2.Скачать браузеры со вшитой защитой от майнинга. Opera и «Яндекс.Браузер» поддерживают такие возможности.

3.Отключить JavaScript в браузере. Решение радикальное, ведь многим сайтам для нормальной работы требуется JavaScript. ◦Chrome: «Настройки» – «Дополнительные» – «Настройки контента» – «JavaScript» – Передвинуть переключатель в положение «Заблокировано».

◦Firefox: «Настройки» – «Содержимое» – снять флажок «Использовать JavaScript».

◦Opera: «Настройки» – «Общие настройки» – «Дополнительно» («Расширенные») – «Содержимое» – снять флажок «Включить JavaScript».

4.Приложение Anti-Web Miner. Скачиваете с GitHub, устанавливаете, пользуетесь.

5.Расширения для браузеров. NoCoin, AntiMiner, MineControl, MineBlock и т. д.

6.Расширение для браузеров AdBlock. В фильтры нужно добавить:

•||coin-hive.com^$third-party

•||jsecoin.com^$third-party

•||miner.pr0gramm.com^

•||gus.host/coins.js$script

•||cnhv.co^.

7.Приложение Malwarebytes. Премиум-версия защищает от новых майнеров в режиме реального времени. Бесплатная находит всё, что вы подхватили ранее, и переносит в карантин.

8.В Windows – отредактировать файл C:\Windows\System32\drivers\etc\. В macOS введите в терминале команду sudo nano /etc/hosts/.

В конец файла hosts нужно дописать строку 0.0.0.0 coin-hive.com – она не даст устройству соединятся с сервером, на котором лежит самый известный майнинг-скрипт. Можно переадресовывать на 0.0.0.0 и другие домены, уличённые в распространении вредоносов:

•0.0.0 azvjudwr.info
•0.0.0 cnhv.co
•0.0.0 gus.host
•0.0.0 jroqvbvw.info
•0.0.0 jsecoin.com
•0.0.0 jyhfuqoh.info
•0.0.0 kdowqlpt.info
•0.0.0 listat.biz
•0.0.0 lmodr.biz
•0.0.0 mataharirama.xyz
•0.0.0 minecrunch.co
•0.0.0 minemytraffic.com
•0.0.0 miner.pr0gramm.com
•0.0.0 reasedoper.pw
•0.0.0 xbasfbno.info

На ПК (вне браузера)

1.Уже упомянутое приложение Malwarebytes.

2.Антивирус со свежей базой. Для пользователей Windows: стандартный Windows Defender чаще всего не блокирует популярный Coinhive, так что стоит установить что-то понадёжнее.

3.Нелишним будет запустить диспетчер задач в Windows или другое приложение для слежения за расходом ресурсов компьютера (AIDA64, AnVir Task Manager или аналоги). Для macOS зайдите в «Программы» – «Утилиты» – «Мониторинг системы». Если активность резко растёт и стабильно держится, даже если у вас открыты «Заметки» и «Калькулятор», диспетчере задач или его аналоге удаляйте процессы, которые отнимают слишком много ресурсов. Затем вычищаете всё антивирусом и Malwarebytes.

4.TDSSKiller поможет убить руткиты, которые маскируют следы пребывания майнера в системе.

5.Утилита AVZ. Скачиваете, обновляете базы, нажимаете «Исследовать систему». Получаете avz_sysinfo.htm. Его можно разместить на форуме «Лаборатории Касперского» и попросить помощи. В случае удачи вам помогут составить скрипт, который обезвредит майнер. Но до этого рекомендуется выполнить всё, о чём мы писали выше.

На смартфоне

1.Прежде всего, не скачивать приложения, которые обещают бешенные тыщщи денег от майнинга на смартфоне. И другие подозрительные приложения. Тем более с левых сайтов. Замена батареи / услуги специалиста стоят больше, чем вы сможете намайнить.

2.Для борьбы с майнингом в браузере используйте браузерные расширения или браузеры с защитой от майнинга.

3.Установите надёжный антивирус и регулярно обновляйте базы.

4.Следите за загрузкой ресурсов смартфона. ◦iOS: «Настройки» – «Аккумулятор».

◦Android: «Настройки» – «Аккумулятор» / «Батарея».

Если видите процессы и приложения, которые потребляют больше, чем им положено, смело удаляйте их.

Выводы

Мир помешался на майнинге. А хакеры не замедлили извлечь из этого пользу. Если вы не хотите, чтобы кто-то получал деньги за ваш счёт, не зевайте и защитите свои гаджеты уже сегодня.

(вгору)

Додаток 26

22.03.2018

Шесть способов увидеть, что интернет знает о вас всё

В середине марта компания Facebook оказалась в центре скандала из-за использования личных данных пользователей без их ведома. Мы собрали несколько примеров того, как крупные сервисы открыто рассказывают о собранных персональных данных – но это все равно может вызвать тревогу (InternetUA).

Что случилось?

Британская The Guardian и американская The New York Times опубликовали серию расследований о компании Cambridge Analytica. Издания утверждают, что компания применила психологический тест, который помог точно классифицировать пользователей. Тест платно прошли 270 тысяч человек, которые открыли информацию о своих друзьях в соцсети. Таким образом Cambridge Analytica получила данные о 50 миллионах американцев и смогла показывать им крайне точно настроенную политическую рекламу. После компания оказалась задействована в предвыборной гонке в США.

Наверняка неизвестно, насколько Cambridge Analytica повлияла на ход выборов в США и какова ее заслуга в победе Дональда Трампа. Однако скандал серьезно ударил по Facebook: акции компании упали в цене примерно на 9 процентов за два дня, Марк Цукерберг потерял более 6 миллиардов долларов. Федеральная торговая комиссия США начала проверку Facebook на предмет нарушений в использовании персональных данных, один из инвесторов подал на компанию в суд, а западные пользователи активно обсуждают, как удалиться из соцсети.

Ваши интересы, клики по рекламным объявлениям, перемещения, друзья – все это очень ценная информация. Мы выбрали шесть способов увидеть, как мы дарим собственные личные данные крупным сервисам. Переходите по ссылкам и смотрите, какими своими данными вы поделились.

1. «Секретный файл» с поисковыми запросами

Где работает: Google

Как увидеть: по ссылке

Корпорация Google позволяет скачать абсолютно все ваши данные, которые у нее хранятся. В архиве будут все ваши поисковые запросы, ссылки на видео, просмотренные на YouTube, взаимодействие с рекламой, а также все маршруты, проложенные на картах, и местности, в которых вы открывали сервис.

2. Ваша анкета, которую вы не заполняли

Где работает: Google

Как увидеть: по ссылке

Из огромного массива собранной информации Google составляет ваш примерный «портрет». У компании есть информация не только о поле и возрасте, но также длинный список ваших возможных интересов – хобби, фильмов, игр и увлечений.

Все это нужно компании для более точного показа рекламы. Отключить персонализацию рекламы в Google для аккаунта можно по ссылке. Любопытно, что портрет составляют даже для тех, кто не зарегистрирован в сервисах Google. Такие пользователи могут выключить персонализацию с помощью специального расширения для браузера.

3.«Жучок» в кармане

Где работает: Android

Как увидеть: по ссылке

Еще одна впечатляющая возможность – просмотр всех ваших перемещений, о которых знает Google. Если у вас смартфон Android, то, скорее всего, это будут вообще все ваши перемещения. Google хранит их, чтобы «результаты поиска, сведения о маршрутах и другая информация в сервисах стали точнее».

Отключить эту опцию можно здесь.

4. Социальное досье

Где работает: Facebook

Как увидеть: по ссылке

Вы можете получить копию всех ваших данных, которые есть у Facebook. Для этого нужно в десктопной версии сайта нажать на маленький треугольник в верхнем правом углу страницы, а дальше выбрать «Настройки» – «Общие» – «Скачать копию ваших данных на Facebook».

После подтвержения личности на вашу электронную почту придет внушительный архив. Там есть абсолютно все: фотографии, друзья, сообщения, контакты из почты, активность с разных устройств и даже все рекламные объявления, на которые вы когда-либо кликали.

5. Очень точная реклама

Любой пользователь Facebook может посмотреть, по каким факторам его выбрали для показа рекламы. Для этого нужно нажать многоточие в правом верхнем углу рекламного поста и выбрать пункт «Почему я это вижу?».

Иногда в подборе рекламы оказываются задействованы ваши друзья, история путешествий или подписки на страницы. Здесь же вы можете отказаться от конкретных объявлений.

6. «Портрет» для маркетологов

Где работает: Facebook

Как увидеть: по ссылке

Еще в настройках аккаунта Facebook есть вся информация о вас, которую могут использовать рекламодатели. Ее очень много – это данные о вашей биографии, интересах, устройствах и друзьях.

Здесь же можно запретить сервису учитывать те или иные данные. Например, если запретить «Рекламу с вашими социальными действиями», то ваше имя не будут использовать в объявлениях страниц, которые вы до этого лайкнули. Да-да, без этого запрета ваше имя используют для рекомендации страниц другим пользователям.

(вгору)

Додаток 27

26.03.2018

Facebook знает о вас всё

Facebook получает 98,5 % выручки от показа рекламы, и в этом нет ничего плохого. Другое дело, что для того, чтобы показывать вам максимально подходящие объявления, Facebook лезет в вашу жизнь (InternetUA).

Любой пользователь Facebook может выкачать из соцсети все свои данные: фотографии, публикации на стене, события и приватные сообщения. Если копнуть глубже, можно найти телефонную книгу и метаданные SMS-переписки и звонков. Зарегистрировавшись в Facebook, вы согласились, что соцсети будет доступно всё это. По умолчанию ничто не шифруется.

Facebook Messenger использует фейковый запрос на доступ к телефонной книге. Если при появлении запроса вы нажмёте «Узнать больше» и попытаетесь выяснить, что именно требуется приложению, вы увидите не подробную информацию, а большую синюю кнопку, которая будет убеждать вас включить доступ. Всё, что вам нужно знать, по мнению Facebook, – «Мессенджер будет работать только тогда, когда у вас есть с кем поговорить». Также указано, что если не включить синхронизацию контактов, добавлять собеседников придётся поштучно, хотя это ложь – с мессенджером автоматически синхронизируются вше ваши друзья из Facebook.

Если предоставить мессенджеру доступ к телефонной книге, а затем отнять его, он всё равно продолжит синхронизировать ваши контакты со своими серверами. Версия приложения для Android может получить доступ к

SMS и будет отправлять в Facebook метаданные: когда вы получили сообщение, от кого, ответили ли на него и т.д. После отзыва доступа собранные ранее данные сохранятся у Facebook. Каждый раз, когда Facebook или Facebook Messenger позволяет вам делиться с информацией о местоположении, эти сведения копируются на серверах компании. С помощью JavaScript соцсеть может отслеживать ваше местоположению почти на любом сайте.

Если вы когда-либо проводили платёж через Facebook, отправляли деньги друзьям или платили за них (такое возможно в некоторых странах), информация о вашей банковской карте сохранилась у соцсети. Facebook покупает информацию о покупках вне интернета. Если вы расплатились за что-нибудь картой, которая была засвечена в соцсети, Цукерберг об этом узнает, а специальный алгоритм решит, какую рекламу вам стоит показать в следующий раз.

(вгору)

Додаток 28

26.03.2018

Самым эффективным методом социальной инженерии оказался фишинг

Специалисты Positive Technologies собрали статистику эффективности атак с применением методов социальной инженерии. В ходе проектов по анализу защищенности корпоративной инфраструктуры эксперты компании имитировали активность хакеров и отправляли сотрудникам компаний-заказчиков сообщения, содержащие вложенные файлы, ссылки на веб-ресурсы и формы для ввода паролей. Всего было отправлено 3332 письма и 17 % из этих сообщений в реальной жизни могли бы в итоге привести к компрометации компьютера сотрудника, а впоследствии – и всей корпоративной инфраструктуры (Компьютерное Обозрение).

Самым эффективным методом социальной инженерии оказались сообщения с фишинговой ссылкой: по ней перешли 2 7% получателей. Пользователи невнимательно читают адрес или даже просто, не глядя, кликают на него и переходят на поддельный сайт. Для повышения эффективности атаки злоумышленники могут комбинировать различные методы: в письме одновременно может присутствовать и вредоносный файл, и ссылка на сайт с набором эксплойтов и формой для ввода пароля. Если вложения могут быть заблокированы антивирусом, то способа защиты от добровольной передачи пароля пользователем не существует.

Сотрудники часто не просто открывают незнакомые файлы и кликают по подозрительным ссылкам, но и вступают в переписку со злоумышленниками. В 88 % случаев это делают работники, не связанные с IT (бухгалтеры, юристы, менеджеры и т.п.). Каждый четвертый участник такой переписки оказался руководителем отдела. Впрочем, на удочку хакеров могут попадаться даже

специалисты по безопасности: в ходе наших экспериментов 3% из них вступили в диалог.

В ходе беседы с хакером пользователи могут жаловаться на то, что присланные зловредные файлы или ссылки не открываются, – в некоторых случаях перед этим они пробовали открыть файлы или ввести пароль по ссылке по 30–40 раз! Часто, если открыть файл сразу не удается, сотрудник пересылает письмо в IT-департамент компании с просьбой о помощи. Это увеличивает риски компрометации инфраструктуры, поскольку технические специалисты доверяют коллегам и с высокой вероятностью запустят файл. Иногда адресаты сообщали о том, что письмо попало к ним по ошибке и предлагали имена других сотрудников организации, кому его следовало бы отправить. Эффективность рассылок от лица поддельных компаний сегодня снижается (11 % потенциально опасных действий), в то время как если сообщение приходит от имени реальной компании и реального человека, вероятность успеха взломщиков возрастает (33 %). Именно так действует, к примеру, группировка Cobalt, которая в ходе атак использует фишинговые письма не только через поддельные доменные имена, но и от лица сотрудников реальных банков и компаний-интеграторов, инфраструктура которых была для этого предварительно взломана.

Киберпреступники используют страх, жадность, надежду и другие эмоции для повышения эффективности своих атак. Поэтому в темах своих писем они используют фразы вроде «список сотрудников на увольнение» (спровоцировали 38 % потенциально опасных действий), «выплаты премий за год» (25 %) и т.п. При получении таких сообщений люди часто забывают об элементарных правилах безопасности.

Электронная почта – далеко не единственный инструмент социальной инженерии. Злоумышленники часто звонят сотрудникам компаний по телефону, чтобы, например, представиться специалистом техподдержки и получить важные данные или заставить собеседника совершить нужное действие. Классический пример – звонок рано утром в воскресенье с просьбой срочно явиться на работу. Когда в итоге смущенному сотруднику говорят, что можно и просто продиктовать свой пароль, чтобы «специалисты» разобрались во всем сами, – многие с радостью соглашаются.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник **Терещенко** Ірина Юріївна

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

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