СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(17.01–30.01)

2018 № 2

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(17.01–30.01)
№ 2

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

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

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2018

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

17.01.2018

WhatsApp получил поддержку одной из самых желанных функций для борьбы со спамом

На днях в мессенджер WhatsApp была добавлена функция, которая автоматически запрещает распространение (пересылку) любых подозрительных сообщений.

Докладніше

***

17.01.2018

В Viber появилась долгожданная возможность

Разработчики Viber выпустили новую версию мессенджера для платформ Windows и Mac. Она получила поддержку ряда новых функций, а также усовершенствование уже имеющихся (InternetUA).

Так, теперь пользователи Viber на десктопах могут искать информацию в интернете, кликнув на выделенный фрагмент текста правой кнопкой мыши. Кроме того, администраторы получили возможность закреплять сообщения в группах не только на мобильных устройствах, но и на компьютерах.

Еще одним нововведением стал фильтр нежелательной рекламы, позволяющий помечать спам специальным флажком. Также в Viber реализована возможность ответа на конкретное сообщение собеседника через контекстное меню (данная возможность реализована также в Telegram и WhatsApp).

***

19.01.2018

Twitter стал помечать ссылки на Telegram как спам

Пользователи Twitter заметили, что сервис микроблогов запретил публиковать ссылки с доменом t.me, который принадлежит Telegram. В сообщении говорится, что такие твиты похожи на автоматизированные запросы от спам-робота (IGate).

В декабре 2017 года под похожие ограничения в Facebook попал принадлежащий Telegram сервис для публикации статей Telegraph. Тем не менее, блокировка была снята в тот же день.

***

21.01.2018

Facebook позволит пользователям оценить достоверность источников новостей

Пользователи Facebook смогут оценить достоверность источников новостей, которые попадают в новостную ленту (InternetUA).

Об этом на своей странице рассказал основатель компании Марк Цукерберг.

«Мы решили, что правильнее будет дать пользователям определять, какой источник является наиболее достоверным», – пояснил Цукерберг.

По его словам, на основе полученных ответов будет составляться рейтинг, лидеры которого будут допущены до новостной ленты.

***

22.01.2018

Facebook поднимет приоритет достоверных источников новостей в лентах пользователей

Facebook изменит алгоритмы выдачи в новостных лентах пользователей таким образом, чтобы в них попадало как можно больше ссылок на достоверные (trustworthy) заметки. Об этом объявил глава компании Марк Цукерберг.

Докладніше

***

23.01.2018

Скоростная версия Telegram вышла под Android

Команда популярного мессенджера Telegram сделала доступной версию альтернативного клиента Telegram X для устройств, работающих под управлением операционной системы Android. В декабре 2017 года Telegram X дебютировал на iPhone и iPad (InternetUA).

Пока Telegram X для Android находится на стадии бета-тестирования. Судя по краткому описанию в Google Play, он базируется на TDLib (Telegram Database Library), может похвастаться более высокой, чем у стандартного Telegram, скоростью, а также более гладкой анимацией и «экспериментальными функциями», темной ночной и еще тремя вариантами тем. У вышедшей ранее версии для iOS имеются анимированные стикеры.

Приложение Telegram X для iOS и Android доступно для бесплатной загрузки в App Store и Google Play.

***

23.01.2018

Ольга Мінченко

У Facebook вже 11 млн українців

Соціальною мережею Facebook користується вже 11 млн українців. Про це свідчать дані внутрішньої статистики сервісу (Watcher).

Внутрішня статистика Facebook зараховує до користувачів лише тих, хто хоча б раз протягом останніх 30 днів був залогінений в сервіс.

За останні 12 місяців кількість українських користувачів соцмережі зросла на 67 % – з 6,6 млн до 11 млн. Найбільший ріст був в травні 2017 року, коли українським провайдерам було заборонено давати доступ користувачам до російських соціальних мереж.

Ріст української аудиторії Facebook відбувається в першу чергу завдяки міграції користувачів Одноклассники та ВКонтакте, оскільки природній приріст інтернет аудиторії в Україні в 2017 року був незначним.

***

23.01.2018

7,3 млн українців користуються Instagram

Українська аудиторія соціальної мережі Instagram (належить компанії Facebook) становить 7,3 млн користувачів. За рік вона зросла вдвічі – з 3,6 млн (Watcher).

Рекламні інструменти Instagram (спільний кабінет для реклами як у Facebook, так й Instagram) зараховує до користувачів соцмережі тих, хто хоча б раз протягом останніх 30 днів був залогінений в сервіс.

Цікаво, що близько 2,5 млн українських користувачів Instagram не є користувачами Facebook.

***

24.01.2018

Павел Красномовец

Защищенные мессенджеры Telegram и Signal растут быстрее в коррумпированных странах. В том числе и в Украине

Самые популярные мессенджеры в мире WhatsApp и Facebook Messenger имеют миллиардные аудитории. Но в некоторых случаях темпы их роста уступают конкурентам, особенно в специфических нишах. Американская аналитическая компания Apptopia провела исследование, в котором сравнила скорость роста аудитории защищенных мессенджеров Signal и Telegram с WhatsApp в благополучных и коррумпированных странах.

Докладніше

***

24.01.2018

Компания Facebook ввела новую единицу измерения времени

Специально для создателей инновационного визуального контента (эффектов для фильмов, виртуальной реальности и прочего) была введена абсолютно новая единица измерения, в которой измеряется время. Знакомьтесь – «флик». Своим названием эта единица обязана словам «frame» («кадр») и «tick» («пометка»).

Докладніше

***

24.01.2018

В Instagram появилась GIF-анимация

В разделе Stories приложения Instagram пользователи смогут добавлять специальные стикеры в формате GIF (InternetUA).

Новые стикеры появятся в соответствующем меню во вкладке GIF. Пользователь сможет воспользоваться поиском и найти тот стикер, который наиболее точно подходит к его «истории». На текущий момент новые анимированные стикеры доступны в последней версии Instagram для iOS и Android.

***

25.01.2018

В Telegram появились стикеры для маркетологов «Слезы маркетолога»

В маркетинговом агентстве Royenko Agency, решили подытожить весь свой профессиональный опыт общения с клиентами и коллегами и добавить в это общение фана и трендов. Все отобранные фразы уместились в стикерпаке для мессенджера Telegram «Слезы маркетолога». «Это наша ежедневная боль, радость и разочарование. То, что мы говорим друг другу и что сразу дает понять наше отношение к ситуации. Иногда проще прислать один стикер, чем писать абзац текста», – говорят в агентстве. В агентстве отмечают, что это первая серия стикеров «Слезы маркетолога» будут дорабатываться и пополнятся новыми перлами. Стикерпак доступен для скачивания в Telegram. Ранее украинские креативщики создали набор стикеров о типичном дизайнере (InternetUA).

***

28.01.2018

Twitter, как и другие соцсети, создаст свою копию Snapchat

Twitter планирует запустить функцию-аналог Snapchat, с помощью которой будет удобнее публиковать видео (InternetUA).

Внутри компании уже существует рабочий прототип новой функции, но он ещё не готов для публичного использования. Также пока не известно, будут

ли опубликованные видео оставаться доступными всегда или только некоторое время, как в Snapchat.

Сейчас, чтобы разместить видео в Twitter, нужно открыть приложение на телефоне, начать создавать новый твит, нажать на иконку камеры, снять видео, и только после этого опубликовать. С новым инструментом Twitter можно будет использовать как Snapchat и публиковать видео намного быстрее.

Для Snapchat изменения в Twitter не сулят ничего хорошего. Социальная сеть стабильно растёт с 2014 года, но за последний год этот рост заметно сократился.

По данным Statista, аудитория Twitter с 2015 года выросла с 302 млн пользователей до 330 млн в III квартале прошлого года. За это время компания вложила $86 млн в Periscope, изменила интерфейс, увеличила максимальное количество символов в сообщении и ввела многие другие изменения.

***

29.01.2018

Twitter начал понимать, где на фотографии находится самая важная ее часть

Польза машинного обучения не всегда кроется в крупных функциях – зачастую оно помогает привнести некое мелкое нововведение, которое делает продукт гораздо более удобным. Так произошло и в случае с Twitter, которая с помощью нейронных сетей начала обрезать наиболее интересные части фотографий для создания их миниатюр.

Докладніше

***

29.01.2018

Как запретить Instagram следить за вами

Подобно WhatsApp и Facebook Messenger, раздел Direct приложения Instagram позволяет вашим друзьям и подписчикам получать сведения о вашей недавней активности. Благодаря новой функции, ставшей частью обновленной версии Instagram, это стало можно отключать (InternetUA).

Заходя в Direct, под пользовательским именем подписчика вы видите информацию о том, когда он в последний раз пользовался программой. Если вы считаете, что данная информация о ваших действиях слишком деликатна, чтобы ей делиться, вот как данную функцию можно сделать неактивной.

Касаетесь иконки со своей аватаркой в нижней части экрана, после чего вверху нажимаете на шестеренку, обозначающую настройки. Затем прокручиваете вниз, находите пункт Show Activity Status и переводите ползунок в режим «ВЫКЛ». Описание функции пока не локализовано и доступно только на английском языке.

***

30.01.2018

Чатбот Facebook получит биографию и научится «болтать ни о чем»

Facebook собирается исправить недостатки предыдущего виртуального помощника в новой версии чатбота. Оказалось, что бот требует постоянных доработок и отнимает очень много времени разработчиков. Но, вопреки прогнозам о смерти технологии в целом, исследования в этой области продолжаются. И специалисты намерены решить неожиданно трудную задачу: научить бота поддерживать беспредметную беседу.

Докладніше

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

20.01.2018

Флешмоб UnitedUkraine: в акції на підтримку України взяли участь українці з усього світу

У соцмережах публікують фотографії з різних куточків світу українці, які проживають у різних частинах світах, беруть часть у міжнародному флешмобі на підтримку єдності України UnitedUkraine. Так, у столиці Чехії Празі учні української суботньої школи 20 січня долучилися до флешмобу, написав посол України у Чехії Євген Перебийніс на сторінці у Twitter. Він опублікував фото школярів, які тримають у руках постери з написами «Україна Єдина». «Урок Єдності у старших класах української суботньої школи “Ерудит” у Празі. Поговорили про події січня 1918 та 1919 років – 4-й Універсал, Злуку, Крути та інші важливі сторінки української історії. І звичайно ж приєдналися до флешмобу #UnitedUkraine», – написав посол.

Співробітники українських посольств активно долучаються до флешмобу, публікуючи світлини з Бразилії, Канади, Білорусі, Південної Африки. Флешмоб «United Ukraine» – міжнародна акція в соціальних мережах на підтримку України. Традиційно проводиться в середині лютого і присвячений Дню соборності України. Люди публікують у соціальних мережах фото з постерами на підтримку єдності України та вказубють хеш-тег #UnitedUkraine. Започатковано флешмоб у 2015 році. У 2016 році у флешмобі взяли участь понад 15 000 учасників із 68 країн світу, що розташовані на п’яти континентах. Цьогоріч флешмоб стартував 10 січня.

***

23.01.2018

NASA заморозило свои аккаунты в Twitter и Facebook из-за «шатдауна»

Американское аэрокосмическое агентство NASA прекратило использовать социальные сети из-за правительственного «шатдауна» в США (InternetUA).

«Простите, но мы не будем твитить/отвечать на сообщения во время правительственного “шатдауна”. Кроме того, все публичные мероприятия NASA отменены или отложены до дальнейшего уведомления», – говорится в сообщении NASA в Twitter.

Аналогичные сообщения опубликованы во всех официальных Facebook-аккаунтах агентства, а также в Instagram.

***

30.01.2018
Ирина Фоменко
Социальные медиа достигли пика в политике

Когда предстоят промежуточные выборы 2018 года в США (и мы начинаем говорить о президентской гонке 2020 года), не возникает никаких сомнений, что кандидаты и дальше будут использовать Facebook, Twitter и другие медиа платформы, чтобы сплотить своих сторонников.

Докладніше

***

30.01.2018
Зроби селфі поруч із Тарасом Шевченком у рамкам Всеукраїнського флешмобу

Світлини, які наберуть найбільшу кількість лайків, отримають спеціальний приз (Кременчуцька газета).

Арт-група «Творчий Кременчук» та активісти #Adapter ініціюють Всеукраїнський флешмоб до Дня народження великого Тараса. Мета флешмобу – визначити найкращий пам’ятник Кобзарю серед обласних центрів.

Проте у конкурсі можуть брати участь громадяни із найрізноманітніших населених пунктів (не лише обласних центрів), де є пам’ятник Кобзарю.

Правила флешмобу дуже прості:

Крок 1: Віддай свій голос за пам’ятник Кобзареві, який встановлено в одному з обласних центрів України.

Крок 2: з 1 лютого до 1 березня зроби фото або селфі біля пам’ятника Тарасові Шевченку у твоєму місті, селищі, селі/ОТГ та завантаж на свою сторінку у фейсбуці фото або селфі з хештегами #Sheva_204 #Taras #Kobzar_2018 та та назву Вашого міста /населеного пункту.

Світлини, які наберуть найбільшу кількість лайків, отримають спеціальний приз.

***

29.01.2018

Переяславці запустили флешмоб на підтримку проекту зі стерилізації безпритульних собак

Жителі Переяслава-Хмельницького долучаються до проекту зі стерилізації безпритульних собак. Навіть запустили відповідний флешмоб #ястерилізую у Facebook. Публікують свої фотографії з тваринами, яких привели на стерилізацію, і запрошують інших містян підтримати ініціативу (Вісник Переяславщини).

***

27.01.2018

#WeRemember: люди по всьому світу приєднались до флешмобу у пам'ять про жертв Голокосту

Нащадки пам'ятають. Люди по всьому світу беруть участь у флешмобі у пам'ять про жертв Голокосту (24 канал).

У соціальних мережах публікують фотографії із плакатом з написом «Ми пам'ятаємо».

Світлини оприлюднюють діти, дорослі, єврейські співтовариства і навіть ті, хто особисто пережив Голокост.

У своїх дописах люди нагадають, наскільки важливо пам'ятати про геноцид єврейського народу та доносити це наступному поколінню, аби таких жертв у світі більше не було.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

17.01.2018

YouTube ужесточил правила монетизации для видеоблогеров

После «тяжелого года» YouTube Google представил ряд мер для обеспечения безопасности брендов, чья реклама часто демонстрировалась рядом с несоответствующим контентом. Среди мер: более строгиие критерии для монетизации контента на канале, ручной контроль контента в программе Google Preferred, более сильный контроль для рекламодателей относительно того, что они считают «подходящим контентом» и более сильная защита креаторов YouTube. Теперь креаторы контента должны иметь 1000 подписчиков и 4000 часов просмотров видео за последние 12 месяцев – кроме 10000 общих просмотров – чтобы получить квалификацию для YouTube Partner Program, которая и позволяет им монетизировать контент. Изменения коснутся большой части креаторов, которые зарабатывали менее 100 долларов в год на платформе. Так платформа намерена оградить талантливых креаторов, которые

зарабатывают на жизнь в YouTube, от плохих актеров (Marketing Media Review).

***

19.01.2018

WhatsApp запустил отдельное Android-приложение для бизнеса

Разработчики мессенджера WhatsApp сообщили о выходе отдельной версии сервиса для бизнеса. Приложение WhatsApp Business пока доступно только на Android и только в пяти странах: Великобритании, Индонезии, Италии, Мексике и США (IGate).

Компания обещает запустить бизнес-сервис в других странах в ближайшие недели, а также выпустить в будущем приложение для iOS.

С помощью отдельного приложения компании и бренды могут заводить бизнес-профили с описанием деятельности, указанием дополнительных контактов, адреса и часов работы.

Через WhatsApp Business можно отвечать клиентам, в том числе с помощью готовых ответов на часто задаваемые вопросы. В сервисе также доступна аналитика ответов, которая позволит понять, какие сообщения компании наиболее эффективны, говорят в WhatsApp.

Бизнес-профили должны помочь компаниям, которые получают большой объём обращений через WhatsApp, сказал Reuters операционный директор сервиса Мэтт Идема (Matt Idema).

Пока WhatsApp для бизнеса полностью бесплатный, но в будущем компания будет думать над возможностями монетизации сервиса. Пока обсуждать этот вопрос слишком рано, добавил Идема.

***

22.01.2018

Александр Симудров

Мимо кассы: как делать платежи с помощью Telegram и мобильных денег

Отечественный разработчик Hubbot старается сделать украинский бизнес более современным. На данный момент командой создано 16 ботов, в которых можно расплачиваться за услуги за пару кликов. Теперь оплачивать покупки через Telegram стало еще проще – с помощью мобильных денег «Киевстар».

Докладніше

***

23.01.2018

Facebook инвестирует в повышения цифровой грамотности малого бизнеса ЕС

Facebook сообщила 22 января, что рассчитывает к 2020 г. предоставить возможности цифрового обучения для миллиона жителей ЕС, включая владельцев малого бизнеса. С этой целью компания, в сотрудничестве с местными властями, откроет три социальных центра повышения квалификации – в Испании, Польше и Италии.

Докладніше

***

25.01.2018

Facebook купила Confirm.io, разработчика решений для идентификации личности

Facebook приобрела стартап Confirm.io, который занимается разработкой решений для идентификации личности. Сумма сделки не разглашается (Компьютерное Обозрение).

Confirm.io предоставляет клиентам API, с помощью которого можно проверить на подлинность различные документы пользователей. Также стартап ведет разработки в области биометрии и распознавания лиц.

За три года своего существования стартап привлек более 4 млн долл. от различных инвесторов, включая крупную инвестиционную компанию Cava Capital.

На сайте Confirm.io отмечается, что все ранее действовавшие предложения для пользователей будут закрыты. Все сотрудники стартапа станут членами команды Facebook, где они будут работать над повышением безопасности соцсети.

***

27.01.2018

YouTube платит артистам за раскрутку и требует не оскорблять компанию

За последние месяцы YouTube потратила сотни тысяч долларов на музыкальных исполнителей – деньги уходят на раскрутку и работу со студиями звукозаписи. По слухам, позже в этом году YouTube планирует запустить собственный сервис потоковой музыки Remix, поэтому компания работает с артистами (InternetUA).

Деньги на раскрутку исполнителей тратят все компании с платными потоковыми сервисами, в том числе Apple и Google. Однако только YouTube требует от исполнителей формально отказаться критиковать компанию, с которой они работают.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

19.01.2018

Підлітки перед камерами їдять пральну рідину і вважають це ознакою крутості.

У США та Канаді набрав популярності небезпечний челендж, у якому підлітки заради яскравих роликів у соцмережах їдять перед камерами побутову хімію. Він почався з випадків, коли маленькі діти плутали пральний гель із цукерками (ТСН).

Яскраві капсули з концентрованою пральною рідиною справді приваблюють малюків, котрі не можуть розрізнити небезпеку. Однак дорослiші почали повторювати не з цікавості, а заради популярності та схвалення однолітками. Фахівці пояснюють, що тікати від буденщини, кидати виклик собі та демонструвати власні нестандартні здібності великій віртуальній аудиторії – це мотиви, цілком реальні для підліткового віку. Пошесть набула такого поширення, що YouTube заборонив викладати відео з челеджем, а провідні американські ЗМІ випустили сюжети-застороги для дітей і батьків.

***

24.01.2018

Зависимые от гаджетов подростки чувствуют себя несчастными

Американские ученые обнаружили связь между ощущением счастья у подростков и количеством времени, проведенного ими у экрана. Тинейджеры, чей взгляд постоянно прикован к гаджетам, чаще не удовлетворены своей жизнью (Телекритика).

К таким выводам пришла ведущий автор исследования государственного университета Сан-Диего и профессор психологии Джин М. Твенге.

Чтобы исследовать эту связь, Твенге вместе с коллегами использовали данные исследования «Мониторинг будущего» (MtF), в котором участвовали более миллиона американских школьников 8-х, 10-х и 12-х классов. Студентам задавали вопросы о том, как часто они проводят время со своими телефонами, планшетами и компьютерами, а также вопросы об их социальных взаимодействиях и общем уровне счастья.

***

24.01.2018

Ирина Фоменко

Почему биг-боссы социальных сетей не используют свои платформы?

Разработчики таких платформ, как Facebook, признали, что социальные медиа были спроектированы таким образом, чтобы они вызывали привыкание. Должны ли мы следовать примеру руководителей и отказаться от социальных сетей?

Докладніше

***

27.01.2018

ИИ предотвращает самоубийства, наблюдая за соцсетями

Правительство Южной Кореи решило бороться с растущим числом самоубийств в стране с помощью программы Facebook под названием «AI Saving Lives». Она использует алгоритмы машинного обучения, чтобы отслеживать и анализировать активность пользователей в социальных сетях и мессенджерах. Алгоритм Facebook также способен обнаружить видео-признание, которое, как правило, делают самоубийцы перед смертью. При обнаружении подобного контента программа отправляет предупреждение пользователю и его друзьям (InternetUA).

«Мы сделали “I Saving Lives”, собрав мнения психологов за последние 10 лет, – говорит представитель Facebook Korea. – В сотрудничестве с Центром по предотвращению самоубийств и Центром общественного здравоохранения мы обсуждаем, как эффективно предотвратить самоубийства в Корее».

Сервис Bark.us уже проанализировал 500 млн сообщений и спас 25 детей, которые собирались покончить жизнь самоубийством. Bark.us использует машинное обучение и статистический анализ для сканирования разговоров подростков по электронной почте, SMS и в сервисах вроде Snapchat, Instagram и WhatsApp. Когда обнаруживаются тревожные признаки, Bark.us предупреждает родителей через электронную почту и предлагает возможные шаги. Подписка на сервис стоит $9 в месяц или $99 в год для семьи.

***

29.01.2018

Искусственный интеллект Facebook спас женщину от смерти

Запущенная соцсетью новая программа с использованием искусственного интеллекта (ИИ) помогла правоохранительным органам предотвратить суицид. 55-летняя аргентинка выложила на своей странице в Facebook фотографию сильнодействующих препаратов и подписала ее словами «Прощайте, друзья». Запущенная в ноябре прошлого года специальная программа для поиска потенциальных самоубийц на базе ИИ сразу же обнаружила тревожную

публикацию и уведомила о ней администраторов Facebook в США, которые немедленно связались с аргентинскими службами спасения (InternetUA).

Определить домашний адрес женщины, проживающей в Сантьяго-дель-Эстеро, властям не составило труда. По прибытии спасатели нашли ее без сознания. Женщина была госпитализирована, и медикам удалось вернуть ее к жизни. В настоящее время ей ничего не угрожает.

***

30.01.2018

Американец застрелил подростка во время массового флешмоба в соцсетях

Житель американского города Мемфис в штате Теннесси Шерман Лэкланд (Sherman Lackland) случайно застрелил 17-летнего подростка во время исполнения вирусного флешмоба #NoLackinChallenge. Об этом сообщает The Maven (InternetUA).

Как утверждается в материале издания, Лэкланд с своим несовершеннолетним приятелем решили поучаствовать в популярной среди американских подростков игре #NoLackinChallenge, в рамках которой тысячи пользователей социальных сетей в шутку направляют огнестрельное оружие друг на друга. Таким образом они хвастаются пистолетами и проверяют готовность товарища отразить нападение грабителей.

***

30.01.2018

Обережно! «Синій кит» знову приплив

На теренах соціальних мереж України поширюється нова небезпечна гра «Новий шлях» (Версії.if.ua).

Як відомо, в цієї «гри» є куратор, який створює групи в мережах і дає підписникам завдання. У поліції вже блокують групи смерті та хештеги, але натомість з’являються нові.

Підлітків зацікавлюють до суїцидальної гри по хештегах #сованикогданеспит та #тихийлес , #групысмерти. Група, яка йде звісно ж від Росії «Новый путь», з’явилась в соціальній мережі «ВКонтакте» та поширились в мессенджер «Телеграм».

Для участі у грі «Новий шлях» потрібно розмістити хештег з певним написом, але попередньо потрібно розмістити картинку з пентаграмою. В кожного учасника є свій «куратор», який доводить до фіналу – самогубство.

Маніпулятивні технології

17.01.2018

Facebook расширит расследование влияния России на голосование по Brexit

Компания Facebook заявила, что проведет более подробное расследование того, пыталась ли Россия повлиять на голосование по выходу Великобритании из ЕС (Brexit). Об этом сообщает Daily Mail (InternetUA).

Ранее социальная сеть предоставляла данные о том, что нашла только три связанные рекламные объявления по Brexit, связанные с расположенным в России «Агентством интернет-исследований», набравшие в сумме 200 просмотров.

Но член парламента Великобритании Дэмиан Коллинз обвинил Facebook в недостаточно эффективном расследовании российского вмешательства.

В ответ на это в Facebook заявили, что займутся поиском других похожих объединений, вовлеченных в координированную деятельность вокруг Brexit, не выявленных до этого.

***

18.01.2018

Twitter может уведомлять пользователей о воздействии российской пропаганды

Компания Twitter может начать уведомлять пользователей, подвергались ли они влиянию контента, сгенерированного предполагаемым российским сервисом для распространения пропаганды. Об этом сообщил представитель компании, передает Reuters (InternetUA).

Социальная сеть «работает, чтобы идентифицировать и лично проинформировать» ее пользователей, которые увидели во время президентской компании 2016 года твиты аккаунтов, связанных с прокремлевским «Агентством интернет-исследований», рассказал Карлос Монйе, директор Twitter по общественной политике.

***

20.01.2018

Twitter обнаружил более 3 тыс. аккаунтов, связанных с российской «фабрикой троллей»

Администрация Twitter обнаружила 1062 аккаунта, связанных с российским «Агентством интернет-исследований», также известным как «фабрика троллей», сообщается в официальном блоге соцсети.

Докладніше

***

23.01.2018

Facebook усилит борьбу с российским вмешательством

Организации, которые размещают политическую рекламу на Facebook, должны будут пройти процедуру идентификации. Об этом заявил представитель компании Самид Чакрабарти (InternetUA).

По его утверждению, эта мера вводится для предотвращения возможного российского вмешательства в ход будущих выборов в США. «Организации, публикующие касающуюся выборов рекламу, будут подтверждать свою принадлежность, чтобы пользователи могли видеть, кто оплачивал эту рекламу. Мы будем архивировать образцы электоральной рекламы и делать их доступными для поиска в целях повышения отчетности», – рассказал он.

«Компания недооценила степень опасности использования сторонними игроками социальных СМИ в качестве информационного оружия, – заявил Чакрабарти. – во время выборов 2016 года российские субъекты создали 80 тысяч постов, которые за два года дошли до около 126 миллионов человек в Соединенных Штатах».

Спецслужби і технології «соціального контролю»

17.01.2018

Власти Китая начнут борьбу с «похожими на криптобиржи» площадками

Правительство Китая продолжает оказывать давление на сферу криптовалютного трейдинга. Теперь в центре внимания чиновников оказались «онлайн-платформы и мобильные приложения, предлагающие похожие на биржи услуги», сообщает Bloomberg со ссылкой на осведомленные источники (InternetUA).

Власти страны намерены заблокировать доступ к местным и иностранным платформам для централизованного трейдинга, отметил собеседник издания. Впрочем, пока неизвестно, как законодатели планируют классифировать подобные площадки.

Кроме того, правительство будет бороться с компаниями и отдельными лицами, предоставляющими расчетные и клиринговые услуги. Отмечается, что небольшие P2P-транзакции под запрет не попадут.

***

18.01.2018

У Львові СБУ викрила адміністратора антиукраїнських груп у соцмережах

Співробітники Служби безпеки України у Львівській області припинили діяльність адміністратора антиукраїнських груп у соцмережах (InternetUA).

Оперативники спецслужби встановили, що модератор розміщував в Інтернеті матеріали із закликами до зміни меж території України та висловлювався на підтримку терористичних організацій «Л/ДНР».

Під час санкціонованого обшуку за місцем проживання проросійського пропагандиста правоохоронці, у рамках раніше відкритого СБ України провадження за ст. 258-3 Кримінального кодексу України, виявили техніку та носії інформації, які будуть передані на експертизу.

Триває досудове слідство.

***

20.01.2018

Погранслужба США сможет проверять ноутбуки и телефоны туристов

Работники пограничной службы США теперь смогут проверять телефоны и ноутбуки прибывающих в страну в целях безопасности (InternetUA).

По новым правилам, если потребуется, путешественники обязаны предоставить свой телефон и ноутбук для проверки сотруднику пограничной службы в аэропорту США. Аппарат при этом должен быть включен и разблокирован.

Офицер вправе провести беглый осмотр устройства. В случае возникновения подозрений, гаджет будет исследован более детально. В случае отрицательного ответа, человеку может быть отказано во въезде в США. Также устройство могут изъять на срок до недели.

Проверять сотрудники пограничной службы США будут на связь с террористическими организациями, наличие детской порнографии, нарушение норм экспортного контроля и прав интеллектуальной собственности.

***

22.01.2018

В РФ мессенджерам запретили рассказывать о своем сотрудничестве с ФСБ

В то, как организаторы распространения информации в интернете взаимодействуют с правоохранительными органами, внесен ряд изменений. Об этом в понедельник, 22 января, сообщает информагентство ТАСС (InternetUA).

Согласно внесенным изменениям, администрация организатора распространения информации (то есть, мессенджера) должна следить за «неразглашением любой информации о конкретных фактах и содержании такого взаимодействия третьим лицам». Другими словами, мессенджер не имеет права сообщать кому-либо о своем сотрудничестве с правоохранительными органами. Также правительство РФ ввело запрет на размещение программно-технических средств, используемых в рамках такого взаимодействия, не на российской территории.

Помимо прочего, отныне администрация мессенджеров должна предоставлять ФСБ удаленный доступ к своей информационной системе не позже, чем через три месяца после получения соответствующего уведомления от спецслужбы.

Организатор распространения информации в сети Интернет – лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет.

***

22.01.2018

У Криму чоловіка засудили за «поширення екстремістських ідей антиросійського характеру» в інтернеті

У Криму підконтрольний Кремлю Керченський міський суд засудив 55-річного місцевого жителя до 2,5 років позбавлення волі умовно і штрафу в 50 тис руб за «русофобські висловлювання в інтернеті, зберігання тротилу і патронів» (InternetUA).

Про це повідомляє підконтрольний кримській владі сайт «Крыминформ» з посиланням на прес-службу управління ФСБ.

«Встановлено, що Кухаренко, відчуваючи неприязнь до громадян Росії і росіянам, у 2016 році став ініціатором створення в спеціальному додатку інтернет-каналу для поширення екстремістських ідей антиросійського характеру, – йдеться у повідомленні ФСБ. – Крім того, доведено причетність Кухаренка до зберігання за місцем проживання вибухових речовин (тротил) і боєприпасів (патрони)».

Також зазначено, що «свою провину чоловік визнав». Керчанина засуджено за трьома статтями КК РФ та засуджено до 2,5 років позбавлення волі умовно і штрафу в 50 тис рубл.

***

24.01.2018

Екатерина Шпачук

IT-гиганты потратили рекордную сумму на лоббирование в 2017 году

В 2017 году компании Apple, Amazon, Facebook и Google потратили рекордные 50 миллионов долларов на лоббирование в правительстве США. Отмечается, что IT-компании противостояли новым федеральным правилам администрации Дональда Трампа. Это означает, что технологическая отрасль в США все больше и больше находится под политическим влиянием.

Докладніше

***

24.01.2018

Таинственная структура сдает правительствам в аренду ПО для слежки за собственными гражданами

Фонд электронных рубежей (EFF) совместно с компанией Lookout, занимающейся вопросами сетевой безопасности, объявили об обнаружении шпионской платформы Dark Caracal (степная рысь), которую некие неизвестные пока разработчики предлагает правительствам разных стран для шпионажа и слежки за собственными гражданами.

Докладніше

***

24.01.2018

Британія створить спецпідрозділ для боротьби з фейковими новинами

Уряд Великої Британії має намір створити підрозділ по боротьбі з фейковими новинами, який протистоятиме дезінформаційним кампаніям інших держав (Espreso.tv).

Про це заявив представник британського прем'єр-міністра Терези Мей, повідомляє Reuters.

«Ми живемо в епоху фальшивих новин і конкурентних повідомлень. Уряд буде намагатися якомога ефективніше використовувати комунікації в цілях національної безпеки», – сказав представник Мей.

За його словами, новий спецпідрозділ з питань національної безпеки у сфері комунікацій відповідатиме за боротьбу з дезінформацією з боку інших держав і приватних осіб.

«Ми будемо використовувати існуючі можливості, створивши спеціальний блок зв'язку національної безпеки, якому буде доручено боротися з дезінформацією з боку державних діячів та інших. Це буде більш систематично утримувати наших супротивників і допомагати нам виконувати пріоритети національної безпеки», – додав він.

***

24.01.2018

Слежка за частной жизнью целых наций незаметно становится нормой

Помимо невинных и полезных применений, таких как борьба с вредителями, поиск новых лекарств и написание шуточных текстов, алгоритмы искусственного интеллекта и машинного обучения начали массово использоваться, в первую очередь, для наблюдения за людьми.

Докладніше

***

25.01.2018

На Донеччині СБУ припинила діяльність мережі інформаторів терористичної організації «ДНР»

Співробітники Служби безпеки України під час виконання комплексу заходів із забезпечення інформаційної безпеки держави зафіксували чергові факти використання спецслужбами РФ соціальних мереж для проведення підривної діяльності на шкоду національній безпеці України (InternetUA).

Оперативники спецслужби задокументували, що четверо мешканців Донеччини, які входили до агентурної мережі терористів, регулярно передавали через аккаунти у соцмережах інформацію про сили антитерористичної операції. Зловмисники, зокрема, повідомляли кураторам з спецслужб РФ дані про дислокацію та пересування військових підрозділів, задіяних в АТО у Краматорському та Слов'янському районах.

Співробітники СБУ також встановили, що інформатори адміністрували антиукраїнські спільноти у російських соцмережах, де розміщували спеціально підготовлені матеріали із закликами до зміни меж території України.

Під час санкціонованих слідчих дій правоохоронці виявили у чотирьох інформаторів комп'ютери та мобільні телефони, які використовувалися для передачі інформації представникам терористів та здійснення антиукраїнської пропаганди.

***

28.01.2018

Нидерландские спецслужбы с 2014 года шпионили за «русскими» хакерами

Сотрудники Общей службы разведки и безопасности Нидерландов (Algemene Inlichtingen-en Veiligheidsdienst, AIVD) с 2014 года шпионили за участниками российской хакерской группировки Cozy Bear (она же APT29), подозреваемой в атаке на серверы Демократической партии США во время предвыборной кампании в 2016 году, сообщает издание deVolkskrant со ссылкой на осведомленные источники (InternetUA).

Агенты AIVD проникли в компьютерную сеть Cozy Bear и в период с 2014 по 2017 годы передавали полученную информацию Агентству национальной безопасности (АНБ) и Федеральному бюро расследований (ФБР) США, утверждает издание.

***

30.01.2018

Пентагон перевірить використання фітнес-трекерів військовими через витік даних

Міністерство оборони США має намір оцінити загрозу, яку можуть представляти для американських військових баз фітнес-трекери і переглянути правила використання таких пристроїв військовими.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

17.01.2018

Уязвимость в интеграции Oculus-Facebook позволяла получить контроль над чужими учетными записями

Очки виртуальной реальности Oculus позволяют пользователям подключаться к своим учетным записям Facebook для более богатого «социального» опыта. Подключение осуществляется как с помощью родного приложения для Windows, так и через браузер. Исследователь безопасности Йосип Франькович (Josip Franjković) проанализировал приложение и обнаружил уязвимость, позволяющую осуществить межсайтовую подделку запросов (CSRF).

Докладніше

***

17.01.2018

Киберполиция назвала количество раскрытых за год преступлений

Количество выявленных киберпреступлений ежегодно увеличивается в среднем на 2,5 тыс. Об этом рассказал глава Киберполиции Сергей Демедюк (IGate).

Так, в 2017 году Киберполиция сопровождала около 7 тыс уголовных производств. Из них 4,5 тыс – исключительно киберпреступления. За 11 месяцев 2017 года ведомство направило в суд обвинительные акты в отношении 726 человек.

По словам Сергея Демедюка, наиболее распространенным видом преступлений является кибермошенничество, когда преступник пытается путем обмана завладеть информацией о банковских картах жертв. Это также кардинг – кража данных банковских карт и получение доступа к интернет-банкингу жертвы.

На втором месте – противоправный контент. Речь идет о защите интеллектуальной собственности и борьбе с распространением детской порнографии.

На третьем месте – распространение вредоносного программного обеспечения и создание площадок для продажи похищенной информации.

***

18.01.2018

Обнаружен самый мощный вирус для Android

«Лаборатория Касперского» обнаружила новый вирус для устройств на базе операционной системе Android, работа которого сравнима с возможностями продвинутых спецслужб. Частичный код и описание вируса Skygofree опубликовано в блоге компании.

Докладніше

***

18.01.2018

В магазине Google Play обнаружены игры с троянским модулем

«Доктор Веб» предупреждает о появлении в магазине Google Play ряда игр для операционной системы Android, в состав которых интегрирован вредоносный компонент (InternetUA).

Сообщается, что в небезопасные приложения встроен троянский модуль, который незаметно скачивает и запускает дополнительные компоненты. Они могут выполнять различные функции – например, скрытно открывать те или иные сайты и «нажимать» на определённые элементы на этих страницах.

В процессе работы вредоносный модуль загружает с указанного управляющим сервером адреса скрипт, которому предоставляет возможность совершать различные действия на странице, в том числе симулировать клики по указанным скриптом элементам. Таким образом, если в задании трояна был переход по ссылкам или рекламным объявлениям, злоумышленники получают прибыль за накрутку счётчика посещений веб-страниц и нажатия на баннеры.

Теоретически на мобильное устройство жертвы могут также загружаться модули для демонстрации рекламы или отображения фишинговых окон с целью кражи логинов, паролей и другой конфиденциальной информации, скажем, данных банковских карт.

***

18.01.2018

«Антонов» заявил о взломе сайта и публикации там фейкового письма

На сайте появилось якобы открытое письмо руководства предприятия с обвинениями в адрес правительства. В пресс-службе ГП письмо назвали провокацией (InternetUA).

Госпредприятие «Антонов» заявило о хакерской атаке на сайт – там появилосьь письмо с обвинениями в адрес Кабинета министров и премьера Владимира Гройсмана. Письмо фейковое, сообщили в пресс-службе «Антонов» Громадському.

В предприятии такие действия назвали провокацией.

В письме, которое появилось на сайте, говорилось, что правительство усложняет работу предприятия и не предоставляет необходимой поддержки.

Пресс-служба ГП пока не знает, когда именно взломали сайт и кого можно подозревать в этой атаке.

***

21.01.2018

Сколько пользователей пострадало от утечки OnePlus?

Компания OnePlus признала утечку данных о банковских картах 40 тысяч пользователей своих смартфонов. OnePlus провела расследование, подключив к нему сторонних специалистов, которые пришли к заключению, что номера банковских карт, срок действия и коды безопасности были скомпрометированы (InternetUA).

В разосланном пользователям сообщении, OnePlus, помимо принесения извинений, рекомендует проверить состояние банковских карт и известить банк о любых подозрительных изменениях, что облегчит получение компенсации в случае необходимости. Для пострадавших от утечки пользователей OnePlus собирается предоставить год бесплатного кредитного мониторинга.

***

22.01.2018

Хакери зламали сторінку президента Болгарії у Facebook і дещо запостили

21 січня на сторінці президента Болгарії Румена Радєва у соцмережі Facebook з'явилася стаття турецькою мовою з відповідним електронним посиланням на турецький сайт, що займається кредитуванням (Espreso.tv).

Про це повідомляє Newscafe.

Після появи статті користувачі попередили про те, що, найімовірніше, сторінка була зламана хакерами, і порадили не відкривати посилання на статтю, бо воно може містити віруси.

Інформацію про злам сторінки згодом підтвердили в прес-службі болгарського президента.

Правоохоронні органи і спецслужби Болгарії проводять перевірку за цим фактом.

***

22.01. 2018

Криптомайнеры атаковали 55 % компаний в мире

Исследователи Check Point обнаружили, что в декабре криптомайнеры атаковали 55 % компаний во всем мире. При этом 10 разновидностей этого

вредоносного ПО попали в топ-100 самых активных киберугроз, а два из них вошли в тройку лидеров.

Докладніше

***

22.01.2018

Snap пригрозила сотрудникам тюрьмой за утечку данных

Компания Snap, развивающая сервис Snapchat, пригрозила своим сотрудникам санкциями за намеренную организацию утечек конфиденциальной информации.

Докладніше

***

22.01.2018

Более 90 % пользователей всех сервисов Google находятся в большой опасности

Согласно официальным данным от Google, более 90 % пользователей всех ее сервисов находятся в большой опасности. Она утверждает, что с каждым годом злоумышленники находят все более изощренные способы кражи ценной информации, а пользователи на это совсем никак не реагируют.

Докладніше

***

22.01.2018

Крупнейшие британские интернет-магазины обвинили в раскрытии данных покупателей

Крупнейшие британские интернет-магазины передают данные о клиентах сторонним компаниям с помощью сотен средств для отслеживания действий покупателей на своих сайтах, сообщает издание The Times со ссылкой на данные аналитической компании Evidon (InternetUA).

По словам аналитиков, на сайте компании Debenhams было выявлено 65 инструментов для отслеживания действий пользователей, у Mothercare – 51, у Marks & Spencer – 45, у Boots – 42, у House of Fraser – 40, у Amazon – 25, у компании Tesco – 13. С помощью данных инструментов можно отследить IP-адреса клиентов, их местонахождение, а также получить информацию об устройстве и браузере пользователя.

Как отметили представители правозащитной организации Privacy International, хотя система online-рекламы и построена на заявлении, что отслеживаемая информация является полностью анонимной, есть множество примеров, когда данные удавалось связать с конкретным лицом.

Как сообщило издание, одна из компаний-покупателей данных создавала видео, на которых полностью воспроизводила действия посетителей сайтов интернет-магазинов. При этом, по словам представителей компании, они не обладали данными из учетных записей пользователей.

***

22.01.2018

Мобильные браузеры Opera получили защиту от добычи криптовалют

22 января официально объявлено о том, что в мобильных браузерах Opera появилась функция защиты от добычи криптовалют (InternetUA).

Новое решение, предназначенное для борьбы с майнерами, активируется по умолчанию, когда включается блокировщик рекламы в Opera Mini (версии для iOS и Android) и Opera для Android. Блокировщик рекламы можно активировать в настройках. Он будет автоматически определять и отключать скрипты для майнинга криптовалют, встраиваемые в коды веб-страниц, говорится в сообщении разработчиков.

На фоне роста курса биткоина и других криптовалют все чаще можно видеть, как посетители некоторых сайтов предоставляют мощности своих компьютеров в обмен на доступ к контенту, и зачастую обе стороны все устраивает.

Чтобы пользователи могли определить, защищен ли их браузер от несанкционированного криптомайнинга, Opera создала специальный сайт. На нем можно проверить, существует ли угроза майнинга для смартфона или десктопного компьютера пользователя.

***

23.01.2018

Мошенники похищают криптовалюту через фишинг-аккаунты в Facebook

Специалисты «Лаборатории Касперского» выявили новую фишинговую схему, с помощью которой мошенники пытаются похитить криптовалютные средства пользователей Facebook (InternetUA).

Злоумышленники копируют страницы популярных криптовалютных сообществ, после чего используют фотографии участников реальных сообществ, отмечая их в посте как победителей программы лояльности к платформе.

«Пользователей заманивают обещаниями выплаты большой суммы, для получения которой необходимо пройти по ссылке на поддельный сайт – и оставить там свои приватные данные», – рассказывают специалисты.

Также компания напомнила о фишинговой «классике» – спам-рассылках. Часто их рассылают от имени криптокошельков или криптобирж, например, с

оповещениями безопасности или предложением принять участие в опросе. При этом чаще всего пользователей направляют на подделки сайта blockchain.info для ввода своих учетных данных.

«Сайт самого популярного биткоин-кошелька выглядит довольно просто, но в то же время узнаваемо – это помогает преступникам эффективно его подделывать», – отмечают эксперты.

***

23.01.2018

В «Касперском» обнаружили вирус в пиратской книге о Трампе

Исследователь безопасности в «Лаборатории Касперского» Майкл Мольснер обнаружил в пиратской электронной версии книги «Огонь и ярость» Майкла Вольфа вредоносное ПО, с помощью которого хакеры могут получить доступ к компьютерам других пользователей. Об этом сообщает издание Fortune.

Издание Daily Beast сообщило, что «зараженная» версия книги имеет чуть более 230 страниц в формате PDF, а не 328 страниц, как в официальной версии. В тестах, которые провели журналисты Daily Beast, входящее вредоносное ПО было легко обнаружено антивирусным программным обеспечением (Новости ИТ).

***

24.01.2018

За прошлый год хакеры обокрали не менее миллиарда человек

Фирма Norton опубликовала очередной ежегодный доклад Norton Cyber Security Insights, базирующийся на результатах онлайнового опроса, проводившегося для неё исследовательским агентством Reputation Leaders с 5 по 24 октября 2017 г. Исследование охватило 21549 человек возрастом от 18 лет (Компьютерное Обозрение).

Согласно выводам Norton, за прошлый год жертвами киберпреступлений во всем мире стали 978 млн человек, что составляет треть населения 20 охваченных опросом стран и половину их онлайновой популяции. В среднем каждый из них в результате деятельности хакеров стал беднее на $142 (всего 172 млрд долл.) и потратил 23,6 часов (три рабочих дня) на устранение последствий атак.

По числу жертв ведущее место занимает Китай – 352,7 млн, за ним следуют Индия – 186,44 млн, США – 143,7 млн и Бразилия – 62,21 млн. Обнародованные цифры дают общее представление о шокирующих масштабах, которые приобрела киберпреступность, но не отражают полной картины, так как из рассмотрения исключены страны Восточной Европы, Африки и Латинской Америки (кроме Бразилии и Мексики).

***

24.01.2018

Михаил Сапитон

В Tinder нашли уязвимость. Хакеры могут узнать о ваших фото, лайках и парах

Исследователи из тель-авивской компании Checkmarx обнаружили, что дейтинг-приложение Tinder имеет серьезные проблемы с безопасностью. Несмотря на то, что большинство передаваемых между пользователем и облачными серверами данных проходят по защищенному протоколу HTTPS, разработчики не потрудились ввести его поддержку для фотографий профиля. Любой пользователь одной и той же сети Wi-Fi может посмотреть чужие снимки из Tinder или даже добавлять свои в посторонние аккаунты (AIN.UA).

Свайпы и лайки, в свою очередь, хотя и передаются в защищенном виде, генерируют запросы с четко определенным объемом в байтах. Например, однажды установив, что смахивание влево это 278 байт, вправо – 370 байт, а совпадение равняется 570 байтам, можно следить за активностью другого юзера.

В ответ на запрос издания The Verge представители Tinder ответили, что без защиты находятся только фотографии профиля, но в приложении они и так предоставлены в свободном доступе. Тем не менее, веб-версия сервиса уже шифрует эти снимки, а разработчики планируют внедрить эту функцию и в мобильных клиентах. Остальные подробности об улучшении безопасности неизвестны. По словам Checkmarx, они сообщили в Tinder о бреши еще в ноябре, но она по-прежнему не исправлена.

***

24.01.2018

В Канаде заявили об атаке хакеров из КНДР через Россию

По словам представителя компании Metrolinx, которая занимается обеспечением работы систем общественного транспорта и аэропортов Торонто и его пригородов, Анны-Мари Эйкинс, компания подверглась атаке хакеров из КНДР, передает CBC (InternetUA).

«Кибератака не привела к нарушению конфиденциальности и не нарушила работу каких-либо систем безопасности», – сказала Эйкинс.

По словам источника, хакеры запустили вирус, поразивший компьютеры компании, через Россию.

***

25.01.2018

Троянец Mezzo способен менять реквизиты в бухгалтерских файлах

«Лаборатория Касперского» обнаружила новую угрозу – троянец Mezzo, способный подменять реквизиты в файлах обмена между бухгалтерскими и банковскими системами.

Докладніше

***

28.01.2018

Более 2000 сайтов на WordPress заражены кейлоггером и браузерным майнером

В декабре 2017 года аналитики компании Sucuri предупреждали о вредоносной кампании, развернутой против плохо защищенных и давно не обновляющихся сайтов на базе WordPress (InternetUA).

Теперь специалисты Sucuri представили новый отчет, согласно которому злоумышленники по-прежнему не прекратили свою операцию. Преступники все так же компрометируют сайты через уязвимые темы или плагины, а также эксплуатируют баги в старых версиях WordPress, а затем внедряют в админку код, который подгружает кейлоггера, хостящегося на стороннем домене. На фронтэнде взломщики размещают браузерный майнер Coinhive, использующий компьютеры посетителей таких сайтов для майнинга криптовалюты Monero.

Если ранее преступники размещали свою малварь на домене cloudflare.solutions, то теперь список доменов пополнили cdjs.online, cdns.ws и msdns.online. Согласно данным PublicWWW, скрипты с этих доменов загружаются более чем для 2000 сайтов (1, 2, 3). Однако далеко не все сайты индексируются PublicWWW, так что исследователи полагают, что на самом деле пострадавших ресурсов гораздо больше.

***

29.01.2018

Ольга Карпенко

Вредоносный код для майнинга встраивают даже в рекламу на YouTube

О том, как программы-майнеры зарабатывают на ресурсах пользователя, подгружаясь из браузера без ведома владельца устройства, и зарабатывая криптовалюту для своих создателей, мы уже рассказывали ранее. На днях стало известно, что подобные программы-паразиты могут подгружаться даже из рекламы YouTube (AIN.UA).

По данным ArsTechnica, еще в конце прошлой недели пользователи стали жаловаться, что их антивирусы сообщают о майнинговом коде, когда они смотрят ролики на YouTube. Причем, если в процессе поменять браузер, майнинговая активность все равно продолжается.

Исследователи из Trend Micro заявили, что новая механика – размещение майнеров в рекламе – втрое повысила количество обнаружений подобных

программ. Создатели этих программ использовали платформу Google DoubleClick, чтобы добраться до мощностей центрального процессора пользователей-любителей YouTube.

***

30.01.2018

Хакеры из КНДР атаковали крупнейшую энергетическую компанию Израиля

Северокорейские хакеры атаковали ведущего израильского поставщика электроэнергии – «Электрическую компанию Израиля» (ЭКИ). Атаки проводятся на «очень высоком уровне», сообщили японскому изданию Sankei источники в руководстве компании (InternetUA).

По словам представителей корпорации, реального ущерба кибератаки не нанесли, однако хакеры использовали серьезное вредоносное ПО, а уровень подготовки атакующих был весьма высоким. Предположительно, данные атаки проводились в учебных целях для отработки новейших технологий и методик взлома, поскольку считается, что ЭКИ имеет одну из лучших в мире систем по защите от киберугроз.

Ранее кибератаки, направленные на уничтожение или нарушение функционирования систем ЭКИ, осуществлялись в основном странами Ближнего Востока, однако с прошлого года число атак, совершенных Северной Кореей, резко увеличилось, отметили специалисты.

«У хакеров из КНДР уже есть все необходимое, чтобы нанести ущерб инфраструктуре Японии, США, и каких либо других стран», – отметил один из экспертов ЭКИ.

***

30.01.2018

Хакерские атаки на голландские банки осуществлялись с российских серверов

Хакерские атаки, от которых пострадали три крупнейших голландских банка, осуществлялись с российских серверов, сообщает издание De Telegraaf со ссылкой на компанию ESET, которая специализируется на вопросах цифровой безопасности (InternetUA).

«Это не обязательно означает, что исполнители атак также в России – они могут быть где угодно», – отмечают специалисты.

Как сообщили в компании, хакеры использовали так называемый ботнет – сеть зараженных компьютеров. Используя программу Zbot, они отдаленно направляли сигналы устройств посетить определенные сайты и тем самым перегружали сервера, неспособные справиться с резким ростом числа посетителей. При этом командные серверы находились преимущественно в России.

***

30.01.2018

В США компания использовала данные реальных людей для создания интернет-ботов

В США прокуратура завела дело на компанию Devumi, занимающуюся продвижением страниц в социальных сетях на заказ. Компания обвиняется в регистрации поддельных аккаунтов с использованием данных реальных людей. Незаконную деятельность Devumi выявили корреспонденты издания The New York Times в ходе журналистского расследования (InternetUA).

Компания предлагает услуги по продвижению страниц путем накрутки подписчиков, несмотря на то, что во многих сервисах это запрещено. Согласно публикации, в распоряжении Devumi находится порядка 3,5 млн учетных записей в различных соцсетях, многие из которых были проданы многократно. Клиентами Devumi стали около 200 тыс. человек, в том числе несколько известных медийных персон, купивших в общей сложности около 200 млн новых подписчиков.

По данным издания, по меньшей мере 55 тыс. учетных записей Devumi используют имена, фото профилей и другие персональные данные других людей. При этом аккаунты ботов тщательно подражают оригиналу и выявить их можно по необычно большому числу подписок.

Как заявил основатель Devumi Герман Калас (German Calas), компания не имеет никакого отношения к поддельным учетным записям и лично он ничего не знает об использовании персональных данных других людей для регистрации ботов.

ДОДАТКИ

Додаток 1

17.01.2018

WhatsApp получил поддержку одной из самых желанных функций для борьбы со спамом

Очень многие люди живут тем, чтобы вредить законопослушным гражданам. Они делают это самыми разными способами, начиная от мошенничества и заканчивая распространением спама. Порой доходит даже до того, что пользователи пересылают друг другу по цепочке спам, вирусы и другие фейковые сообщения, чем администрация сервиса WhatsApp совершенно недовольно. На днях в мессенджер была добавлена функция, которая автоматически запрещает распространение (пересылку) любых подозрительных сообщений (InternetUA).

За последние дни многие пользователи WhatsApp столкнулись с ошибкой вида «Сообщение было перенаправлено уже много раз». Увидеть ее можно в

том случае, если распространяется какой-то шок контент или же что-то еще, что на самом деле не соответствует действительности. Очевидно, что в мессенджер на уровне сервером компании-разработчика была добавлена одна из самых желанных функций для борьбы со спамом.

Злоумышленники создают какие-то удивительные истории, после чего рассылают их своим друзьям и знакомым с просьбой тех отправить их своим контактах, а те, в свою очередь, должны сделать то же самое. Порой доходит до того, что одно и тоже сообщение в WhatsApp получают более 1 млн человек из различных стран мира, но в пределах одного языка. Причем распространение ложных данных происходит с рекордной скоростью – за несколько часов.

Для борьбы с этим в мессенджер WhatsApp и добавили долгожданную функцию, которая запрещает пересылать подозрительные сообщения кому угодно. Некоторые пользователи, конечно, останутся недовольны таким нововведением, однако нужно понимать, что пойти на такие меры было просто необходимо, так как в противном случае мошенники и дальше бы распространяли фейковую информацию, вирусы и наглый спам. Увидеть сообщение с информацией о невозможности отправки того или иного сообщения теперь можно во всех клиентах сервиса, включая таковые для Android и iOS.

(вгору)

Додаток 2

22.01.2018

Facebook поднимет приоритет достоверных источников новостей в лентах пользователей

Надёжность сайтов будет измеряться с помощью опросов – это должно повысить качество материалов, которые видят пользователи, уверен Марк Цукерберг (IGate).

Facebook изменит алгоритмы выдачи в новостных лентах пользователей таким образом, чтобы в них попадало как можно больше ссылок на достоверные (trustworthy) заметки. Об этом объявил глава компании Марк Цукерберг.

Новости в Facebook будут измеряться по трём параметрам: достоверность, информативность и близость к пользователю (news that is relevant to people’s local community), говорится в пояснении соцсети. Первые два параметра будут определяться с помощью опросов среди пользователей.

Эти изменения не повлияют на количество новостей, которые попадают в новостные ленты, однако такие сообщения будут более полезными для пользователей. Тестирование новых алгоритмов начнётся «в ближайшие недели», сначала изменения затронут США, а затем будут распространены на весь мир.

В начале января Цукерберг объявил, что в 2018 году Facebook планирует уменьшить долю ссылок на новости в лентах. Он рассчитывает, что этот

показатель сократится с 5 % до 4 %, чтобы пользователи больше общались с друзьями и близкими, а не пассивно потребляли информацию. Представители СМИ уже возмутились из-за возможного падения охватов в соцсети.

«В современном мире слишком много сенсаций, дезинформации и полярных мнений. Социальные медиа позволяют людям распространять информацию быстрее, чем когда-либо прежде – если мы не будем устранять такие проблемы, то в итоге окажется, что мы их только усиливаем. Вот почему важно, чтобы новостная лента поддерживала качественные новости, которые создавали бы ощущение общеё почвы для пользователей», – написал глава Facebook.

(вгору)

Додаток 3

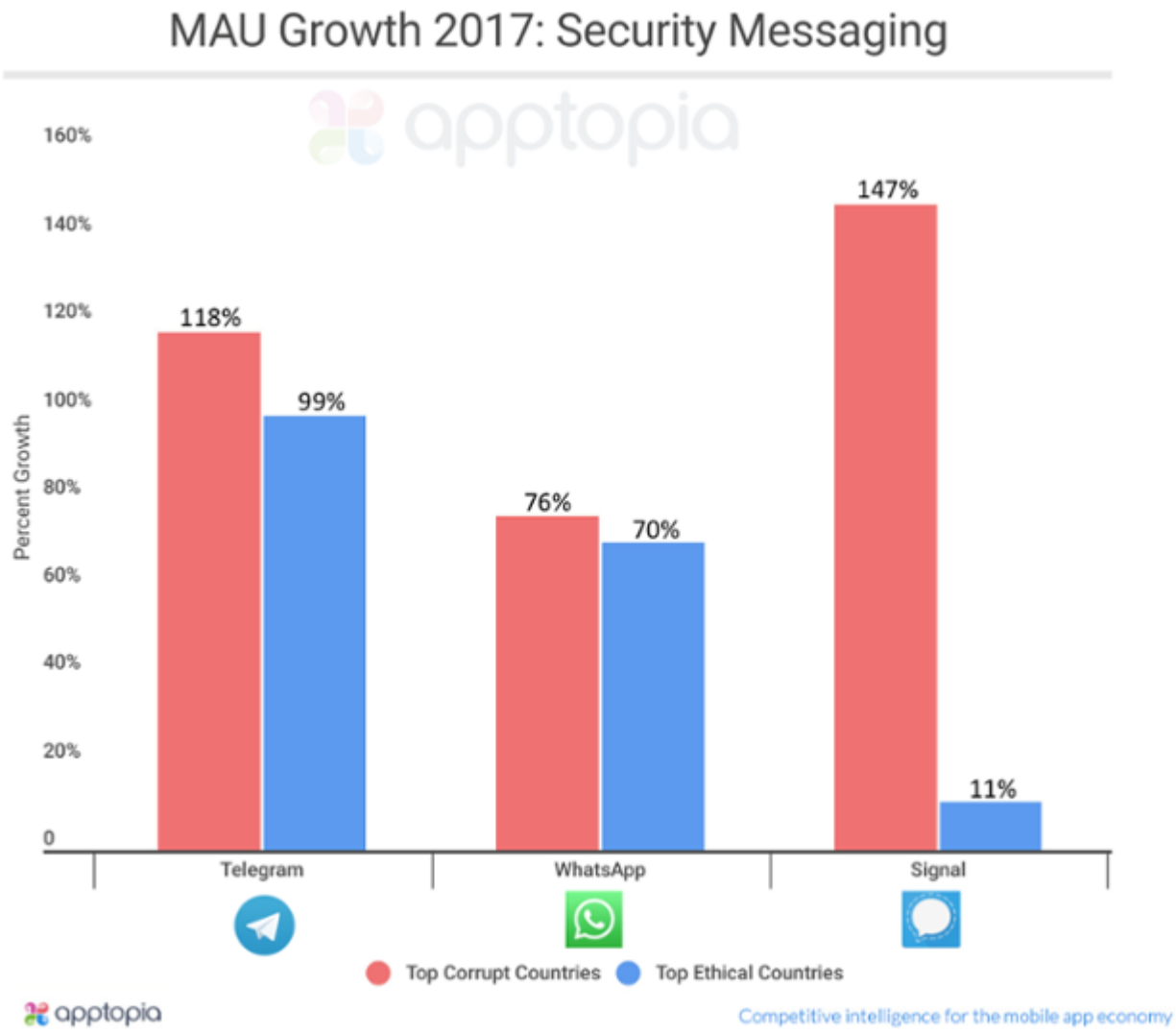
24.01.2018

Павел Красномовец

Защищенные мессенджеры Telegram и Signal растут быстрее в коррумпированных странах. В том числе и в Украине

Самые популярные мессенджеры в мире WhatsApp и Facebook Messenger имеют миллиардные аудитории. Но в некоторых случаях темпы их роста уступают конкурентам, особенно в специфических нишах. Американская аналитическая компания Apptopia провела исследование, в котором сравнила скорость роста аудитории защищенных мессенджеров Signal и Telegram с WhatsApp в благополучных и коррумпированных странах (AIN.UA).

В Apptopia проанализировали рост активных месячных пользователей трех мессенджеров за 2017 год в десяти государствах: пяти наиболее и наименее коррумпированных. Уровень взяточничества определялся согласно индексу восприятия коррупции Transparency International. В когорту «коррумпированных» попали Венесуэла, Нигерия, Кения, Россия и Украина. В группу «этичных» исследователи отнесли Данию, Швецию, Швейцарию, Финляндию и Новую Зеландию.



WhatsApp в прошлом году рос примерно одинаково в обоих группах стран. Мессенджер Павла Дурова, который стал одним из первых сервисов, делавших акцент на защищенность и шифровании, вырос в коррумпированных странах на 20 % больше, чем в добропорядочных.

Если в безопасности Telegram еще могут быть сомнения, учитывая происхождение основателя и периодически сообщения СМИ о взломах, то Signal имеет имидж самого защищенного. Этот сервис рекомендует в том числе и Эдвард Сноуден. Львиную долю роста мессенджеру принесли пользователи именно в коррумпированных странах – 147 % увеличения месячной аудитории против 11 % в развитых странах.

В общемировых показателях Signal снова показал свою нишевость. Количество его пользователей выросло в 2017 году на 20 %. WhatsApp, несмотря на текущую аудиторию в более чем 1,3 млрд, вырос на 64 %. Telegram же показал темпы почти вдвое быстрее – 112 %. Мессенджер Дурова за прошлый год загрузили 94,2 млн раз, а 80 % установок пришлось на магазин приложений Google Play.

(вгору)

Додаток 4

24.01.2018

Компания Facebook ввела новую единицу измерения времени

Мы с вами привыкли к тому, что время измеряется в секундах, минутах, часах, месяцах, годах и так далее. В случае, когда требуется высокая точность, мы прибегаем к миллисекундам или наносекундам. Казалось бы, зачем изобретать колесо и вводить совершенно новую единицу измерения времени, когда устоявшаяся система прекрасно себя зарекомендовала? Но компания Facebook так не считает. Специально для создателей инновационного визуального контента (эффектов для фильмов, виртуальной реальности и прочего) была введена абсолютно новая единица измерения, в которой измеряется время. Знакомьтесь – «флик». Своим названием эта единица обязана словам «frame» («кадр») и «tick» («пометка») (IGate).

Флик придумал Кристофер Норват – бывший сотрудник Facebook, работавший в ныне закрывшейся студии Oculus Story Studio. Один флик эквивалентен 1/705600000-й секунды, или 1,417 наносекунды. В Facebook выбор подобной продолжительности флика объясняют максимально доступным языком. Когда вы работаете над созданием визуальных эффектов для кино, телевидения или виртуальной реальности, вам приходится пользоваться симуляцией или другими процессами, разбивающими единичный кадр на фиксированное целое число мелких отрезков. Например, длительность одного кадра в стандартном видео с частотой 24 кадра в секунду составляет 0,0416666666666667 секунды. Производить математические вычисления с такими числами не очень удобно, а если эти значения округлять, собьётся точность синхронизации.

Введение новой единицы измерения времени позволит увеличить точность синхронизации и упростить математические операции с кадрами видео. Например, длительность кадра при 24 fps составит 29 400 000, при 25 fps – 28 224 000, а при 120 fps – 5 880 000 фликов. Заметьте, что теперь нет никаких лишних цифр после запятой. Флик также позволит максимально комфортно работать с высокочастотными камерами. При частоте съёмки 192 000 кадров в секунду продолжительность одного фрейма составит 3675 фликов. Именно поэтому было важно сделать флик таким коротким по времени. Помимо всего прочего, флик идеально сочетается с монтажным аудио наиболее распространённых частот от 8 до 192 килогерц. Facebook очень надеется, что в будущем флик станет общепринятой единицей измерения времени в популярных программах для создания видеоконтента и монтажа.

(вгору)

Додаток 5

29.01.2018

Twitter начал понимать, где на фотографии находится самая важная ее часть

Польза машинного обучения не всегда кроется в крупных функциях – зачастую оно помогает привнести некое мелкое нововведение, которое делает продукт гораздо более удобным. Так произошло и в случае с Twitter, которая с помощью нейронных сетей начала обрезать наиболее интересные части фотографий для создания их миниатюр (IGate).

Компания начала работать над нововведением уже достаточно давно, но подробно рассказала о нём лишь сейчас. Исследователь в области машинного обучения Лукас Тис (Lucas Theis) и его руководитель Зехан Вонг (Zehan Wang) поведали, что сначала обрезали с помощью новой функции только лица, а вот с пейзажами, предметами и кошками метод не работал.

Решением проблемы стал метод «обрезания с использованием заметной части». Под «заметной частью» в данном случае подразумевается самая интересная часть картинки – неважно, лицо это или нет. Сотрудники Twitter воспользовались данными исследований в области отслеживания глаз для определения зон изображений, на которые люди смотрят в первую очередь. «Эти данные могут использоваться для тренировки нейронных сетей и алгоритмов, прогнозирующих, на что человек хочет бросить взгляд», – написали Тис и Вонг.

Когда исследователи научили нейронную сеть определять такие зоны, им потребовалось оптимизировать технологию, чтобы она работала на сайте в реальном времени. К счастью, обрезание фотографий для создания миниатюр довольно простое – достаточно выделить примерно треть картинки с самым привлекательным содержимым. Это позволило сузить критерии отбора материала.

В результате получилась нейронная сеть в 10 раз более быстрая, чем первоначальный вариант. «Это позволяет нам производить обнаружение заметной части на всех изображениях по мере их загрузки и обрезать их в реальном времени», – добавили Тис и Вонг.

Вскоре нововведение станет доступно всем пользователям Twitter на настольных устройствах, а также в приложениях для iOS и Android.

(вгору)

Додаток 6

30.01.2018

Чатбот Facebook получит биографию и научится «болтать ни о чем»

Чатботы сносно помогают в решении конкретных вопросов пользователей, но совсем не умеют просто болтать. В Facebook рассудили, что в беспредметных диалогах должна проявляться личность собеседника – и в случае с чатботом ее придется создать с нуля (InternetUA).

Facebook собирается исправить недостатки предыдущего виртуального помощника в новой версии чатбота. От использования «М», даже экспериментального, соцсеть отказалась осенью прошлого года. Оказалось, что

бот требует постоянных доработок и отнимает очень много времени разработчиков. Но, вопреки прогнозам о смерти технологии в целом, исследования в этой области продолжаются. И специалисты намерены решить неожиданно трудную задачу: научить бота поддерживать беспредметную беседу.

Как отмечает The Verge, ботам прилично удается помогать пользователям в решении конкретных задач: задавать вопросы, ответы на которые ведут к конкретным действиям. Один из первых успешных чатботов ELIZA, разработанный в 1960-х, делал именно так – задавал общие вопросы. Совсем другое дело – бесцельный разговор, болтовня. Разобраться в его структуре и подводных течениях гораздо сложнее.

Обычно для обучения бота здесь использовался массив фраз из фильмов. Однако реальные диалоги показали, что такой ИИ-собеседник часто отвечает невпопад, забывает, о чем говорил раньше и странно шутит – если это вообще шутки. Специалистам Facebook надо было придумать что-то универсальное и в то же время простое, чтобы не повторился опыт трудоемкой разработки «М».

Они выявили самую трудную точку диалога – его начало. Заговорить с незнакомцем может быть проблемой и для людей. И, чтобы боту было проще сформулировать первую мысль, его решили наделить некоторыми чертами биографии. Назвали новую технологию Persona-Chat. Опорные точки очень просты, например: «Я художник. У меня четверо детей. Недавно завел кошку. Люблю гулять и упражняться. Люблю смотреть «Игру престолов».

Второй частью задачи стало обучение бота новым фразам и ходам – тут тоже понадобилась иная система. Теперь для этих целей используют разработку Amazon Mechanical Turk – площадку для назначения работникам-людям задач по обучению ИИ. Их просили сравнить диалоги с Persona-Chat, обычным «фильмовым» чатботом и живым человеком. И хотя пока Persona не так раскованна и последовательна, как люди, она намного лучше прежних версий.

Например, в одном из диалогов Persona-Chat все время сводит разговор к своему прописанному в биографии любимому делу — «писать книги». Издание отмечает, что это было больше похоже на настоящее общение. Однако при этом участники эксперимента указывают, что бот стал скучнее. Впрочем, это присуще и некоторым людям.

(вгору)

Додаток 7

30.01.2018
Ирина Фоменко
Социальные медиа достигли пика в политике

Когда предстоят промежуточные выборы 2018 года в США (и мы начинаем говорить о президентской гонке 2020 года), не возникает никаких сомнений, что кандидаты и дальше будут использовать Facebook, Twitter и другие медиа платформы, чтобы сплотить своих сторонников (InternetUA).

«Социальные медиа достигли своего пика в качестве влиятельного игрока в политике», – считает модератор Meet the Press, директор политических новостей NBC Чак Тодд.

В последнем эпизоде Recode Decode, размещенном Карой Свишер, Тодд утверждал, что у каждого в социальной сети есть своя точка зрения, и человек будет воспринимать твиты и посты просто как еще одну тактику, а не как истинное мнение или поведение политика.

«Они больше не могут быть незапланированными, не могут нас удивлять. Нет никаких новых методов использования социальных медиа для политики; все про них уже знают. Будет что-то еще», – прокомментировал Тодд.

«На мой взгляд, следующим будет персонализация политики», – добавил он. – «Сейчас мы персонализировали ее вплоть до ваших кабельных каналов и лент новостей. Что будет дальше: мы увидим рекламу Trump-for-president, но ваша реклама будет касаться того, что непосредственно может вызвать у вас интерес».

В новом подкасте Тодд также рассказал о том, почему он отвергает идею о расколе в современной политике из-за технологий. Вместо этого он рассматривает их как силу, которая ускорила тенденции, появившиеся после Уотергейта.

«Роджер Аайлс создал эту культуру – он работал медиаконсультантом у Ричарда Никсона. Поэтому идея “предвзятых СМИ” началась именно с Уотергейта», – заявил Тодд. – «Я думаю, что влияние СМИ преувеличено. Если медиа настолько влиятельны, то как Дональд Трамп стал президентом? Ни одна редакционная коллегия в стране не заявила, что он должен быть президентом. Аайлс создал из медиа целую бизнес-модель, с “честными киваниями и подмигиваниями”. Он вел политическую тактику, чтобы выиграть выборы, а затем превратил ее в тактику СМИ».

(вгору)

Додаток 8

22.01.2018

Александр Симудров

Мимо кассы: как делать платежи с помощью Telegram и мобильных денег

Сфера финансовых услуг меняется во всем мире. Деньги становятся все более виртуальными, а пластиковые банковские карты уже начинают устаревать. Украинцы чувствуют эти изменения и все чаще пользуются технологией бесконтактных платежей NFC, изучают преимущества mobile-only банкинга, интересуются криптовалютами и создают общественные организации вроде Bitcoin Foundation Ukraine (AIN.UA).

Отечественный разработчик Hubbot также старается сделать украинский бизнес более современным. На данный момент командой создано 16 ботов, в которых можно расплачиваться за услуги за пару кликов. Теперь оплачивать

покупки через Telegram стало еще проще – с помощью мобильных денег «Киевстар».

Прежде, чем приступить к обзору новшества – мобильных денег «Киевстар» в ботах Hubbot, я поинтересовался, как осуществляются денежные транзакции и списание средств со счета. Оказалось, что мобильные деньги работают на основе платежной системы EasyPay. Правила ее использования зарегистрированы в НБУ, потому в надежности операций можно не сомневаться. Ранее я использовал боты Hubbot для покупки билетов на киносеансы. Платежные операции с банковской картой всегда осуществлялись быстро – в ботах этот процесс автоматизирован и нет необходимости многократно вводить реквизиты. Зачем же тогда нужны мобильные деньги «Киевстар» и в чем преимущества такой платежной технологии? Узнаем прямо сейчас.

Оплата мобильными деньгами «Киевстар» доступна в ботах для заказа билетов на киносеансы: «Киноафиша», Кинотеатр «Жовтень», «Кінопалац» и «Оскар». Разработчики обещают в скором времени добавить такую опцию и в другие боты, что особенно актуально для бота для доставки воды по Украине Delivery of water.

Воспользоваться опцией можно, если вы абонент предоплаченной связи «Киевстар». В других случаях приобрести билеты можно с использованием банковской карты.

Для тестирования мобильных денег я выбрал свой любимый киевский кинотеатр «Жовтень». Открываю бот «Жовтня» в Telegram, задаю команду /start, бот приветствует меня и предлагает выбрать дату и сеанс. Навигацию можно осуществлять как по дате сеанса, так и по репертуару.

Определившись с датой и интересующей меня картиной, выбираю удобное время нажатием на соответствующую кнопку. После этого бот предлагает выбрать места в зале – вручную или автоматически. При ручном выборе на экране появляется схема зала с доступными местами.

После выбора мест, бот бронирует билеты на 15 минут, чтобы никто не мог выкупить их раньше вас. После этого самое интересное – оплата.

Раньше я оплачивал покупки в ботах банковской картой. Мои реквизиты были сохранены, и платеж производился автоматически в течение нескольких секунд. Теперь в интерфейсе бота появилась кнопка «Мобильные деньги Киевстар». Выбираю именно этот способ оплаты и бот просит указать, свой номер телефона. «Киевстар», разумеется. Затем на номер отправляется SMS-подтверждение с кодом, который нужно набрать и отправить боту. Через несколько секунд бот отправляет билет со штрих-кодом и информацией о сеансе.

До осуществления платежа на моем мобильном счету было 140 грн. После оплаты билета стоимостью 98 грн. баланс составил 42 грн., а значит никакой дополнительной комиссии по транзакции не взимается. При повторной оплате вводить номер телефона не нужно. Так же мобильные деньги работают и в других ботах для покупки билетов от Hubbot: «Киноафиша»,Кинотеатр

«Жовтень», «Кінопалац» и «Оскар». Разработчики обещают вскоре добавить эту опцию во все остальные свои боты.

Для меня такой способ оплаты по скорости транзакции равносилен оплате картой, ведь в ботах Hubbot платежи автоматизированы и повторно вводить реквизиты не нужно. Но если обычный способ оплаты недоступен, а вам необходимо быстро осуществить платеж, то мобильные деньги «Киевстар» – очень удобная опция. А если банк при оплате взимает комиссию, то использовать мобильные деньги еще и выгоднее.

(вгору)

Додаток 9

23.01.2018

Facebook инвестирует в повышения цифровой грамотности малого бизнеса ЕС

Facebook сообщила 22 января, что рассчитывает к 2020 г. предоставить возможности цифрового обучения для миллиона жителей ЕС, включая владельцев малого бизнеса. С этой целью компания, в сотрудничестве с местными властями, откроет три социальных центра повышения квалификации – в Испании, Польше и Италии (Компьютерное Обозрение).

Её специализированное предложение для среднего и малого бизнеса будет включать онлайновые курсы для 250 тыс. предпринимателей и занятия в обычных классах для ещё 100 тыс.

В течение следующей пары лет, Facebook вместе с Freeformers охватит обучением ещё 300 тыс. человек в Великобритании, Франции, Германии, Польше, Италии и Испании.

Предполагается, что получаемые на этих курсах навыки пользования цифровыми технологиями буду ориентированы на индивидуальные потребности занимающихся: кто-то будет учиться программировать, а кто-то – создавать учётные записи в онлайновом банке.

Кроме того Facebook инвестирует 10 млн евро в свой парижский центр исследований искусственного интеллекта. Это позволит увеличить его персонал с 10 до 40 человек, имеющих научную степень, и удвоить число инженеров – с 30 до 60 человек. Предусмотрено дополнительное финансирование стипендиальных грантов и десяти серверов с открытыми базами данных для французских публичных организаций.

В ноябре прошлого года, аналогичную просветительскую инициативу компания анонсировала для 30 городов США. С 2011 г. на поддержку небольшого бизнеса во всём мире Facebook израсходовала более миллиарда долларов.

(вгору)

Додаток 10

24.01.2018

Ирина Фоменко

Почему биг-боссы социальных сетей не используют свои платформы?

Разработчики таких платформ, как Facebook, признали, что социальные медиа были спроектированы таким образом, чтобы они вызывали привыкание. Должны ли мы следовать примеру руководителей и отказаться от социальных сетей (InternetUA)?

Марк Цукерберг не пользуется Facebook – согласно Bloomberg, у 33-летнего исполнительного директора есть команда из 12 модераторов, которые удаляют комментарии и спам с его страницы. Также сотрудники помогают ему писать посты, а профессиональные фотографы делают снимки Цукерберга с ветеранами в Кентукки или владельцами малого бизнеса в Миссури. Об этом сообщает издание The Guardian.

Ограничения Facebook не позволяют нам видеть посты Цукерберга на его профиле. Это относится не только к основателю социальной сети. Ни у кого из руководителей компании нет своей страницы на Facebook. Вы не можете добавить их в друзья, они редко делают публикации и не раскрывают конфиденциальную информацию, которую Facebook предлагает обнародовать по умолчанию, например, количество друзей.

С Twitter та же история. В среднем, из девяти руководителей компании всего четверо пишут твиты более одного раза в день. Финансовый директор Нед Сигал зарегистрирован в Twitter уже 6 лет, а пишет твиты не более двух раз в месяц. Соучредитель сети Джек Дорси написал около 23 тысяч твитов с момента запуска Twitter, но это намного меньше, чем другие пользователи написали за тот же период. Дорси редко отвечает незнакомым людям и избегает обсуждений или споров на сайте. Он действительно практически не использует Twitter, просто пишет в нем время от времени.

Пока вся отрасль сфокусирована на использование собственных сервисов, самые заядлые пользователи социальных сетей редко оказываются руководителями.

Многие пользователи социальных медиа не понимают, почему руководители не используют собственные платформы – ведь в социальных сетях они регулярно сталкиваются с ошибками, злоупотреблениями или плохими проектными решениями, которые руководители никогда не смогли бы понять, не используя сайты.

Сооснователь Facebook Шон Паркер в октябре прошлого года на конференции в Филадельфии заявил, что он отказался от социальных сетей из собственных соображений. «Главная идея, которой мы руководствовались при создании Facebook, была: “Как можно привлечь ваше внимание еще больше и как заставить вас тратить на нас свое время?” Каждый раз нам нужно давать вам дозу дофамина, например, кто-то лайкнул или прокомментировал вашу фотографию. Это заставляет вас делать больше публикаций, что, в свою очередь, позволяет получать больше лайков и комментариев», – рассказал Шон

Паркер. – «Это цикл социальной ответной реакции (фидбэк) – мы используем уязвимости в человеческой психологии. Основатели – я, Марк Цукерберг, Кевин Систром (Instagram) – мы понимали это. И все равно создали социальные сети».

Через месяц к Паркеру присоединился еще один «протестующий» против Facebook, бывший вице-президент по привлечению пользователей Чамат Палихапитья. «Краткосрочный цикл ответной реакции, который мы создали, разрушает общество. Нет гражданского дискурса, нет сотрудничества, только дезинформация и ложь. Это глобальная проблема – она разрушает то, как люди ведут себя друг с другом. Я могу контролировать свое решение, а, значит, я не использую социальные сети. Я могу контролировать решения своих детей – значит, им также запрещено пользоваться соцсетями», – заявил Чамат Палихапитья на конференции в Стэнфорде.

Заявления Чамата негативно отразились на Facebook – компании пришлось оправдываться за свои прошлые неудачи. «Когда Чамат работал в Facebook, мы были сосредоточены на развитии и популяризации Facebook по всему миру. Facebook тогда был совсем другой компанией. Сейчас мы выросли и поняли, насколько важны наши обязанности. Мы очень серьезно относимся к нашей роли, и прилагаем все усилия для улучшения Facebook», – прокомментировала пресс-секретарь компании.

Несколько дней спустя Facebook опубликовал данные исследований, согласно которым пользователь социальной сети чувствует себя плохо, если редко делает публикации. «В целом, когда люди тратят много времени, пассивно потребляя информацию, – читают, но не взаимодействуют с людьми, – пользователи после этого чувствуют себя только хуже. В свою очередь, активное взаимодействие между людьми – особенно обмен сообщениями и комментариями с близкими друзьями – значительно улучшают настроение пользователя», – говорится в исследовании.

Психолог Адам Алтер считает, что влияние социальных медиа на настроение человека не является серьезной проблемой – гораздо хуже то, что такие платформы вызывают привыкание. «Концепция зависимости гораздо шире и применяется к большему количеству поведенческих действий, чем мы думали, а потому касается гораздо большего числа людей. Примерно половина взрослого населения имеет хотя бы одну поведенческую зависимость. У многих из нас ее нет, но сейчас в мире существует очень много привычек, которым нам трудно противостоять», – заявляет Адам.

Алтер утверждает, что зависимость «случайно» не появляется – это прямой результат намерений таких компаний, как Facebook и Twitter, создающих «цепкие» продукты, которые мы с каждым днем хотим все больше использовать. «Компании создают такие платформы с целью “зацепить” пользователя. Они делают все возможное, чтобы мы тратили все свое время на их медиа. Основная цель таких компаний – создать продукт, от которого люди будут зависимы и не смогут перестать его использовать», – считает Алтер. – «Паркер и Чамат делают все возможное, чтобы “взломать” человеческую

психологию и понять, что именно вызывает привычку у людей, а затем использовать это для того, чтобы максимизировать взаимодействие человека и социальной сети».

Паркер и Палихапитья – не единственные жители Силиконовой долины, которые рассказывают о своем отказе от современных технологий, вызывающих зависимость. Как сообщало издание в октябре, все больше программистов и дизайнеров уходят с работы, разочаровываясь в том, чем они занимаются. Например, Крис Марчеллино – один из разработчиков службы push-уведомлений Apple – покинул компанию, чтобы стать нейрохирургом.

У многих возникает такая же проблема, но они мирятся с ней – например, консультанты Dopamine Labs. Компания предлагает расширение для приложений, персонализирующее «моменты радости» в них.

Исходя из этих соображений, руководители социальных медиа не используют собственные платформы. «Многие титаны новых технологий очень осторожно пользуются социальными сетями и следят за тем, как их используют дети. Кроме того, обычно они ограничивают доступ детей к планшетам, различным приложениям и программам. Несмотря на то, что руководители заявляют всем, что “это самый лучший продукт”, они сами не используют его и не разрешают своим детям», – прокомментировал Алтер.

На прошлой неделе исполнительный директор Apple Тим Кук сообщил The Guardian: «У меня нет ребенка, но у меня есть племянник, которому я запрещаю некоторые вещи. Есть то, что я не могу допустить – чтобы он был в социальной сети. Сама по себе технология ни хорошая, ни плохая – именно человек решает, какой ей быть».

По словам Алтера, классическим примером такого подхода является позиция Стива Джобса, который рассказывал о достоинствах iPad всему миру, но сам не позволял своим детям даже приближаться к планшету.

Впрочем, утверждает Алтер, не только дети осторожничают в использовании социальных сетей. Такого же мнения придерживается Джек Дорси – он очень мало времени проводит в Twitter. Тем не менее, это не относится к остальным пользователям Twitter – многие утверждают, что они зависимы от этой социальной сети. «Я уверен в том, что Twitter – это просто черная дыра, которая затягивает вас все сильнее и сильнее, и почти невозможно прекратить ее использовать», – заявил Алтер.

Разработчик Кевин Холеш является одним из тех, кто пытался минимально использовать социальные сети. Он написал программу, которая отслеживает, сколько времени вы ежедневно тратите на свой телефон. Для обычного пользователя – это около трех часов. Статистика Холеша была достаточной, чтобы обеспечить мотивацию к изменениям. «Как только у меня появились эти данные, я стал меньше использовать свой телефон. С тех пор я сделал несколько шагов в этом направлении и тратил всего час в день на смартфон», – рассказал Холеш.

В конечном итоге Кевин удалил все социальные сети и свою учетную запись электронной почты с телефона. «Этот шаг помог мне больше всего.

Сначала моей целью было просто узнать, сколько нужно потрать времени на смартфон, чтобы стать счастливее. Но теперь я понял, что лучше чувствую себя, не когда читаю новости или публикации на Facebook, а когда общаюсь с людьми вживую», – прокомментировал Кевин.

По словам психолога, сила воли может помочь в борьбе с зависимостью, однако лучшим решением будет удаление всех социальных медиа с телефона. Тем не менее, считает Алтер, в одиночку сложно избавляться от привычек.

«Возможно, что через 20 лет мы оглянемся на нынешнее поколение детей и скажем: “Послушайте, они же отличаются от всех других поколений, и это огромная проблема. Возможно, нам стоит контролировать их поведение”. Или, может, мы скажем: “Я не знаю, почему мы так беспокоились”. Пока у нас нет доказательств или каких-то заметных результатов, поэтому будет невероятно сложно изменить человеческое поведение», – заявил Алтер.

Если вы не можете заставить себя отказаться от социальных сетей, попробуйте последовать примеру Цукерберга – нанять команду из 12 человек, чтобы они занимались этим за вас. Это может быть не так дешево и просто, как удаление Facebook, но, вероятно, такой стратегии поведения будет легче придерживаться.

(вгору)

Додаток 11

20.01.2018

Twitter обнаружил более 3 тыс. аккаунтов, связанных с российской «фабрикой троллей»

Администрация Twitter обнаружила 1062 аккаунта, связанных с российским «Агентством интернет-исследований», также известным как «фабрика троллей», сообщается в официальном блоге соцсети (InternetUA).

Эти аккаунты были заблокированы за спам и нарушение правил пользования социальной сетью.

Twitter провел исследование страниц пользователей и контента за период в 10 недель до выборов американского президента в 2016 году.

«За исследуемый нами период 3814 идентифицированных аккаунтов, связанных с “Агентством интернет-исследований”, разместили 175 993 твитов, из которых около 8,4% были связаны с выборами», – сказано в сообщении.

Компания представила полученные сведения Конгрессу США. Кроме того, администрация соцсети уведомила 677 тыс. пользователей в том, что они делали «ретвиты» и «лайкали» записи аккаунтов, связанных с российской пропагандой.

Facebook, Twitter и Google подозревают Россию в использовании их интернет-платформ для вмешательства в избирательную кампанию в США. 31 октября 2017 года представители этих компаний давали пояснения в Конгрессе Соединенных Штатов.

Ученые университета Свонси и Калифорнийского университета в Беркли пришли к выводу, что Россия с помощью ботов в Twitter пыталась повлиять на голосование по Brexit, писало издание The Times.

В докладе Robotrolling Центра передового опыта НАТО по стратегическим коммуникациям говорилось, что 60 % всех русскоязычных учетных записей в Twitter имеют признаки того, что их ведут автоматизированные программы.

(вгору)

Додаток 12

24.01.2018
Екатерина Шпачук
IT-гиганты потратили рекордную сумму на лоббирование в 2017 году

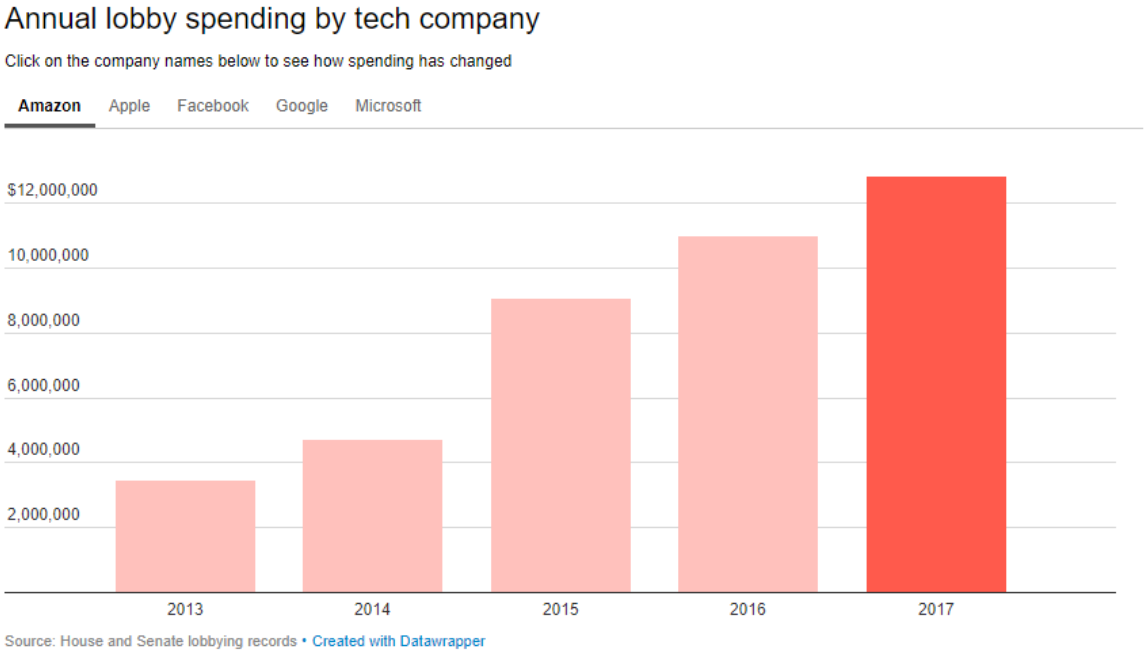
В 2017 году компании Apple, Amazon, Facebook и Google потратили рекордные 50 миллионов долларов на лоббирование в правительстве США. Об этом сообщает издание Recode (InternetUA).

Отмечается, что IT-компании противостояли новым федеральным правилам администрации Дональда Трампа. Это означает, что технологическая отрасль в США все больше и больше находится под политическим влиянием.

В течение 2017 года крупнейшие IT-компании «сражались» с Белым домом за сохранение принципа сетевого нейтралитета, но потерпели поражение. Кроме того, они пережили расследование конгресса по делу о распространении российскими троллями пропаганды через их платформы во время последних выборов в США.

Технологические компании подвергались усиленным проверкам и критике за все, начиная секс-торговлей и заканчивая фейковыми новостями. Именно это побудило ряд компаний тратить больше средств на лоббирование в правительстве США. Отмечается, что в 2018 году ожидается еще больший прессинг отрасли.

В прошлом году самым «щедрым» политическим спонсором среди IT-компаний была Google, которая выделила более 18 миллионов долларов на лоббирование своих интересов в правительстве. Как и другие технологические гиганты, Google стремилась помешать внедрению новых правил, касающихся контента и рекламы.



В свою очередь, компания Amazon потратила более 12,8 миллионов долларов на лоббирование в 2017 году – почти в четыре раза больше, чем четыре года назад. Среди сферы интересов компании – онлайн-налоги на продажи, облачные вычисления и доставка посылок с помощью дронов.

Facebook не сильно отстала от своих «коллег», потратив на лоббирование 11,5 миллионов долларов – рекордную для себя сумму. Социальной сети пришлось защищаться из-за фейковых новостей и другого контента, который появлялся в ленте пользователей.

Apple тоже потратила на лоббирование рекордные для себя 7 миллионов долларов. Компания продолжала настаивать на вопросах, касающихся шифрования и иммиграции. Apple, как и вся технологическая индустрия, выступала за закон о налоговой реформе, недавно подписанный Трампом.

Apple и Facebook отказались от комментариев относительно лоббирования. Amazon и Google медлили с ответами на запросы журналистов.

Для технологического мира тяжелый период начался со вступления Дональда Трампа в должность. В частности, когда новоизбранный президент США подписал распоряжение, ограничивающее права иммигрантов и беженцев из мусульманских стран. Документ, в том числе ограничивал деятельность высококвалифицированных иностранных специалистов.

Недавно технологические гиганты, такие как Amazon, Apple, Facebook, Google и Microsoft, использовали свое огромное лобби для возрождения программы, известной как DACA – программа помощи несовершеннолетним детям незаконных мигрантов. Во время согласования бюджета 19 января сенаторы-демократы отказались принимать документ. В результате 20 января работа всех федеральных ведомств была приостановлена, а значительная часть служащих отправлены в неоплачиваемый отпуск.

Для таких компаний, как Facebook, Google и Twitter, 2017 год ознаменовался бесконечными расследованиями по делу дезинформации в лентах социальных сетей.

Некоторые законодатели пытались внедрить новые федеральные правила для технических компаний по выдаче политических сообщений в ленте новостей. Но Facebook, Google и Twitter использовали максимум своих усилий, чтобы так называемый Закон о честной рекламе не был принят.

Кроме того, это трио боролось с инициативой о том, чтобы социальные сети и рекламные агентства были ответственны за то, что они позволили или не смогли выявить сексуальную торговлю на своих платформах. Эти и другие технические гиганты активно лоббировали в 2017 году сохранение принципа сетевого нейтралитета, который Федеральная комиссия (FCC) окончательно отменила в декабре.

Эти три вопроса – политические сообщения, сексуальная торговля и сетевой нейтралитет все еще остаются нерешенными. Между тем законодатели и федеральные регуляторы начинают подвергать сомнению «полезность» социальных сетей. Так, председатель FCC Аджит Пай стал одним из самых ярых критиков «недостатков» социальных сетей.

Между тем, компания Uber также потратилась на лоббирование среди законодателей и федеральных регуляторов в прошлом году. В 2017 году компании надо было решать вопросы по обвинению в сексизме, численные расследования по деловой практике и серьезные нарушения безопасности данных.

(вгору)

Додаток 13

24.01.2018

Таинственная структура сдает правительствам в аренду ПО для слежки за собственными гражданами

Обнаружена платформа Dark Caracal, сдаваемая в аренду правительствам разных стран для шпионажа и слежки за гражданами (InternetUA).

«Дикая кошка» в темной комнате

Фонд электронных рубежей (EFF) совместно с компанией Lookout, занимающейся вопросами сетевой безопасности, объявили об обнаружении шпионской платформы Dark Caracal (степная рысь), которую некие неизвестные пока разработчики предлагает правительствам разных стран для шпионажа и слежки за собственными гражданами. На данный момент известно, что платформу использует Директорат общей безопасности Ливана – разведывательное агентство, которое уже вытянуло гигабайты информации из мобильных устройств на базе Android и ПК на базе Windows.

Ранее ту же инфраструктуру предположительно использовало правительство Казахстана в рамках своей «Операции “Манул”», направленной, по данным EFF, против журналистов, политических активистов и членов их семей. Описание операции было представлено ещё в 2016 году на конференции Black Hat.

По мнению экспертов EFF и Lookout, существует некая «третья сторона», которая занималась разработками платформы, а затем стала сдавать ее в аренду.

В настоящее время EFF и Lookout пытаются установить подлинных авторов Dark Caracal. Очевидно, какие-то сведения по этому поводу у них уже есть, но они хотят убедиться в правильности своих выводов. К лету 2018 г. ими обещана новая публикация по этой теме.

«Погладь кота!»

К настоящему моменту Dark Caracal использовался в том или ином виде для шпионажа и хищения данных у тысяч жертв в 21 странах мира, – личных документов, записей звонков, аудиозаписей, текстовых сообщений, контактных данных, а также фотографий военных объектов, правительственных учреждений и коммерческих предприятий.

Большая часть целей платформы приходится на Ближний Восток, но затронуты также США, Западная Европа, Китай и Северная Африка.

После публикации EFF досье на «Операцию “Манул”» в 2016 г. Lookout обнаружили ещё один компонент платформы Dark Caracal – вредоносную программу для Android под названием Pallas, используемый для захвата контроля над смартфонами. Pallas распространяется вместе с фальшивыми клиентами WhatsApp и Signal (устанавливаемыми из неофициальных магазинов). Pallas не использует никаких неизвестных уязвимостей, полагаясь целиком на доверчивость пользователей.

После установки на устройство, Pallas может выполнять множество разных функций – от записи аудио, до перекачивания данных на смартфоны операторов трояна.

Кроме того, исследователи обнаружили ещё одно средство слежения – FinFisher, ранее неизвестную разновидность шпионского инструмента, разработанного европейскими компаниями, специализирующимися на «законных» инструментах для слежки. Пока неизвестно, был ли он приобретен создателями Dark Caracal официально, или это взломанная и модифицированная демо-версия.

Для десктопов Dark Caracal использует троянец Bandook, распространяемый с помощью поддельных сертификатов безопасности и Word-файлов с вредоносными макросами. Bandook в случае необходимости скачивает и другие вредоносные программы с удаленных серверов.

(вгору)

Додаток 14

24.01.2018

Слежка за частной жизнью целых наций незаметно становится нормой

Помимо невинных и полезных применений, таких как борьба с вредителями, поиск новых лекарств и написание шуточных текстов, алгоритмы искусственного интеллекта и машинного обучения начали массово

использоваться, в первую очередь, для наблюдения за людьми. Этот тренд стал особо заметен во второй половине 2017 года. Как в лучших антиутопиях XX века, присутствие «Большого брата» подается как необходимая мера по повышению безопасности и борьбе с терроризмом (InternetUA).

Системы слежки и наблюдения будут внедряться повсеместно под видом оборудования для умных городов. ФБР США уже располагает обширной базой данных с фотографиями 117 млн граждан. Китай вообще перестал стесняться и собирает не только фотографии, но и ДНК своих жителей. Сколько подобных случаев пока еще просто скрыто под грифом секретности, можно только догадываться. И если не забывать, что данные – это «новая нефть», станет очевидным, что слежка за частной жизнью целых наций обещает многомиллиардные прибыли тем, кто сможет этим правильно воспользоваться.

Око Саурона – это спутник

Уже не первое десятилетие жители больших городов попадают на записи камер видеонаблюдения, которые фиксируют почти каждый шаг. Но до сегодняшнего дня мы знали, что эту видеозапись будут просматривать только в том случае, если случится что-то противозаконное. Но с появлением ИИ, который способен проанализировать каждое видео, распознать на нем каждого человека, связать его изображение с аккаунтами в социальных сетях и хранить эту информацию бесконечно долго, идея о защищенности частной жизни попадает под сомнение.

В теории, если не пользоваться общественным транспортом, не бывать в центре города и не ходить в супермаркеты, от камер можно скрыться даже жителю мегаполиса. А уж если уехать из города, то и подавно: в маленьких поселках все камеры местные жители знают наперечет, а в особенно глухих местах даже нет интернета, чтобы данные с этих камер куда-то передать.

Но на практике скрыться от камер уже сегодня гораздо сложнее, чем мы думаем. Недавно на рынке появилась камера на основе ИИ под названием DNNCam, которая может работать без интернета и практически «не убиваема», а также миниатюрная камера Caply размером с флешку.

Вполне вероятно, что нас ждет будущее по сценарию фильма «Сфера», в котором повсюду установлены мини-камеры, которые можно просто приклеить к дереву или стене. Характерно, что кульминацией фильма стал эпизод, когда во время очередной презентации пользователи «Сферы» сначала находят преступницу за 10 минут, но затем, когда они пытаются найти обычного человека без аккаунта в социальных сетях, он погибает в автокатастрофе, пытаясь скрыться от камер, установленных на дронах.

Но камеры, установленные повсюду, представляют собой только часть проблемы. Серьезнее то, что уже появился гораздо более простой способ получать изображение с улиц: высокоточные спутниковые данные. Например, спутники компании DigitalGlobe могут фотографировать объекты на поверхности Земли в мельчайших деталях. Система способна разглядеть даже книгу на столе.

Что хуже, в прошлом году DigitalGlobe заключила партнерское соглашение с Amazon, подразделением ЦРУ CosmiQ Works и Nvidia. Все они вложат громадные средства, чтобы обучить ИИ распознавать объекты и лица на спутниковых снимках. Мрачный прогноз «Сферы» на фоне этого – детская страшилка.

Обмани меня

Казалось бы, раз вопрос стоит настолько остро, почему бы жителям мегаполисов просто не носить головные уборы, солнечные очки или медицинские маски, как в Азии? Закрывают же автолюбители свои номера от камер, снимающих нарушения ПДД. Но все не так просто. Благодаря новым технологиям человека можно опознать и другими способами.

Например, ученые из Университета Центральной Флориды и Университета Карнеги-Меллон разработали технологию, которая может идентифицировать человека не по лицу целиком, а по его отдельным частям – глазам, носу или рту. Разработка ученых решила проблему «закрытого лица», когда для распознавания есть помехи, например, если лицо закрыто рукой, что было особенно сложным, так как рука и лицо похожи по цвету и текстуре. А ученые из Гонконгского баптистского университета научили ИИ распознавать человека по движениям губ.

Но даже если человеку удастся полностью скрыть лицо от камер, система все равно его распознает. В Китае создали метод, способный идентифицировать человека по походке с 50 метров за долю секунды. Благодаря технологии анализа в реальном времени обнаружить человека можно даже в большой толпе.

Но и это еще не все. Стартап Evolv Technology разработал микроволновые сканеры с ИИ, которые могут досматривать людей без их ведома, пока они просто проходят мимо. Теоретически разработка предназначена для аэропортов, чтобы экономить время пассажиров, но нет никакой гарантии, что ее не будут использовать для контроля за гражданами.

Слишком умный дом

Угрозу конфиденциальности несут не только привычные меры наблюдения в общественных местах. Благодаря «удобным» технологиям сбываются самые худшие опасения в духе Замятина и Оруэлла о тотальном контроле над людьми прямо у них дома. Умные звонки и умные замки расскажут, кто и когда посещал квартиру, IoT-счетчики выдадут количество израсходованных воды и электричества, а виртуальные помощники сохранят на своих серверах улики.

Например, умная камера Kuna Systems с помощью ИИ непрерывно оценивает все, что находится в ее поле зрения. Устройство умеет распознавать подозрительное поведение и призвано защитить владельца от краж. Однако это работает и в обратную сторону: устройство способно шпионить за хозяином. В случае, если он сам совершает преступление, умная камера не будет молчать и также заявит в полицию. Создатели говорят, что это будет использоваться только в случае особо тяжких преступлений. Но что если система будет

отслеживать и менее ясные случаи, например, «непатриотичное» или «потенциально опасное» поведение? Предмет контроля не так важен: важен сам факт возможности подобной слежки.

Многие современные устройства могут выступать в качестве свидетелей, причем совершенно случайно. Это произошло с колонкой Amazon Echo, которая находилась в доме предполагаемого преступника. Полиция сочла аудиоданные на устройстве потенциальными уликами. Также в ночь предполагаемого убийства в доме умные счетчики воды зарегистрировали расход более 500 литров. Предполагается, что так преступник пытался отмыть следы крови и замести следы преступления.

Марк Макардл, технический директор канадской компании eSentire говорит о том, что людям придется смириться с угрозой потери конфиденциальности, которую несут с собой устройства умного дома. Шпионами становятся смартфоны, финтес-трекеры и даже кардиостимуляторы.

На службе у государства

Правоохранительные органы все чаще стремятся использовать цифровые данные для предотвращения преступлений или терроризма. Немецкий Бундестаг недавно принял закон, который предоставляет правоохранительным органам возможность взламывать любые устройства, принадлежащие подозреваемым в совершении преступления, причем не только связанного с терроризмом. По данным Deutsche Welle, немецкие правоохранительные органы уже закупили ПО, необходимое для взлома устройств на iOS, Android и BlackBerry.

Департамент транспорта Нью-Йорка объявил, что он совершил более четырех тысяч арестов, используя технологию распознавания лиц. Вместо сканирования полицейских кадров, алгоритм сравнивает фотографии на водительских правах с изображениями из баз данных, что усложняет подделку личности мошенниками. Полиция вскоре сможет получить доступ к изображениям половины взрослых американцев через базы данных, вроде DMV.

Компания Axon, крупнейший поставщик нательных камер для полиции США, также планирует внедрять ИИ, в частности, для автоматизации полицейских отчетов. А Motorola, еще один крупный поставщик видеокамер, предлагает ИИ для идентификации лиц во время поиска пропавших детей.

Черное зеркало

Главы государств обещают, что большие данные и ИИ будут использоваться только для защиты от правонарушений, а тотальная слежка никогда не будет использована в ущерб личной свободе граждан.

Однако в Китае тестируют систему социальных кредитов, в которой гражданам присуждают или снимают баллы в зависимости от их поступков. За нарушение ПДД и жалобы в интернете рейтинг снижают, за помощь соседям и следование плану партии – прибавляют. Как сообщает официальный сайт рейтинговой системы, с помощью анализа больших данных власти учитывают 160 тыс. различных параметров. Сведения собирают по разным

государственным ведомствам, а также через доносы. Доносы, кстати, поощряются баллами, а в городе даже есть штат наблюдателей, которые следят за людьми. Кроме доносов и данных государственных и муниципальных структур, сведения будут поставлять восемь частных компаний. Среди них такие гиганты, как Alibaba и Tencent.

Нарушителей порядка будут наказывать и ограничивать, в том числе и в бытовых правах. Так, обладатели низкого рейтинга не смогут пользоваться спальными вагонами поездов и летать первым классом, а также снимать номера в дорогих отелях, отдавать детей в элитные школы и ездить за границу. На роль главного судьи Госсовет назначил Коммунистическую партию КНР.

Ситуация напоминает первую серию последнего сезона «Черного зеркала», в которой жизнь человека полностью подчиняется его рейтингу в соцсети. Наличие популярных друзей, дружелюбие и общительность открывают новые двери, а неудачи в социальной жизни перекрывают все возможности. Разница только в том, что герои сериала точно знают, за что и почему им присудили или сняли баллы. В Китае все не так однозначно, потому что точные правила проставления рейтингов нигде не зафиксированы.

Китай в стремлении к тотальному контролю и цензуре пошел еще дальше: он намерен создать самую крупную в мире базу биометрических данных граждан. Сбор информации давно перестал быть добровольным. По данным Human Rights Watch, в Синьцзян-Уйгурском автономном районе образцы ДНК, отпечатки пальцев и сканы радужки у жителей собирают в принудительном порядке. Процедуру проводят как часть бесплатного медобследования, после чего сведения передают полиции. Наличие генетических данных позволяет отслеживать не только самого человека, но и его родственников. Полиция заявила, что отслеживает «фокусные группы подозрительных граждан». К этой категории, как выяснила HRW, в первую очередь попадают мигранты, диссиденты и уйгуры-мусульмане.

Понятие приватности в этих условиях становится относительным – скрыться от постоянной слежки практически невозможно, а с внедрением искусственного интеллекта людям будет все сложнее оставаться анонимными. Интересная жизнь в этом смысле у нас всех только начинается.

(вгору)

Додаток 15

30.01.2018

Пентагон перевірить використання фітнес-трекерів військовими через витік даних

Міністерство оборони США має намір оцінити загрозу, яку можуть представляти для американських військових баз фітнес-трекери і переглянути правила використання таких пристроїв військовими (Espreso.tv).

Про це повідомляє Defencetalk.

Дані з пристроїв фітнес-трекерів дозволяють користувачам відстежувати маршрути тренування, які потенційно можуть бути використані противником для виявлення засекречених військових баз або маршрутів патрулювання.

В даний час військовим не заборонено використовувати фітнес-трекери, йдеться в заяві представника Пентагону полковника Роба Меннінга.

Раніше американський сервіс Strava, за допомогою якого користувачі можуть аналізувати свої дані про фізичну активність і поділитися результатами з іншими людьми, опублікував глобальну карту фітнес-активності.

На цій карті відображаються території планети, на яких люди найактивніше використовують фітнес-трекери і діляться своїми результатами через акаунти в Strava. На карті, крім цілком передбачуваних міст, відображені і маршрути користувачів фітнес-трекерів на військових базах, причому не тільки американських і російських, але і багатьох інших.

Завдяки відображеним на карті маршрутам можна, наприклад, дізнатися, як саме проходять доріжки всередині відомих військових баз. За словами Меннінга, карта може бути використана бойовиками для пошуку невідомих їм американських військових баз, а також для виявлення маршрутів патрулювання. Таке завдання стає навіть простіше, якщо врахувати в країнах, де сьогодні присутні американські військові (Сирія, Ірак, Афганістан) місцеві жителі фітнес-трекери майже не використовують.

Опублікована сервісом Strava карта фітнес-активності може дати загальні уявлення про тривале місцезнаходження тієї чи іншої військової бази і навіть дуже наближено оцінити чисельність персоналу на ній.

(вгору)

Додаток 16

17.01.2018

Уязвимость в интеграции Oculus-Facebook позволяла получить контроль над чужими учетными записями

Очки виртуальной реальности Oculus позволяют пользователям подключаться к своим учетным записям Facebook для более богатого «социального» опыта. Подключение осуществляется как с помощью родного приложения для Windows, так и через браузер. Исследователь безопасности Йосип Франькович (Josip Franjković) проанализировал приложение и обнаружил уязвимость, позволяющую осуществить межсайтовую подделку запросов (CSRF). По словам исследователя, проэксплуатировав уязвимость, злоумышленник мог подключить чужую учетную запись Facebook к своей учетной записи Oculus, получить токен для доступа и с помощью запросов GraphQL захватить контроль над учетной записью жертвы (InternetUA).

Для осуществления атаки злоумышленник должен создать определенные мутации GraphQL и отправить их на graph.oculus.com/graphql с токеном для доступа к своей учетной записи Oculus. В ответ придет ссылка, делающая возможной интеграцию двух сервисов всего в один клик. Если жертва нажмет

на ссылку, ее учетная запись Facebook подключится к учетной записи Oculus атакующего.

Франькович намеревался сообщить Facebook о своем открытии, однако решил сначала подробнее изучить Windows-приложение Oculus. Как пояснил исследователь, app.asar приложения содержит ссылки на запрос GraphQL, возвращающий информацию о подключенной учетной записи Facebook. Франькович обнаружил, что с помощью запроса можно получить токен для доступа к учетной записи Facebook жертвы, а значит, захватить над ней полный контроль.

Исследователь уведомил Facebook о своей находке в октябре 2017 года, и проблема была исправлена. Тем не менее, спустя несколько недель Франькович обнаружил CSRF-уязвимость, позволявшую злоумышленнику перенаправлять жертв на URL-адрес Oculus на свой выбор. Проблема была исправлена в декабре 2017 года.

(вгору)

Додаток 17

18.01.2018
Обнаружен самый мощный вирус для Android

«Лаборатория Касперского» обнаружила новый вирус для устройств на базе операционной системе Android, работа которого сравнима с возможностями продвинутых спецслужб. Частичный код и описание вируса Skygofree опубликовано в блоге компании (InternetUA).

Аналитики назвали Skygofree «невиданным»: многие из его 48 функций любые другие вирусы выполнить не способны. К примеру, согласуя перехват геолокации с микрофоном смартфона, он может подслушать любые разговоры в определенном месте и записать их.

Также вирус самостоятельно подключает гаджет к контролируемым сетям Wi-Fi, крадет телефонные звонки и сообщения и практически всю информацию из мессенджеров, самостоятельно делает фотографии и передает их взломщикам.

Помимо перехвата данных, Skygofree сразу берет под контроль всю информацию, хранящуюся на смартфоне – календари, фотографии и записи. При этом он автоматически включает себя в список особо важных приложений, что обеспечивает бесперебойную работу даже в режиме энергосбережения.

Распространяется вредоносное программное обеспечение через страницы в сети, маскирующиеся под сайты мобильных операторов. Троян существует уже три года и постоянно совершенствуется. По данным «Касперского», существуют модули Skygofree под Windows. Обнаружить вирус крайне сложно, так как вся слежка производится незаметно.

«Лаборатория» отметила, что все жертвы Skygofree, на устройствах которых удалось найти следы вируса, живут в Италии. Аналитики уверены, что

за разработкой редкого трояна стоит итальянская компания, специализирующаяся на профессиональных решениях для слежки.

(вгору)

Додаток 18

22.01. 2018
Криптомайнеры атаковали 55 % компаний в мире

Компания Check зафиксировала в декабре резкий рост распространения вредоносного ПО для майнинга криптовалюты (ITnews).

Исследователи Check Point обнаружили, что в декабре криптомайнеры атаковали 55 % компаний во всем мире. При этом 10 разновидностей этого вредоносного ПО попали в топ-100 самых активных киберугроз, а два из них вошли в тройку лидеров. Используя криптомайнеры злоумышленники захватывают контроль над центральным процессором или видеокартой и используют их ресурсы для добычи криптовалюты.

Check Point обнаружил, что вредоносное ПО для майнинга криптовалюты целенаправленно внедрялось в популярные веб-сайты без ведома пользователей, большинство таких сайтов – это сервисы стриминговых медиа и файлообменники. Хотя в основном такие сервисы являются легальными, их можно взломать, чтобы генерировать больше мощности и получать доход, используя до 65 % ресурсов ЦП пользователя.

«Пользователи все чаще используют ПО для блокировки рекламы, поэтому веб-сайты стали использовать ПО для майнинга криптовалюты в качестве альтернативного источника дохода, – отмечает Майя Хоровиц, руководитель группы Threat Intelligence компании Check Point Software Technologies. – К сожалению, зачастую это происходит без ведома пользователей, чьи процессоры используются для криптомайнинга. Вероятно, мы будем наблюдать, как эта тенденция возрастет в ближайшие несколько месяцев».

В декабре ПО для майнинга криптовалюты CoinHive сместило с лидирующей позиции вредоносную рекламу RoughTed, в то время как набор эксплойтов Rig ek сохранил второе место рейтинга. Новый криптомайнер Cryptoloot замкнул тройку самых активных зловредов декабря, впервые войдя в топ-10.

Самые активные зловреды декабря 2017:

↑ CoinHive – зловред, предназначенный для добычи криптовалюты Monero без ведома пользователя, когда тот посещает веб-сайты.

↔ Rig ek – этот набор эксплойтов появился в 2014 году. Rig включает эксплойты для Internet Explorer, Flash, Java и Silverlight. Заражение начинается с перенаправления на целевую страницу, содержащую Java-скрипт, который затем ищет уязвимые плагины и внедряет эксплойт.

↑ Cryptoloot – криптомайнер, использующий мощность ЦП или видеокарты жертвы и другие ресурсы для майнинга криптовалюты, зловред добавляет транзакции в блокчейн и выпускает новую валюту.

По данным Check Point, в декбре количество атак на российские компании по сравнению с предыдущим месяцем уменьшилось. Россия заняла в рейтинге Global Threat Index 82 место, опустившись на 25 позиций. Больше всего в ноябре атакам подверглись Доминиканская Республика, Ботсвана, Камбоджа и Непал. Меньше всего атаковали Мозамбик, Кипр и Уругвай.

Triada, модульный бэкдор для Android. продолжает распространяться, сохраняя позицию самого активного мобильного зловреда, используемого для атак на организации. За ним расположились Lokibot и Lotoor.

Самые активные мобильные зловреды декабря:

Triada – модульный бэкдор для Android, который дает огромные привилегии скачанным зловредам, поскольку помогает им внедриться в системные процессы. Triada также был замечен в подмене URL-адресов, загруженных в браузере.

Lokibot – банковский троян для Android, который крадет пользовательские данные и требует за них выкуп. Зловред может заблокировать телефон, если удалить его права администратора.

Lotoor – хакерский инструмент, использующий уязвимости в операционных системах Android, чтобы получить root-доступ на взломанных мобильных устройствах.

Global Threat Impact Index и ThreatCloud Map разработаны ThreatCloud intelligence, самой большой совместной сетью по борьбе с киберпреступностью, которая предоставляет данные об угрозах и тенденциях атак из глобальной сети датчиков угроз. База данных ThreatCloud, содержащая более 250 миллионов адресов, проанализированных для обнаружения ботов, более 11 миллионов сигнатур вредоносных программ и более 5,5 миллионов зараженных сайтов, продолжает ежедневно идентифицировать миллионы вредоносных программ.

(вгору)

Додаток 19

22.01.2018

Snap пригрозила сотрудникам тюрьмой за утечку данных

На следующий день после предупреждения в прессу попали внутренние показатели Snapchat (IGate).

Компания Snap, развивающая сервис Snapchat, пригрозила своим сотрудникам санкциями за намеренную организацию утечек конфиденциальной информации. Об этом пишет издание Cheddar, в распоряжении которого оказался разосланный по компании меморандум.

Сотрудникам, пойманным на «сливе» информации, грозят увольнения и судебные иски, предупредил в письме старший юрист Snap Майкл О’Салливан.

«Если вы организуете утечку информации о Snap, то потеряете свою работу. И это только начало. Мы будем преследовать и использовать против вас все доступные правовые инструменты. Вы можете столкнуться с личной финансовой ответственностью, даже если не получите выгоду от утечки.

Правительство, наши инвесторы и третьи лица могу также предъявить к вам собственные претензии из-за раскрытия информации. Правительство может даже посадить вас в тюрьму» – из письма старшего юриста Snap сотрудникам компании.

Представитель Snap отказался комментировать Cheddar содержание меморандума.

Письмо было разослано 8 января 2018 года. На следующий день в издании The Daily Beast вышел материал о том, насколько активно люди пользуются определёнными функциями Snapchat. Текст содержал в том числе метрики, предназначенные только для внутреннего пользования.

Snap известна как одна из самых секретных компаний в ИТ-отрасли, напоминает Cheddar. В компании есть список тем, которые запрещается обсуждать вне работы, а большинство сотрудников не всегда знают о предстоящих новых продуктах. Некоторым при трудоустройстве не говорят даже, над чем именно они будут работать.

Однако в последние несколько месяцев Snap сталкивается с массовыми утечками информации. СМИ сообщают о некоторых новых функциях Snapchat ещё до официального анонса.

(вгору)

Додаток 20

22.01.2018

Более 90 % пользователей всех сервисов Google находятся в большой опасности

Американская корпорация Google за двадцать лет своего существования успела создать десятки различных сервисов, которыми пользуются миллиарды людей. Любой современный человек, который выходит в Интернет, хотя бы раз использовал один из ее фирменных продуктов. Это могли быть карты, музыка, почта, облачное хранилище, видеохостинг YouTube или что-либо еще. Для входа во все эти сервисы, чтобы их можно было полноценно использовать, необходимо авторизироваться с помощью единой учетной записи, которая практически наверняка есть у каждого пользователя глобальной сети (InternetUA).

Согласно официальным данным от Google, более 90 % пользователей всех ее сервисов находятся в большой опасности. Она утверждает, что с каждым годом злоумышленники находят все более изощренные способы кражи ценной информации, а пользователи на это совсем никак не реагируют. По сути, если у человека украдут учетную запись Google, то он потеряет буквально

все, вплоть до денег на своих банковских счетах, так как к аккаунте можно привязать сразу несколько банковских карт.

Эксперты по безопасности из Google сумели выяснить, что в зоне риска находятся 90 % пользователей всех фирменных сервисов, в том числе Gmail и YouTube. Все такие пользователи не используют двухфакторную авторизацию, которая исключает возможность взлома учетной записи даже в том случае, если злоумышленник узнал ее логин и пароль. Она работает по очень простому принципу. Когда кто-то пытается войти в аккаунт с нового устройства, то после привычного пароля необходимо ввести одноразовый PIN-код, приходящий в виде SMS-сообщения.

Функция двухфакторной идентификации личности доступна пользователям всех сервисов Google еще с лета 2016 года, однако за полтора года пользоваться ей начало только 10 % от всех пользователей, тогда как остальные предпочитают использовать связку из привычного логина и пароля. Если эти данные каким-то образом попадут к злоумышленникам, то они смогут украсть абсолютно всю информацию из аккаунта без каких-либо сложностей. Именно поэтому «поисковой гигант» просит всех людей, кому дорога собственная безопасность в сети, активировать новый способ защиты.

(вгору)

Додаток 21

25.01.2018

Троянец Mezzo способен менять реквизиты в бухгалтерских файлах

«Лаборатория Касперского» обнаружила новую угрозу – троянец Mezzo, способный подменять реквизиты в файлах обмена между бухгалтерскими и банковскими системами. В настоящий момент зловред просто отправляет собранную с зараженного компьютера информацию на сервер злоумышленникам, и, по мнению аналитиков, это может говорить о том, что создатели троянца готовятся к будущей кампании. Количество жертв Mezzo пока исчисляется единицами, при этом большинство заражений зафиксировано в России (Компьютерное Обозрение).

Распространяется Mezzo с помощью сторонних программ-загрузчиков. После попадания на устройство троянец создает уникальный идентификатор для зараженного компьютера – на его основе на сервере злоумышленников создается папка для хранения всех найденных у жертвы файлов. Каждая из этих папок защищена паролем.

Основной интерес для Mezzo представляют текстовые файлы популярного бухгалтерского ПО, созданные менее двух минут назад. Функциональность троянца предполагает, что после обнаружения таких документов он ждет, последует ли открытие диалогового окна для обмена информаций между бухгалтерской системой и банком. Если это произойдет, зловред может подменять реквизиты счета в файле непосредственно в момент

передачи данных. В противном случае (если диалоговое окно так и не будет открыто) Mezzo подменяет весь файл поддельным.

Кроме того, анализ кода Mezzo показал, что зловред может быть связан с другим нашумевшим троянцем, охотящимся за криптовалютами, – CryptoShuffler. Эксперты «Лаборатории Касперского» обнаружили, что код Mezzo и программы AlinaBot, осуществляющей загрузку CryptoShuffler, идентичны практически до последней строчки. По всей видимости, за обоими зловредами стоят одни и те же вирусописатели, а, значит, их интерес может также затрагивать криптокошельки пользователей.

(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.