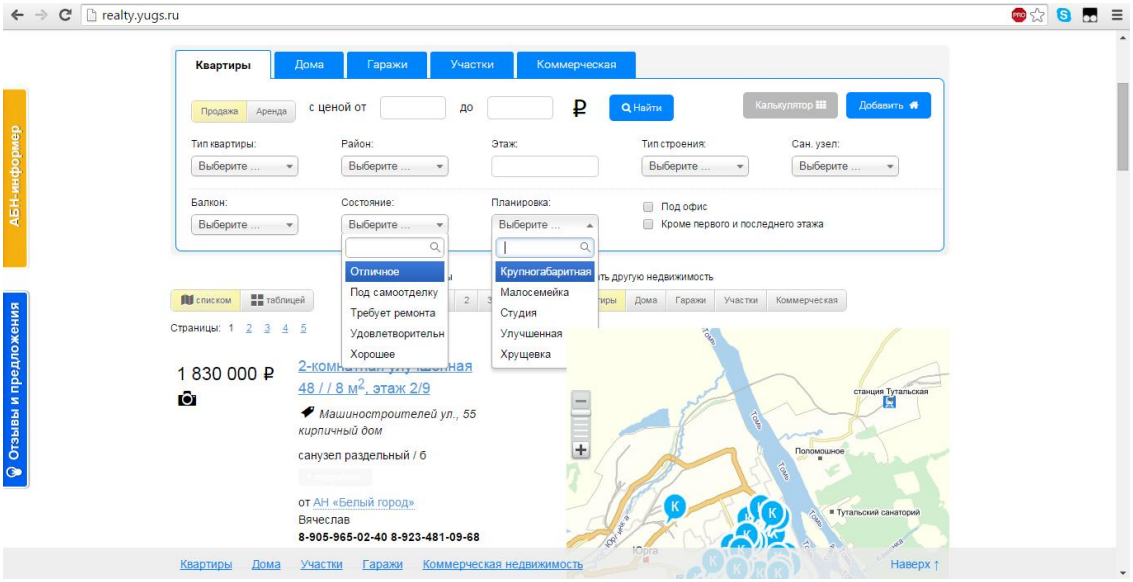

Рис. 2. Выбор подходящих альтернативных вариантов

Литература.

1. Недвижимость в Юрге // [Электронный ресурс] – режим доступа: http://realty.yugs.ru/.
2. АБС-Информрмер // [Электронный ресурс], URL https://play.google.com/store/apps/details?id=com.yugs.abninformer&hl=ru/.
3. Разработка управляемого интерфейса. – / В.А. Ажеронок, А.В. Островерх, М.Г. Радченко, Е.Ю. Хрусталева. – М.: ООО «1С-Паблишинг», 2010. – 731 с.: ил.

УЯЗВИМОСТЬ МОБИЛЬНЫХ ПЛАТФОРМ ANROID, IOS

Ф.М. Абдулназаров
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-maiLl: mirzosharifovich@mail.ru

В данной статье рассматривается современное вредоносное программное обеспечение для гаджетов на платформе android, ios.

Каждый человек при выборе оптимального телефона руководствуется несколькими критериями, к которым относится также безопасность самой операционной системы. Пользователей настолько волнует сохранность своих персональных данных, что при покупке того же пк они сразу приобретают антивирусное программное обеспечение, потому как число вредоносных программ для смартфонов и планшетов возрастает с каждым годом.

Большинство вирусов выпускается для операционной системы android, но эксперты в последнее время замечают попытки создания вредоносного программного обеспечения и для гаджетов apple.

Основной причиной хакерских атак на ос android является открытость исходного кода операционной системы и ее распространенность на многочисленных устройствах. По данным фбр, 79% всех вирусов, обнаруженных в ходе исследования, приходилась именно на android. Для сравнения, вирусов, написанных под ios, всего 0,7% от общего числа. [1]

В основном мошеннические или вредоносные приложения осуществляют отправку платных сообщений, копируют базы контактов или сообщения для авторизации в интернет – банкинге.

троян trojan-sms.androidos.fakeplayer.a проникает на носители, замаскировавшись под установочную программу видеоплеера. Вирус рассылает сообщения на платные номера. Существует также аналогичный вирус trojan-sms.androidos.fakeplayer.b, который распространяется через платное видео.

Наиболее опасными вирусами на ос android являются [2]:

1. Golddream и noname. Эти вирусы крадут персональные данные владельца смартфона: телефонные номера контактов, даты, информацию из сообщений, а также осуществляют платную sms-рассылку.

2. Droiddream и droiddreamlight. Эти вирусы распространяются через официальный каталог приложений android market. Согласно неофициальной статистике, примерно 30% вирусов попадают в смартфоны из этого каталога. Их можно скачать в таких популярных поддельных играх, как angry birds, cut the rope, assassin's creed. После скачивания одной из игр осуществляется отправка платных сообщений, после чего у пользователя снимаются деньги со счета и крадутся все персональные данные.

3. Ggtracker. Этот вирус вместе с двумя приложениями был распространен на фишинговых сайтах. Одно из приложений увеличивало продолжительность жизни заряда батареи. Пользователи теряют не только персональные данные, но и остаются без денег на счету, поскольку вирус осуществляет платную sms-рассылку.

Можно сказать, что пользователи операционной системы android подвержены большей опасности получения на свои устройства вредоносного программного обеспечения, способного передавать злоумышленникам персональные данные и деньги пользователей, чем владельцы гаджетов apple. Однако пользователи ос ios также подвержены угрозам.

В основном, пользователи apple сами являются виновниками заражения своих гаджетов, потому как хотят получить полный доступ к файловой системе ios через программы jailbreak и unlock. Вирусы для ios в большинстве случаев как раз и написаны так, что на немодифицированной операционной системе просто не запустятся, она им не даст сделать этого.

Наибольшее число пострадавших, как было замечено исследователями вопроса, получили ущерб, скачивая программы из app store. Вирусы создаются под видом приложений для ios с полезной функциональностью, которая действительно присутствует. Так как программы работают и соответствуют заявленному назначению, модераторы их пропускают. [3]

Владельцы своих гаджетов готовы скачивать и устанавливать все подряд, хотя в комментариях к такому по можно увидеть и предупреждения от других пострадавших. По мере выявления все это убирается из свободного доступа, но не всегда быстро и своевременно.

Пророссийская группа хакеров под названием "operation pawn storm" разработала новый вирус-шпион, заражающий ios устройства apple, который не может быть установлен без согласия пользователя.[4]

Вирус получает доступ к списку контактов, сообщениям, гео-локационным данным, используемым wi-fi сетям, внутренним процессам и используемым приложениям. Полученные данные пересылаются на сервера хакеров для дальнейшей обработки. Хакеры, имеющие доступ к управляющей программе могут, незаметно для пользователя, активировать микрофон и прослушать не только телефонные разговоры, но и все происходящее вокруг.

Американская компания palo alto networks, занимающаяся безопасностью в сети интернет, выявила новое семейство вредоносных программ, которые атакуют устройства корпорации apple. [5]

Целый ряд вирусов, получившее название wirelurker, были созданы в китае. Вирус атакует операционные системы компьютеров mac и iphone. Он попадает на компьютеры mac через сторонний магазин приложений для устройств apple — китайский maiyadi app store. Этот вирус автоматически устанавливается на iphone или ipad через usb-кабель, подключенный к компьютеру или ноутбуку mac. Причем вирус может проникнуть, даже если iphone или ipad не проходили процедуру jailbreak. После попадания на устройство вирус получает доступ к адресной книге и сообщениям, но конечная цель вредоносной программы пока не выявлена.

Кроме того, плохо защищены и от вредоносных вторжений ранние версий ios, особенно те, что ниже ios 6. Они лучше изучены киберпреступниками и в них больше известных уязвимостей, через которые вирусы и проникают.

Также одним из опасных вирусов является masque attack, так как он может подвергнуть заражению мобильные устройства на любой версии системы ios, не исключая самую последнюю ios 8.1.1 beta 1.[6]

Пользователю предлагается пройти по ссылке и скачать приложение. Скачивание происходит не из app store. Обычно речь идет о популярных приложениях, их новых версиях и так далее. В процессе работы оно подменяет все программы, в которых используются персонаальные данные пользователя, например, его пароли или адрес почты.[7]

Нельзя считать ос ios полностью защищенной от вирусного программного обеспечения. Устройства, функционирующие на этой платформе, с каждым днем набирают все большую популярность, поэтому хакерам становится все интереснее пытаться взломать ос ios.[8]

Пользователи могут сами обезопасить себя от вирусов, соблюдая такие меры защиты такие, как:

- не устанавливать приложения со сторонних сайтов;
- читать отзывы и описания приложений, которые хотите загрузить на смартфон;

- следить за обновлениями на свой телефон и источниками их загрузки;
- устанавливать официальные версии прошивок, ведь новая версия системы - это не только обновленный функционал, но и перекрытые лазейки для вирусов;
- не пользоваться модифицированными версиями, ведь доступ к файловой системе устройства получите не только вы, но и непрошенные гости;
- следить за работой своего антивируса.

Подводя итог, можно сказать, что ни одна из мобильных платформ не защищена от вирусных атак, поэтому владельцы должны сами следить за безопасностью своих гаджетов, работающих и на платформе android, и на ios, ведь с каждым днем выпускается все большее количество вредоносных программ.

Литература.

1. Aggle.ru [электронный ресурс] url: http://aggle.ru/ios/virusy.html (дата обращения: 16.05.2015)
2. Appleface [электронный ресурс] url: http://appleface.ru/iphone-news/virus-atakoval-ustrojstva-apple/ (дата обращения: 16.05.2015)
3. Антамошкин, о.а. модели и методы формирования надежных структур информационных систем обработки информации [текст] / антамошкин о.а., кукарцев в.в. // информационные технологии и математическое моделирование в экономике, технике, экологии, образовании, педагогике и торговле.— 2014.— № 7.— с. 51-94.
4. Железный сайт. Новости и обзоры железа [электронный ресурс] url: http://www.gelezki.info/mobile-news/2090-samyje-rasprostranjennyje-android-virusy-i-sposoby-borby-s-nimi.html (дата обращения: 16.05.2015)
5. Новости apple [электронный ресурс] url: http://apple-dev.ru/3154-novyj-virus-pod-ios-ne-trebuyushhij-jailbreak/ (дата обращения: 16.05.2015)
6. Простомас [электронный ресурс] url:http://www.prostomac.com/2014/11/bezonasnost-ios-snova-pod-ugrozoj-virus-masque-attack/ (дата обращения: 16.05.2015)
7. Терещенко, о.в. применение моделей облачных сервисов в организациях [текст] / терещенко о.в., кукарцев в.в. // логистические системы в глобальной экономике.— 2014.— № 4.— с. 477-481.
8. Яблоко [электронный ресурс] url: http://yablyk.com/79-virusov-napisano-pod-android-pod-ios-07/ (дата обращения: 16.05.2015)

СЕТЬ МАГАЗИНОВ ДЕТСКОЙ ОДЕЖДЫ «МАЛЫШ» АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ТОВАРОВ

Я.А. Берёза, студент гр. ПИм-151, I курс,
К.Е. Пешкова, студент гр. ПИм-151, I курс,
А.Ю. Барсуков студент гр. ПИм-151, I курс
Научный руководитель: Рейзенбук К.Э., ст. преподаватель
Кузбасский государственный технический университет имени Т.Ф. Горбачева
650000, г. Кемерово ул. Дзержинского 9а, тел. 89043797561
E-mail: yana_bereza@mail.ru

В Кемерово существует огромное количество различных магазинов. Это и огромные гипермаркеты, и совсем небольшие частные магазины. Если в большинстве огромных магазинов уже ведется электронный учет товаров, то маленькие магазинчики только приобщаются к автоматизации своей деятельности. Магазин детской одежды «Малыш» как раз из второй категории.

В сеть магазинов детской одежды «Малыш» входят два филиала, так же имеется складское помещение. Магазин специализируется на продаже детской одежды. Кроме того, в ассортименте присутствуют и другие детские товары. Основная аудитория - родители детей в возрасте от 0 до 14 лет.

Ручной учет являлся его основной проблемой магазина. Помимо этого, находясь в одном магазине, нельзя было запросто узнать о наличии какого-либо товара в другом, то есть отсутствовала единая база данных. Кроме того, клиентская база устарела, с ней не велось никакой работа.

Поэтому была разработана автоматизированная система учета товаров для повышения прибыли, снижения трудозатрат, улучшения качества и эффективности работы магазина «МАЛЫШ». Создание собственной системы позволило учесть специфику данного предприятия, автоматизировать все бизнес-процессы, опираясь на принципы работы данного предприятия, а не подстраивать магазин под бизнес-процессы системы. Система разрабатывалась таким образом, чтобы быть как можно более простой и понятной, чтобы любой сотрудник магазина мог без особого труда в ней разобраться (рисунок 1).