СОВРЕМЕННАЯ УГРОЗА МОБИЛЬНЫХ УСТРОЙСТВ - ВИРУСЫ

Веденков А.А.

с. Ольгино, ГБОУ СОШ муниципального района Безенчукский Самарской области, 5 класс

Научный руководитель: Хохрина Е.А., с. Ольгино, ГБОУ СОШ муниципального района Безенчукский Самарской области, Учитель информатики и ИКТ высшей категории

В настоящее время очень актуальна проблема защиты информации. Информация как продукт может продаваться, или покупаться, в связи, с чем мы можем сказать, что она имеет свою стоимость. Показатель стоимости может варьироваться в различных пределах, и когда мы говорим об информации, которая может принести высокую прибыль, здесь и возникает проблема, связанная с ее защитой. Говоря о защите, мы можем выделить два основных момента, это потеря ценности информации или ее исчезновение с устройств хранения данных. Первый момент связан с халатностью владельцев, обладающих какой либо информацией. Второй момент чаще всего происходит из-за сбоев аппаратной части устройств, на которых хранятся данные, или же из-за вирусов, проникших в те или иные устройства. В своей работе я хочу рассмотреть угрозы для мобильных устройств и способы защиты от них.

В наш век мобильных технологий человек не представляет свою жизнь без любимого гаджета, функциональность которого зависит только от желания и размера кошелька. С ростом проникновения смартфонов — миллионы абонентов операторов связи во всем мире подвергаются атакам вредоносного программного обеспечения, вследствие чего теряют огромные суммы. Однако не все обладатели этих устройств осознают реальный масштаб угроз. Нужно помнить, что смартфон — это полноценный компьютер, который находится под управлением операционной системы. Наиболее популярные платформы для данных устройств: Apple iOS, Google Android, Windows Phone, BlackBerry.

Одной из лидирующих платформ мобильных устройств является Android, именно она представляет особый интерес для киберпреступников. Для данной платформы пишется около 97 % от всех существующих образцов вредоносного программного обеспечения для мобильных устройств.

Недавно я стал обладателем нового смартфона, при обновлении одного из приложений на экране моего смартфона появилось следующее изображение:

Оказалось, что обнаружена угроза, вирус, поэтому тема угрозы мобильных устройств от вирусов меня очень заинтересовала.

Объект исследования: мобильный вирусы.

Предмет исследования: узнать, что такое мобильные вирусы, как защитить свое мобильное устройство от них?

При изучении этой темы я поставил следующие цели и задачи.

Цель: Выяснить, существует ли проблема вирусов для мобильных телефонов и как относятся к этой проблеме владельцы сотовых телефонов.

Задачи:

1. Провести анализ литературы, для изучения проблемы мобильных вирусов.
2. Выяснить, что такое мобильные вирусы?
3. Есть ли реальная опасность подхватить мобильные вирусы на свой мобильный телефон?
4. Что делать, если ваш телефон подхватил мобильный вирус?
5. Разработать анкету и провести анкетирование учащихся 2-5 классов нашей школы для выявления осведомленности о вирусах для мобильных устройств и защите от них своих гаджетов.

Актуальность темы: заключается в том, чтобы научиться различать мобильные вирусы, защищаться от заражения телефона.

Тип проекта: информационный, исследовательский.

Область исследования: информатика

Методы: Анализ статистических данных полученных в результате анкетирования учащихся 2-5 классов.

Гипотеза: Можно предположить, что мобильные вирусы существуют, и они могут повлиять на работоспособность мобильных телефонов.

Для подтверждения или опровержения выдвинутой гипотезы было проведено данное исследование.

Информационная часть

История мобильных вирусов с момента появления до современности

Мобильный вирус — это небольшая программа, которая предназначена для вмешательства в работу мобильного устройства (смартфона, планшета), посредством

записи, повреждения или удаления личных данных. (Приложение 1).

Распространяются мобильные вирусы через каналы связи (SMS/MMS, Bluetooth, интернет). Основная цель мобильных вирусов, как и компьютерных — это получение персональной информации, которую можно продать, или использовать в личных нуждах. Однако по сравнению с обычными компьютерами цена ущерба от вирусов для мобильных устройств может быть более высокой. Связанно это с тем, что пользователь хранит в телефоне огромное количество персональной информации (номера телефонов, данные различных аккаунтов и почты, фото), кроме того, вирусы имеют возможность отправлять SMS и звонить на платные номера.

История мобильных вирусов насчитывает чуть менее десяти лет – достаточно серьезный возраст по меркам сотового рынка.

В начале века вирусы для сотовых телефонов не казались чем-то реальным, в 2003 году в одном из интервью Евгений Касперский даже позволил себе заявить о маловероятности появления полноценных мобильных вирусов, предназначенных для заражения сотовых телефонов и смартфонов.

Первый настоящий мобильный вирус — Cabir был разработан 14 июня 2004 года, группой вирусописателей. Cabir — приложение (червь), вред от него заключался в рассылке своей копии по каналу Bluetooth, что приводит к быстрой разрядке батареи устройства. Предназначался для мобильных устройств, работающих под управлением операционной системы Symbian OS. Был разработан в целях демонстрации принципиальной возможности существования мобильных вирусов.

Вирус Cabir постоянно сканирует эфир в поиске новых жертв. При обнаружении потенциального «клиента» зараженное устройство отправляет ему файл caribe.sis объемом 15 кбайт. Для абонента это выглядит так: на экране появляется предложение принять некое письмо, и, если пользователь дает согласие, на его телефон пересылается файл с вирусом, после чего система спрашивает разрешения инсталлировать программу под названием Caribe. Если и на этот вопрос следует утвердительный ответ, червь устанавливается в систему, для верности копируя себя сразу в несколько директорий.

К сожалению, исходный код этого вируса был опубликован в Сети, чем не преминули воспользоваться другие разработчики вирусов. В течение короткого времени для программной платформы Symbian OS были написаны сотни разнообразных вирусов, в числе которых были как черви, так и трояны. Некоторые из них представляли реальную опасность для нормального функционирования мобильных устройств. Видоизменялись и совершенствовались средства распространения вирусов – помимо Bluetooth, заражение происходило за счет MMS-сообщений (первым таким вирусом стал ComWar, появившийся в марте 2005 года).

Понятно, что Symbian OS разработчики вирусов не ограничились. Уже спустя месяц после появления вируса Cabir появилось вредоносное приложение для платформы Windows Mobile – Duts, представлявшее угрозу для файловой системы коммуникатора или КПК. Вслед за этим последовали другие Windows Mobile-вирусы, в частности, Brador, ставший первым из мобильных вирусов, открывавшим доступ к зараженному устройству извне. Наконец, чрезвычайно неприятным стало появление в феврале 2006 года RedBrowser – первого мобильного вируса для телефонов с поддержкой Java, что резко увеличивало потенциальную аудиторию зараженных устройств. Вслед за ним появились другие вирусы, такие как, например, Webster, представлявший угрозу уже не только для функциональности зараженного телефона, но и для баланса самого владельца – речь идет о потере денег вследствие отправки SMS-сообщений.

Если вирусы «грозили» в основном сокращением времени работы от аккумулятора, то впоследствии стала вполне реальна опасность потери всех личных данных (вирус CommWarrior), заражения ПК «настоящими» компьютерными вирусами и потери финансовых средств с баланса телефонного номера. Появились и кроссплатформерные вирусы, которые распространялись во время синхронизации с ПК. Если раньше вирусы писались энтузиастами, то постепенно стали появляться настоящие коммерческие разработки. Речь идет, в частности, о краже конфиденциальной информации вроде содержания телефонного справочника или совершенных звонков (распространявшийся за 50$ троян Flexispy, а также похожий на него Acallno).

Ситуация для мобильных вирусов стала особенно благоприятной с широким распространением смартфонов и коммуникаторов. В отличие от обычного мобильника эти устройства обладают операционными системами, возможностей которых вполне достаточно для того, чтобы стать хорошей средой для распространения вирусов. Кроме того, все современные «умники» и «умницы» снабжены беспроводным модулем Bluetooth, через который вирусы способны

распространяться особенно быстро. Получается, что чем совершеннее ваше средство связи, тем привлекательнее оно для вирусов.

Особенно активно коварные вирусные программы распространяются в местах массового скопления людей: в метро, в кинотеатрах, в аэропортах. Яркий пример – чемпионат мира по футболу. На огромных стадионах, забитых под завязку, мобильные вирусы распространялись с поразительной скоростью. Это, пожалуй, лучшая среда для массового заражения мобильников и смартфонов. Во-первых, в таких условиях вирус очень легко распространять, как вы уже поняли. Компьютер, на котором содержится программа-вредитель, просто начинает рассылать её с помощью MMS или Bluetooth всем мобильникам в радиусе от нескольких метров до одного километра. Во-вторых, создаются очень удобные условия для обмана абонентов. Ведь для заражения телефонов недостаточно просто отправить вирус через Bluetooth. Необходимо, чтобы пользователь запустил вредоносную программу на своём телефоне. Реакция увлечённого футбольным матчем человека, которому приходит сообщение о том, что он якобы выиграл билет на следующую игру, вполне предсказуема. Захваченный зрелищем болельщик наверняка даже не почувствует подвоха, нажмёт OK, и зловредная программа попадёт к нему в телефон.

Точно такая же ситуация может возникнуть во время концерта, митинга и другого подобного мероприятия, на котором присутствует много людей, чем-то страстно увлечённых. Их внимание целиком сосредоточено на зрелище, и большинство из них уж точно не задумаются над тем, принять или не принять новое сообщение.

Пока что большинство мобильных вирусов создаются для операционной системы Symbian (о самых опасных из них речь пойдёт далее). Однако эксперты по антивирусным технологиям считают, что помимо данной платформы, соединения Bluetooth и MMS существует еще одна «благоприятная» среда для распространения зловредных программ. Это операционная система Windows Mobile (for Smartphone и Phone Edition). Она очень уязвима для различных вирусов, так как в ней не существует ограничений для выполняемых приложений. Запущенная программа может запросто получить доступ к любым функциям системы: приёму/передаче файлов, функциям телефонных и мультимедийных служб и т.д. На сегодняшний день известны лишь четыре вида вирусов для этой платформы, но в будущем именно её следует рассматривать как основное поле деятельности мобильных вирусов.

Причины распространения мобильных вирусов

– уязвимости программного обеспечения;

– низкий уровень «мобильной» грамотности;

– отношение владельцев мобильных телефонов к мобильным вирусам, как к проблеме будущего;

– любопытство (а что будет, если я запущу этот файл/игру/программу?);

– несоблюдение элементарных правил безопасности.

Пути проникновения вируса в телефон:

– с другого телефона через Bluetooth-соединение;

– посредством MMS-сообщения;

– с ПК (соединение через Bluetooth, USB, WiFi, инфракрасное…);

– через web- или wap-сайты.

Симптомы заражения

Появление – после копирования и установки каких-либо файлов (как правило, «игр») – всевозможных «глюков» и «багов». Например: беспричинно «зависает» телефон, не запускаются какие-либо приложения, невозможно открыть папку Принятые файлы.

Появление неизвестных подозрительных файлов и иконок.

Мобильник самопроизвольно отправляет SMS и MMS, быстро опустошая счет владельца.

Блокируются какие-либо функции телефона.

Деструктивные действия мобильных вирусов (одно из неписаных правил гласит, что вирус, получая управление, может делать в системе всё то, что может делать пользователь!):

• незаметная для пользователя массовая рассылка SMS и MMS;

• несанкционированные звонки на платные номера;

• быстрое опустошение счета абонента (в результате звонков на платные номера и массовой рассылки SMS и MMS);

• уничтожение данных пользователя (телефонная книга, файлы и т.д.);

• похищение конфиденциальной информации (пароли, номера счетов и т.д.);

• блокировка функций телефона (SMS, игры, камера и т.д.) или аппарат в целом;

• быстрая разрядка аккумулятора;

• рассылка (от имени владельца телефона) зараженных файлов всеми возможными способами (e-mail, WiFi, Bluetooth и т.д.);

• при синхронизации телефона с компьютером – пересылка на ПК деструктивного кода;

• возможность удаленного управления аппаратом.

Мобильные антивирусы

Теперь поговорим о методах защиты от вирусов. На сегодняшний день большинство разработчиков антивирусов для персональных компьютеров стали выпускать мобильные версии антивирусов. Проблемы современных киберугроз решаются мобильными версиями антивирусов «Лаборатории Касперского», «Dr.Web» и других известных производителей антивирусного программного обеспечения.

Существуют также и сетевые решения операторов связи, позволяющие обойтись без установки антивируса на смартфон. Например, сетевая версия антивируса МТС при выходе в интернет с мобильного устройства блокирует зараженные веб-страницы непосредственно на операторском оборудовании. Таким образом, обеспечивается защита на более высоком аппаратно-программном уровне, разработанном по стандартам информационной безопасности для крупных предприятий, финансовых и банковских учреждений.

Возьмем пять крупнейших антивирусных компаний:

AVG Mobilation Anti-Virus Pro; BitDefender Mobile Security; Dr.Web Mobile Security; Kaspersky Mobile Security; Norton Mobile Security.

Выделим категории для сравнения данных антивирусных программ:

Фильтр звонков и SMS, Антивирус, Техническая поддержка, Антивор.

Проанализировав предоставляемые антивирусные услуги этих компаний, можно сделать вывод, что наилучшими антивирусами на сегодня являются Dr.Web Mobile Security и Kaspersky Mobile Security. (Приложение 2)

Представленное исследование показало, что большинство антивирусов включает в себя фиксированный набор компонентов безопасности: антивирусное ядро (сканер и монитор); антивор; фильтрацию звонков и SMS.

Исследовательская часть

Анкетирование учащихся

Одной из задач, которую я ставил, работая над данной темой, была следующая: разработать анкету и провести анкетирование учащихся 2-5 классов нашей школы для выявления осведомленности о вирусах для мобильных устройств и защите от них своих гаджетов. С помощью учителя информатики я разработал анкету для учащихся 2-5 классов и в течение недели проводил анкетирование учащихся.

Всего в анкетировании участвовало 47 учащихся. (Приложение 3).

Анкета

1. Есть ли у вас смартфон или планшет? Да – 35, нет - 12

2. Слышали ли вы о мобильных вирусах? Да – 33, нет - 14

3. Знаете ли Вы каким способом мобильный вирус проникает в телефон? Да – 18, нет - 29

4. Было ли у Вас заражение телефона вирусом? Да – 13, нет – 5, не знаю - 17

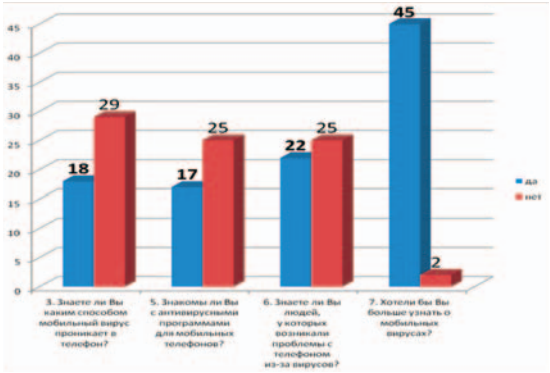
5. Знакомы ли Вы с антивирусными программами для мобильных телефонов? Да – 17, нет – 25

6. Знаете ли Вы людей, у которых возникали проблемы с телефоном из-за вирусов? Да – 22, нет – 25

7. Хотели бы вы больше узнать о мобильных вирусах? Да – 45, нет – 2

Результаты анкетирования учащихся

Социологическое исследование показало, что у большинства учащихся 2-5 классов нашей школы (74 %) есть свой смартфон или планшет, который им подарили родители или родственники, но, несмотря на это, большинство (70%) опрошенных никогда не сталкивалось с вирусами для мобильных устройств, 53% ответили, что не знают людей у которых, были проблемы с телефонами из-за вирусов. 95% отметили, что задумались о проблеме вирусов для мобильных устройств.



Заключение

Проведенный анализ изученной литературы, полученных данных помог мне сделать вывод всей моей работы над исследованием и разработать для учащихся, участвовавших в анкетировании Памятку «Как защищаться от мобильных вирусов».

Действительно, в современном мире существуют вирусы, способные стать угрозой для мобильных устройств. До недавнего времени считалось, что мобильные вирусы, если и угрожают, то только продвинутонавороченным мобильникам, владельцам обычных мобильников бояться нечего. Увы, это уже не соответствует действительности!.. А т.к. доля обычных телефонов как минимум на порядок превосходит долю смартфонов, есть повод задуматься! Поскольку уже созданы кроссплатформенные мобильные вирусы, приверженность какой-то одной ОС не гарантирует защиту от вирусов. Первоначально существовавшая грань между мобильными и компьютерными вирусами стерта. Теперь эти устройства могут взаимно заражать друг друга. Компьютерным вирусам для широкого распространения потребовалось более двадцати лет. Мобильные вирусы прошли этот путь всего лишь за два года (очевидно, что мобильные вирусописатели активно используют опыт создания и распространения компьютерных вирусов). В мире насчитывается около 3 млрд. абонентов сотовой связи. Многие буквально не расстаются со своими мобильниками. На мобильниках хранится конфиденциальная информация. Нетрудно представить масштабы последствий в случае возникновения эпидемий мобильных вирусов.

Как относиться к проблеме мобильных вирусов? Не нужно ее преувеличивать, паниковать. Но не стоит и отмахиваться от нее, считая, что проблема искусственно раздувается антивирусными компаниями и жадными до сенсаций СМИ. Таким образом, гипотеза, сформулированная в начале работы, полностью подтвердилась, цель и задачи, поставленные в начале моего исследования, достигнуты. Считаю самой главной ценностью моего исследования практическую значимость для меня и моих родных, одноклассников, так как теперь я узнал, как защитить свое мобильное устройство от угроз.

Список литературы

1. https://ru.wikipedia.org/wiki - Википедия

2. http://www.hackzona.ru – территория взлома

3. http://www.mobi.ru – экспертный сайт цифровой техники

4. http://www.vipmks.ru – мобильный корпоративные системы

5. Создаем вирус и антивирус. Автор: И.А. Гульев, 304с. – М.: Просвещение, 1999г.

6. Защита от мобильных вирусов [Электронный ресурс] — Режим доступа. — URL: http://www.utro.ru/articles/2013/10/29/1153228.shtml

7. Все о мобильных телефонах: Возможности, выбор, этикет. Автор: Инджиев А.А. – М.: Феникс, 2006г.

8. http://www.softmixer.com/2011/08/blog-post_8103.html - сетевой журнал