Лекция №3

Толкование №301

На прошлой лекции шла речь о том, что существуют некоторые классификации или рейтинги угроз, которые характерны для информационных систем. Одной из таких угроз является распространение так называемых нехороших изделий (madware, mailware), соответственно раз они есть, их пытаются каким-то образом классифицировать. В различных источниках можно найти различную классификацию этих самых нехороших изделий.

Понятно, что с этими нехорошими изделиями борются во всём мире, в том числе с помощью так называемых антивирусных программ. Среди них: Caspersky, Kaspersky, avira, avast, Node32 и другие.

В одном из источников, данных вам в изучении БИС, тоже есть своя классификация: «Программно-технические угрозы безопасности».

Под вирусом будет пониматься программа, которая характеризуется двумя основными чертами: 1) без ведома пользователя или пользователей компьютера осуществлять несанкционированное действие, направленное либо: а) на создание/изменение/искажение/удаление/несанкционированную передачу данных; б) разрушение принципов функционирования систем обработки данных (на создание новых или на изменение существующих программ обработки данных); 2) без ведома пользователя компьютера размножается путём заражения других файлов посредством изменения или полной замены функционирующих программ, либо исполнимых файлов.

Как было сказано, вирусы классифицируются различным образом. На помойке, в одном из источников можно найти так называемые: parasitic viruses (13%), bootsector viruses (23%), macroviruses (64%).

Замечание: В контексте данного курса лекций будут рассматриваться и будут считаться вирусами (программами, которые наносят вред компьютеру) только паразитические (файловые) вирусы и bootsector-вирусы. Это связано с тем, что мы будем понимать под вирусами некоторые программы, которыми называются совокупности команд или операций, которые после декодирования самой электронно-вычислительной машиной могут заставить эту машину выполнить некоторую последовательность действий. Вот эта возможность декодирования программы или последовательности команд самой электронно-вычислительной машиной отличает понятия программы от понятия исполнимого модуля или исполнимого файла. Исполнимый файл – не является программой. Он становится программой после того, как с помощью средств операционной системы этот файл попадает в оперативную память и ей (этой программе) передаётся управление. Вирус – это программа, которая находится в оперативной памяти и в какой-то момент времени в этой оперативной памяти этой программе передается управление и соответственно происходит некоторое изменение в работе компьютера (в работе других программ). В том случае, когда вирус (некоторая badware) представляет собой исполнимый файл или же он представляет собой совокупность операций, записанных на каком-либо макро-языке какой-либо программной оболочки или какого-либо программного средства, мы в этом случае не будем считать это за вирус. Макро-вирусы, которые есть в некоторых классификациях, – это тексты на внутреннем языке той или иной программной системы.

Для того, чтобы текст на макро-языке стал вирусом, необходимо, чтобы каким-то образом он (этот текст) был преобразован на машинный языке и был передан в оперативную память. Только тогда можно будет рассматривать, что она (программа) представляет собой угрозу компьютеру.

К файловым вирусам относятся программы, которые поражают файлы компьютера. В большинстве случаев они сделав какую-либо неприятность с данными, хранящимися на компьютере, либо с исполнимыми файлами, обеспечивающими функционирование системы обработки данных, проникают, заражают исполнимые файлы, либо заражают отдельные компоненты того, что называется DLL. А при последующих загрузках уже зараженных исполнимых файлов в оперативную память эти вирусы размножаются и заражают другие файлы (чаще всего исполнимые). Хотя есть вирусы, которые «портят все подряд».

Загрузочные вирусы характеризуются тем, что они (программы) располагаются в так называемом bootsector-е.

Ранее мы говорили, что под операционной системой мы будем подразумевать совокупность программных и аппаратных средств, предназначенных для управления устройствами компьютера и для предоставления сервиса прикладным программам для управления этими устройствами. Часто говорят, что после включения компьютера осуществляется *загрузка операционной системы*. Далее, это словосочетание будем считать ненормативной лексикой. Это связано с тем, что система состоит из программной и аппаратной частей. И не совсем понятно, как загрузить аппаратную часть, следовательно, возможна загрузка только программной части в операционной системе.

Для загрузки программного обеспечения, необходимого для загрузки программной части операционной системы используется так называемый bootsector. И загрузочные вирусы характеризуются тем, что в какой-то момент времени при загрузке программной части операционной системы в этом загрузочном секторе может оказаться вредоносная программа, при чём замаскированная таким образом, что в какой-то момент времени, ей может быть передано управление. И такую программу, в том случае, когда она что-то портит, называют загрузочным вирусом.

P.S. Боров – (из новозеландского) Hog. Считается, что одним из первых вирусов была программа, которая получалась в результате загрузки в оперативную память исполнимого файла с названием Dhog68.com. Этот вирус один из самых нехороших. Он заражал собой все файлы, которые были в том или ином каталоге (текстовые, исполнимые модули, файлы конфигурации), тем самым превращая их все в вирус Dhog68, при этом имена файлов не менялись, а просто-напросто, если, например, текстовый файл запустить, то происходило тоже самое, что и делал этот самый вирус

P.S.S. Селфи – это направление, которое будет предполагать рассмотрение вопросов, связанных с тем, каким образом составлять так называемые самоуничтожающиеся программы.

P.S.S.S. Спай – (от англ. Spy – Шпион) класс программ, предназначенных для осуществления шпионажа, а именно, например, определение того, каким образом пользователь работает на клавиатуре. Соответственно, есть клавиатурные шпионы. Чаще всего эти клавиатурные шпионы являются составной частью так называемых червей. В отличие от вирусов, черви не заражают собой другие файлы на том или ином компьютере, они просто шпионят, при необходимости создают копии себя, но не заражают другие файлы. Далее, будем говорить, каким образом связана безопасность информационных систем и вот это самое шпионство.

На ряду с червями и вирусами есть ещё целый класс плохих изделий, которые называются троянами. Это программы, которые кроме описанных в документации на ту или иную систему функций, исполняют некоторый не задокументированный функционал. Чаще всего, эти самые трояны являются составной частью легальной везде продаваемой и всеми желающими используемой программы. При этом дополнительный функционал, чаще всего, может уничтожать какие-то данные, может осуществлять модификацию программного обеспечения, может осуществлять перехват и передачу данных несанкционированному пользователю адресату, а также осуществлять сбор статистики о том, каким образом осуществляется использование того или иного программного обеспечения, в том числе могут собирать статистику в рамках социальных сетей: кто куда ходил, у кого какие друзья, кто какую рекламу смотрит, какие ботинки покупал и так далее и тому подобное. В отличие, от вирусов и червей, трояны не самовоспроизводятся и не распространяются сами по себе.

И ещё один тип изделий, о котором мы будем говорить, – это Rootkit-ы. Это программы, которые предназначены для сокрытия вредоносной активности путём модификации программных средств операционных систем таким образом, чтобы информация о функционировании как самой программы Rootkit, так и других нехороших badware, была скрыта от программных средств защиты.

Толкование №302

Загрузка программной части операционной системы осуществляется средствами BIOS (базовой системы ввода/вывода), при чём базовая система ввода/вывода, точно также, как система, состоит из программной и аппаратной части. Предполагается следующая последовательность действий:

1. Нажатие кнопки включения питания. При нажатии этой кнопки на материнскую плату попадает напряжение и запускается так называемый тактовый генератор. После этого начинает выполняться действие для включения базовой системы ввода/вывода.
2. Осуществляется проверка BIOS. А именно так называемая контрольная сумма системных программ, находящихся в постоянном запоминающем устройстве (ПЗУ), т.е. программ, которые зашиты в железе, пересчитывается и сравнивается с эталонным значением. Если все хорошо, то осуществляется переход к третьему действию.
3. Идентификация процессора. Базовая система ввода/вывода (BIOS) подаёт запрос на идентификацию процессора и по полученному ответу определяется тип процессора, частота и другие характеристики.
4. Настройка так называемых базовых элементов, а именно инициализируются и тестируются компоненты системной платы, такие как: блок прямого доступа к памяти, таймер и блок аппаратных прерываний.
5. Тестирование оперативного запоминающего устройства (ОЗУ). При этом тестируются первые 64 килобайта этой самой оперативной памяти. Поэтому самой программистской песней Beatles является When I’m 64.
6. Организация рабочих структур оперативной памяти. А именно выделяется место под программную компоненту базовой системы ввода/вывода и осуществляется надстройка программных прерываний.
7. Осуществляется проверка заряженности батарейки. В том случае, если батарейка неисправна, все настройки BIOS теряются, загрузка последней конфигурации становится невозможной, однако есть возможность осуществить загрузку стандартных заводских значений для BIOS.
8. Осуществляется поиск, инициализация и настройка жесткого диска, клавиатуры, мыши, устройств ввода/вывода и этим устройствам выделяются так называемые соответствующие линии прерывания.
9. Идентифицируются устройства, подключенные через так называемые системные разъемы.
10. Включение видеосистемы. Запускается система, которая настраивает видеоконтроллер на режим: VGA, HDMI, SVGA, EGA.
11. На экране монитора должно появится сообщение о фирме производителя базовой системы ввода/вывода, тип и частота процессора, тип и объем оперативной памяти (ОЗУ).
12. Тестирование оперативной памяти.
13. Инициализация контроллера жестких дисков.
14. Инициализация клавиатуры.
15. Поиск устройств с собственной базовой системой ввода/вывода.
16. Передача управления так называемому загрузчику программной части операционной системы. На дисковых накопителях (чаще всего, на жестком диске) ищется загрузчик программной части операционной системы (boot record). Он (этот загрузчик) находится, чаще всего, на жестком диске. Его местоположение везде одинаково. Этот загрузчик занимает строго определённое количество байт.

Для дальнейшего рассмотрения нам понадобится так называемая структура оперативной памяти. Про неё – на следующей лекции.