ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 63 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник_____С.Войцеховский

«___» _____ 201_ г.

Автор: старший преподаватель 27 кафедры
Кандидат технических наук
майор С.Краснов

Лекция № 14

Тема: «ОБЩИЕ СВЕДЕНИЯ О КОМПЬЮТЕРНЫХ ВИРУСАХ»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 27 кафедры
протокол № __ «____» _____ 201_ г.

Санкт-Петербург
2015

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Понятие компьютерного вируса и основные этапы его жизненного цикла – 40 мин.
2. Наиболее распространённые компьютерные вирусы и их классификация – 40 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области вредоносно ПО.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на жизненном цикле вирусов.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Перечислите основные группы вредоносного ПО?
2. Охарактеризуйте жизненный цикл вируса?
3. Перечислите наиболее распространённые компьютерные вирусы?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 12

Тема «Общие сведения о компьютерных вирусах»

В. 1. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов

Каждая программа обязательно несет в себе некоторую смысловую нагрузку - точно в соответствии с задумками программиста или же вследствие каких-либо причин немного видоизмененную. Например, электронный словарь должен помочь пользователю быстро и точно найти перевод заданного слова, браузер - просмотреть запрошенный веб-сайт, а калькулятор - вычислить квадратный корень. Ряд программ выполняют неявную цель - примером могут служить драйвера, которые в фоновом режиме обеспечивают взаимосвязь различных устройств компьютера.

Все упомянутые выше программы предназначены для выполнения полезной нагрузки и не должны выполнять какие-либо дополнительные действия, не связанные с обеспечением возложенных на них задач - калькулятор не должен проверять орфографию введенных формул или показывать точное время. То есть в идеальном варианте все программы должны вести себя четко в соответствии с их описанием и приложенной документацией, при этом пользователь должен полностью контролировать установку и удаление программы на свой компьютер. Однако на деле это не всегда так.

Существует класс программ, которые были изначально написаны с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов и т. п., или же приобрели такие свойства вследствие каких-либо причин. Такие программы несут вредоносную нагрузку и соответственно называются вредоносными.

Вредоносная программа - это программа, наносящая какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети.

Поскольку мало пользователей в здравом уме добровольно поставят себе на компьютер заведомо вредоносную программу, их авторы вынуждены использовать различные обманные методы или специальные технологии для несанкционированного проникновения в систему.

Определение компьютерного вируса — исторически проблемный вопрос, поскольку достаточно сложно дать четкое определение вируса, очертив при этом свойства, присущие только вирусам и не касающиеся других программных систем. Наоборот, давая жесткое определение вируса как программы, обладающей определенными свойствами, практически сразу же можно найти пример вируса, таковыми свойствами не обладающего.

Приведем несколько формулировок определения:

Хронологически наиболее раннее определение от Евгения Касперского (книга "Компьютерные вирусы"). **Обязательным (необходимым) свойством компьютерного вируса** является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Определение по ГОСТ Р 51188-98. ***Вирус*** — программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Легко заметить, что определение в ГОСТ практически полностью повторяет определение Е. Касперского.

Можно дать другое определение. ***Под компьютерным вирусом*** будем понимать компьютерную программу, разработанную с целью нанесения ущерба пользователям вычислительной системы.

Основной особенностью большинства компьютерных вирусов является способность к скрытому саморазмножению. Саморазмножение или, как его еще называют, репродуцирование вируса выполняется путем включения в исполняемые или хранящиеся программы своей, возможно модифицированной копии, сохраняющей способность к дальнейшему саморазмножению.

Свойство саморазмножения вирусов само по себе представляет одну из его опасностей и может привести к снижению, вплоть до нуля, производительности вычислительной системы. Это происходит за счет повышения количества ресурсов ВС, расходуемых на выполнение программ-вирусов:

• увеличивается время процессора, расходуемое на выполнение саморазмножающихся вирусных программ;

• увеличивается задействованное пространство оперативной памяти зараженного компьютера, которое последовательно занимают получаемые в результате саморазмножения копии вируса;

• увеличиваются объемы ресурсов внешних устройств, задействованных в процессе саморазмножения.

Проблема, связанная с определением компьютерного вируса кроется в том, что сегодня под вирусом чаще всего понимается не "традиционный" вирус, а практически любая вредоносная программа. Первые широко известные вредоносные программы были именно вирусами, и в течение следующих десятилетий число вирусов значительно превышало количество всех остальных вредоносных программ вместе взятых. Однако в последнее время наметились тенденции к появлению новых, невирусных технологий, которые используют вредоносные программы. При этом доля истинных вирусов в общем, числе инцидентов с вредоносными программами за последние годы значительно сократилась. На сегодняшний день вредоносные программы - это уже большей частью именно не вирусы, хотя такие термины как "заражение вирусом", "вирусный инцидент" применяются по отношению ко всем вредоносным программам повсеместно. Поэтому термином "компьютерный вирус" часто называют любую вредоносную программу.

Это приводит к путанице в терминологии, осложненной еще и тем, что практически все современные антивирусы способны выявлять указанные типы вредоносных программ, таким образом ассоциация "вредоносная программа-вирус" становится все более устойчивой.

Исходя из этого, а также из назначения антивирусных средств, в дальнейшем, если это не будет оговорено отдельно, под вирусами будут подразумеваться именно вредоносные программы.

2. Классификация вредоносных программ

Классифицировать вредоносные программы удобно по способу проникновения, размножения и типу вредоносной нагрузки.

Все вредоносные программы в соответствии со способами распространения и вредоносной нагрузкой можно разделить на четыре основные типа:

- компьютерные вирусы,
- черви,
- трояны,
- другие программы.

Вирусы

Определения компьютерного вируса приведены выше. Основная черта компьютерного вируса - это способность к саморазмножению.

Жизненный цикл компьютерного вируса может включать следующие этапы:

- проникновение на чужой компьютер (внедрение или инфицирование),
- латентная фаза, в течение которой вирус не выполняет никаких действий,
- активация (фаза проявления),
- поиск объектов для заражения,
- подготовка копий,
- внедрение копий,
- этап выполнения специальных целевых функций.

Перечисленные этапы, кроме первого, могут выполняться в любой последовательности, повторяться, и не все являются обязательными. Особую опасность представляют стадии выполнения специальных функций и саморазмножения, которые могут иметь катастрофические последствия для компьютерной системы.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения - фактически, все каналы, по которым можно скопировать файл. Однако в отличие от червей, вирусы не используют сетевые ресурсы - заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал. Например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует ***активация вируса.*** Это может происходить несколькими путями и в соответствии с выбранным методом вирусы делятся на такие виды:

1. **Загрузочные вирусы** заражают загрузочные сектора жестких дисков и мобильных носителей. (Например: вирус Virus.Boot.DiskFiller заражает MBR винчестера или загрузочные сектора дискет, остается в памяти и перехватывает прерывания - INT 13h, 1Ch и 21h.)
2. **Файловые вирусы** - заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют:

Классические файловые вирусы - они различными способами внедряются в исполняемые файлы (внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы

Пример. Самый известный файловый вирус всех времен и народов — Virus.Win9x.CIH, известный также как "Чернобыль". Имея небольшой размер - около 1 кб - вирус заражает PE-файлы (Portable Executable) на компьютерах под управлением операционных систем Windows 95/98 таким образом, что размер зараженных файлов не меняется. Для достижения этого эффекта вирус ищет в файлах "пустые" участки, возникающие из-за выравнивания начала каждой секции файла под кратные значения байт. После получения управления вирус перехватывает IFS API, отслеживая вызовы функции обращения к файлам и заражая исполняемые файлы. 26 апреля срабатывает деструктивная функция вируса, которая заключается в стирании Flash BIOS и начальных секторов жестких дисков. Результатом является неспособность компьютера загружаться вообще (в случае успешной попытки стереть Flash BIOS) либо потеря данных на всех жестких дисках компьютера.

Макровирусы, которые написаны на внутреннем языке, так называемых макросах какого-либо приложения. В подавляющем большинстве случаев речь идет о макросах в документах Microsoft Office.

Примеры. Одними из наиболее разрушительных макровирусов являются представители семейства **Macro.Word97.Thus**. Эти вирусы содержат три процедуры Document_Open, Document_Close и Document_New, которыми подменяет стандартные макросы, выполняющиеся при открытии, закрытии и создании документа, тем самым обеспечивая заражение других документов. 13 декабря срабатывает деструктивная функция вируса - он удаляет все файлы на диске C:, включая каталоги и подкаталоги.

Модификация **Macro.Word97.Thus.aa** кроме указанных действий при открытии каждого зараженного документа выбирает на локальном диске случайный файл и шифрует первые 32 байта этого файла, постепенно приводя систему в неработоспособное состояние.

Макро-вирусы способны заражать не только документы Microsoft Word и Excel. Существуют вредоносные программы ориентированные и на другие типы документов: **Macro.Visio.Radiant** заражает файлы известной программы для построения диаграмм -Visio, V**irus.Acad.Pobresito** - документы AutoCAD, **Macro.AmiPro.Green** - документы популярного раньше текстового процессора Ami Pro.

Скрипт-вирусы, написанные в виде скриптов для определенной командной оболочки - например, bat-файлы для DOS или VBS и JS - скрипты для Windows Scripting Host (WSH)

Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Это означает, что вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например

Unix. Точно также макровирус для Microsoft Word 2003 скорее всего не будет работать в приложении Microsoft Excel 97.

Примеры. **Virus.VBS.Slin**g написан на языке VBScript (Visual Basic Script). При запуске он ищет файлы с расширениями .VBS или .VBE и заражает их. При наступлении 16-го июня или июля вирус при запуске удаляет все файлы с расширениями .VBS и .VBE, включая самого себя.

Virus.WinHLP.Pluma.a – вирус, заражающий файлы помощи Windows. При открытии зараженного файла помощи выполняется вирусный скрипт, который используя нетривиальный метод (по сути, уязвимость в обработке скриптов) запускает на выполнение уже как обычный файл Windows определенную строку кода, содержащеюся в скрипте. Запущенный код производит поиск файлов справки на диске и внедряет в их область System скрипт автозапуска.

В эпоху вирусов для DOS часто встречались гибридные файлово-загрузочные вирусы. После массового перехода на операционные системы семейства Windows практически исчезли как сами загрузочные вирусы, так и упомянутые гибриды.

Поиск жертв

На стадии поиска объектов для заражения встречается два способа поведения вирусов:

1. Получив управление, вирус производит разовый поиск жертв, после чего передает управление ассоциированному с ним объекту (зараженному объекту).
2. Получив управление, вирус так или иначе остается в памяти и производит поиск жертв непрерывно, до завершения работы среды, в которой он выполняется.

Подготовка вирусных копий

Сигнатура вируса – в широком смысле, информация, позволяющая однозначно определить наличие данного вируса в файле или ином коде. Примерами сигнатур являются: уникальная последовательность байт, присутствующая в данном вирусе и не встречающаяся в других программах; контрольная сумма такой последовательности.

Процесс подготовки копий для распространения может существенно отличаться от простого копирования. Авторы наиболее сложных в технологическом плане вирусов стараются сделать разные копии максимально непохожими для усложнения их обнаружения антивирусными средствами. Как следствие, составление сигнатуры для такого вируса крайне затруднено либо вовсе невозможно.

При подготовке своих вирусных копий для маскировки от антивирусов могут применять такие технологии как:

Шифрование - в этом случае вирус состоит из двух частей: сам вирус и шифратор.

Метаморфизм - при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительного, обычно ничего не делающих команд.

Соответственно в зависимости от используемых методов вирусы можно делить на ***шифрованные, метаморфные и полиморфные***, использующие комбинацию двух типов маскировки.

Внедрение

Внедрение вирусных копий может осуществляться двумя принципиально разными методами:

1. Внедрение вирусного кода непосредственно в заражаемый объект.
2. Замена объекта на вирусную копию. Замещаемый объект, как правило, переименовывается.

Для вирусов характерным является преимущественно первый метод. Второй метод намного чаще используется червями и троянами, а точнее троянскими компонентами червей, поскольку трояны сами по себе не распространяются.

Основные цели любого компьютерного вируса - это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 26 числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Файловые вирусы могут внедряться в файлы следующих типов:

1) программные файлы с компонентами операционной системы;

2) любые исполняемые файлы с расширениями .EXE и .COM;

3) командные файлы и файлы конфигурирования;

4) файлы, составляемые на макроязыках программирования, или файлы, которые могут включать выполняемые макросы, напри¬мер, файлы документов редактора WORD, файлы баз данных-СУБД ACCESS;

5) файлы с внешними драйверами устройств (обычно имеют расши-рения .SYS и .BIN);

6) объектные модули и библиотеки, файлы которых, как правило, имеют расширение .OBJ;

7) оверлейные файлы (обычно имеют расширение .OVR и .RTL);

8) библиотеки динамической компоновки, файлы которых имеют расширение .DLL;

9) исходные тексты программ.

Загрузочные вирусы могут заражать следующие программы:

• системный загрузчик, расположенный в стартовом секторе (BR) дискет и логических дисков;

• внесистемный загрузчик, расположенный в стартовом секторе (MBR) жестких дисков.

Черви

К сожалению, определение червя отсутствует в государственных стандартах и распорядительных документах, поэтому здесь приведено лишь интуитивное определение, дающее представление о принципах работы и выполняемых функциях этого типа вредоносных программ.

Червь (сетевой червь) — тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.

Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов. Для подчеркивания этого свойства иногда используют термин "сетевой червь".

Жизненный цикл червей можно разделить на определенные стадии:

1. Проникновение в систему
2. Активация
3. Поиск "жертв"
4. Подготовка копий
5. Распространение копий

Стадии 1 и 5, вообще говоря, симметричны и характеризуются в первую очередь используемыми протоколами и приложениями.

Стадия 4 – Подготовка копий – практически ничем не отличается от аналогичной стадии в процессе размножения вирусов. Сказанное о подготовке копий вирусов без изменений применимо и к червям.

Каналы распространения

На этапе проникновения в систему черви делятся преимущественно по типам используемых протоколов:

Сетевые черви — черви, использующие для распространения протоколы Интернет и локальных сетей. Обычно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов tcp/ip

Почтовые черви — черви, распространяющиеся в формате сообщений электронной почты

IRC-черви — черви, распространяющиеся по каналам IRC (Internet Relay Chat)

P2P-черви — черви, распространяющиеся при помощи пиринговых (peer-to-peer) файлообменных сетей

IM-черви — черви, использующие для распространения системы мгновенного обмена сообщениями (IM, Instant Messenger - ICQ, MSN Messenger, AIM и др.)

Примеры. Классическими сетевыми червями являются представители семейства **Net-Worm.Win32.Sasser**. Эти черви используют уязвимость в службе LSASS Microsoft Windows. При размножении, червь запускает FTP-службу на TCP-порту 5554, после чего выбирает IP-адрес для атаки и отсылает запрос на порт 445 по этому адресу, проверяя, запущена ли служба LSASS. Если атакуемый компьютер отвечает на запрос, червь посылает на этот же порт эксплойт уязвимости в службе LSASS, в результате успешного выполнения которого на удаленном компьютере

запускается командная оболочка на TCP-порту 9996. Через эту оболочку червь удаленно выполняет загрузку копии червя по протоколу FTP с запущенного ранее сервера и удаленно же запускает себя, завершая процесс проникновения и активации.

В качестве примера почтового червя можно рассмотреть **Email-Worm.Win32.Zafi.d**. Зараженное сообщение включает в себя выбираемые из некоторого списка тему и текст, содержанием которых является поздравление с праздником (большая часть - с Рождеством) и предложение ознакомиться с поздравительной открыткой во вложении. Поздравления могут быть на разных языках. Имя находящегося во вложении файла червя состоит из слова postcard на языке, соответствующем поздравлению, и произвольного набора символов. Расширение файла червя случайным образом выбирается из списка .BAT, .COM, .EXE, .PIF, .ZIP. Для рассылки червь использует адреса электронной почты, найденные на зараженном компьютере. Чтобы получить управление, червь должен быть запущен пользователем.

IRC-Worm.Win32.Golember.a является, как следует из названия IRC-червем. При запуске он сохраняет себя в каталоге Windows под именем trlmsn.exe и добавляет в раздел автозапуска реестра Windows параметр со строкой запуска этого файла. Кроме этого червь сохраняет на диск свою копию в виде архива Janey2002.zip и файл-изображение Janey.jpg. Затем червь подключается к произвольным IRC-каналам под различными именами и начинает слать определенные текстовые строки, имитируя активность обычного пользователя. Параллельно всем пользователям этих каналов отсылается заархивированная копия червя.

Функциональностью распространения через P2P-каналы обладают многие сетевые и почтовые черви. Например, Email-Worm.Win32.Netsky.q для размножения через файлообменные сети ищет на локальном диске каталоги, содержащие названия наиболее популярных сетей или же слово "shared", после чего кладет в эти каталоги свои копии под различными названиями.

IM-черви редко пересылают зараженные файлы непосредственно между клиентами. Вместо этого они рассылают ссылки на зараженные веб-страницы. Так червь IM-Worm.Win32.Kelvir.k посылает через MSN Messenger сообщения, содержащие текст "its you" и ссылку "http://www.malignancy.us/[removed]/pictures.php?email=[email]", по указанному в которой адресу расположен файл червя.

Сегодня наиболее многочисленную группу составляют почтовые черви. Сетевые черви также являются заметным явлением, но не столько из-за количества, сколько из-за качества: эпидемии, вызванные сетевыми червями зачастую отличаются высокой скоростью распространения и большими масштабами. IRC-, P2P- и IM-черви встречаются достаточно редко, чаще IRC, P2P и IM служат альтернативными каналами распространения для почтовых и сетевых червей.

Способы активации

На этапе активации **черви делятся на две большие группы**, отличающиеся как по технологиям, так и по срокам жизни:

1. Для активации необходимо активное участие пользователя
2. Для активации участие пользователя не требуется вовсе либо достаточно лишь пассивного участия

Под пассивным участием пользователя во второй группе понимается, например, просмотр писем в почтовом клиенте, при котором пользователь не открывает вложенные файлы, но его компьютер, тем не менее, оказывается зараженным.

Отличие в этих подходах глубже, чем может показаться на первый взгляд. Активация сетевого червя без участия пользователя всегда означает, что червь использует бреши в безопасности программного обеспечении компьютера. Это приводит к очень быстрому распространению червя внутри корпоративной сети с большим числом станций, существенно увеличивает загрузку каналов связи и может полностью парализовать сеть. Именно этот метод активации использовали черви Lovesan и Sasser. В результате вызванной таким сетевым червем эпидемии, используемая брешь закрывается администраторами либо пользователями, и по мере уменьшения компьютеров с открытой брешью эпидемия завершается. Для повторения эпидемии разработчикам вирусов приходится эксплуатировать другую брешь. В итоге, эпидемии, вызванные активными червями, существеннее влияют на работу сети в целом, однако случаются значительно реже, чем эпидемии пассивных сетевых червей. Обязательной мерой защиты от таких эпидемий

является своевременная установка заплат безопасности. Отметим также, что особенно уязвимыми для этого типа червей являются операционные системы с заложенными возможностями удаленного управления или запуска программ - это семейство Microsoft Windows NT/2000/XP/2003.

Пример. Уязвимость в службе LSASS, впервые использованная в черве MyDoom в начале 2004 года, продолжала успешно применяться и спустя полтора года. Так Net-Worm.Win32.Mytob.be обнаруженный в июне 2005 все еще использовал эту уязвимость как один из способов распространения, в дополнение к распространению через электронную почту.

С другой стороны, активное участие пользователя в активации червя означает, что пользователь был введен в заблуждение методами социальной инженерии. В большинстве случаев основным фактором служит форма подачи инфицированного сообщения: оно может имитировать письмо от знакомого человека (включая электронный адрес, если знакомый уже заражен), служебное сообщение от почтовой системы или же что-либо подобное, столь же часто встречающееся в потоке обычной корреспонденции. Пользователь в суматохе просто не отличает обычное письмо от зараженного и производит запуск автоматически.

Защититься заплатами от такого рода червей невозможно. Даже внесение сигнатуры сетевого червя в вирусную базу данных не решает проблему до конца. Разработчикам вируса достаточно изменить исполняемый файл так, чтобы антивирус его не обнаруживал, и незначительно поменять текст сообщения, используя в том числе и технологии спам-рассылок, применяемые для обхода фильтров.

В результате, эпидемии, вызванные пассивными сетевыми червями, могут быть гораздо продолжительнее и порождать целые семейства однотипных сетевых червей.

В последнее время наметилась тенденция к совмещению в червях обоих способов распространения. Многие представители семейства Mytob обладают функциями распространения через электронную почту и через уязвимость в службе LSASS.

Поиск "жертв"

Способ поиска компьютера-жертвы полностью базируется на используемых протоколах и приложениях. В частности, если речь идет о почтовом черве, производится сканирование файлов компьютера на предмет наличия в них адресов электронной почты, по которым в результате и производится рассылка копий червя.

Точно так же Интернет-черви сканируют диапазон IP адресов в поисках уязвимых компьютеров, а P2P черви кладут свои копии в общедоступные каталоги клиентов пиринговых сетей. Некоторые черви способны эксплуатировать списки контактов интернет-пейджеров, таких как ICQ, AIM, MSN Messenger, Yahoo! Messenger и др.

Подготовка копий для распространения

Сказанное ранее о подготовке копий для распространения вирусов, применимо и для червей.

Наиболее часто среди червей встречаются упрощенные реализации метаморфизма. Некоторые черви способны рассылать свои копии в письмах, как с внедрением скрипта приводящего к автоматической активации червя, так и без внедрения. Такое поведение червя обусловлено двумя факторами: скрипт автоматической активации повышает вероятность запуска червя на компьютере пользователя, но при этом уменьшает вероятность проскочить антивирусные фильтры на почтовых серверах.

Аналогично, черви могут менять тему и текст инфицированного сообщения, имя, расширение и даже формат вложенного файла - исполняемый модуль может быть приложен как есть или в заархивированном виде. Все это нельзя считать мета- или полиморфизмом, но определенной долей изменчивости черви, безусловно, обладают.

Трояны

Приведем интуитивное определение троянской программы или трояна.

Под ***троянской программой*** понимается программа, имеющая законный доступ к компьютерной системе, но выполняющая вместе с основными и скрытые (необъявленные) функции, реализуемые посредством ее вирусоподобного компонента.

Трояны отличаются отсутствием механизма создания собственных копий. Некоторые трояны способны к автономному преодолению систем защиты КС, с целью проникновения и заражения системы. В общем случае, троян попадает в систему вместе с вирусом либо червем, в результате неосмотрительных действий пользователя или же активных действий злоумышленника.

Жизненный цикл

В силу отсутствия у троянов функций размножения и распространения, их жизненный цикл крайне короток - всего три стадии:

- Проникновение на компьютер
- Активация
- Выполнение заложенных функций

Это, само собой, не означает малого времени жизни троянов. Напротив, троян может длительное время незаметно находиться в памяти компьютера, никак не выдавая своего присутствия, до тех пор, пока не будет обнаружен антивирусными средствами.

Способы проникновения

Задачу проникновения на компьютер пользователя трояны решают обычно одним из двух следующих методов.

1. **Маскировка** — троян выдает себя за полезное приложение, которое пользователь самостоятельно загружает из Интернет и запускает. Иногда пользователь исключается из этого процесса за счет размещения на Web-странице специального скрипта, который используя дыры в браузере автоматически инициирует загрузку и запуск трояна.

   Пример. Trojan.SymbOS.Hobble.a является архивом для операционной системы Symbian (SIS-архивом). При этом он маскируется под антивирус Symantec и носит имя symantec.sis. После запуска на смартфоне троян подменяет оригинальный файл оболочки FExplorer.app на поврежденный файл. В результате при следующей загрузке операционной системы большинство функций смартфона оказываются недоступными

   Одним из вариантов маскировки может быть также внедрение злоумышленником троянского кода в код другого приложения. В этом случае распознать троян еще сложнее, так как зараженное приложение может открыто выполнять какие-либо полезные действия, но при этом тайком наносить ущерб за счет троянских функций.

   Распространен также способ внедрения троянов на компьютеры пользователей через веб-сайты. При этом используется либо вредоносный скрипт, загружающий и запускающий троянскую программу на компьютере пользователя, используя уязвимость в веб-браузере, либо методы социальной инженерии - наполнение и оформление веб-сайта провоцирует пользователя к самостоятельной загрузке трояна. При таком методе внедрения может использоваться не одна копия трояна, а полиморфный генератор, создающий новую копию при каждой загрузке. Применяемые в таких генераторах технологии полиморфизма обычно не отличаются от вирусных полиморфных технологий.

2. **Кооперация с вирусами и червями** — троян путешествует вместе с червями или, реже, с вирусами. В принципе, такие пары червь-троян можно рассматривать целиком как составного червя, но в сложившейся практике принято троянскую составляющую червей, если она реализована отдельным файлом, считать независимым трояном с собственным именем. Кроме того, троянская составляющая может попадать на компьютер позже, чем файл червя.

   Пример. Используя backdoor-функционал червей семейства Bagle, автор червя проводил скрытую инсталляцию трояна SpamTool.Win32.Small.b, который собирал и отсылал на определенный адрес адреса электронной почты, имевшиеся в файлах на зараженном компьютере.

   Нередко наблюдается кооперация червей с вирусами, когда червь обеспечивает транспортировку вируса между компьютерами, а вирус распространяется по компьютеру, заражая файлы.

   Пример. Известный в прошлом червь Email-Worm.Win32.Klez.h при заражении компьютера также запускал на нем вирус Virus.Win32.Elkern.c. Зачем это было сделано, сказать тяжело, поскольку вирус сам по себе, кроме заражения и связанных с ошибками в

коде вредоносных проявлений (явно выраженных вредоносных процедур в нем нет), никаких действий не выполняет, т. е. не является "усилением" червя в каком бы то ни было смысле.

Активация

Здесь приемы те же, что и у червей: ожидание запуска файла пользователем, либо использование уязвимостей для автоматического запуска.

Выполняемые функции

В отличие от вирусов и червей, деление которых на типы производится по способам размножения/распространения, трояны делятся на типы по характеру выполняемых ими вредоносных действий. Наиболее распространены следующие виды троянов.

- ***Клавиатурные шпионы*** — трояны, постоянно находящиеся в памяти и сохраняющие все данные, поступающие от клавиатуры с целью последующей передачи этих данных злоумышленнику. Обычно таким образом злоумышленник пытается узнать пароли или другую конфиденциальную информацию.

Пример. В прошлом, буквально пару лет назад еще встречались клавиатурные шпионы, которые фиксировали все нажатия клавиш и записывали их в отдельный файл. Trojan-Spy.Win32.Small.b, например, в бесконечном цикле считывал коды нажимаемых клавиш и сохранял их в файле C:\SYS

Современные программы-шпионы оптимизированы для сбора информации, передаваемой пользователем в Интернет, поскольку среди этих данных могут встречаться логины и пароли к банковским счетам, PIN-коды кредитных карт и прочая конфиденциальная информация, относящаяся к финансовой деятельности пользователя. Trojan-Spy.Win32.Agent.fa отслеживает открытые окна Internet Explorer и сохраняет информацию с посещаемых пользователем сайтов, ввод клавиатуры в специально созданный файл servms.dll с системном каталоге Windows.

- ***Похитители паролей*** — трояны, также предназначенные для получения паролей, но не использующие слежение за клавиатурой. В таких троянах реализованы способы извлечения паролей из файлов, в которых эти пароли хранятся различными приложениями.

Пример. Trojan-PSW.Win32.LdPinch.kw собирает сведения о системе, а также логины и пароли для различных сервисов и прикладных программ - мессенджеров, почтовых клиентов, программ дозвона. Часто эти данные оказываются слабо защищены, что позволяет трояну их получить и отправить злоумышленнику по электронной почте

- ***Утилиты удаленного управления*** — трояны, обеспечивающие полный удаленный контроль над компьютером пользователя. ' Существуют легальные утилиты такого же свойства, но они отличаются тем, что сообщают о своем назначении при установке или же снабжены документацией, в которой описаны их функции. Троянские утилиты удаленного управления, напротив, никак не выдают своего реального назначения, так что пользователь и не подозревает о том, что его компьютер подконтролен злоумышленнику. Наиболее популярная утилита удаленного управления - Back Orifice.

Пример. Backdoor.Win32.Netbus.170 предоставляет полный контроль над компьютером пользователя, включая выполнение любых файловых операций, загрузку и запуск других программ, получение снимков экрана и т. д.

- ***Люки (backdoor)*** — трояны предоставляющие злоумышленнику ограниченный контроль над компьютером пользователя. От утилит удаленного управления отличаются более простым устройством и, как следствие, небольшим количеством доступных действий. Тем не менее, обычно одними из действий являются возможность загрузки и запуска любых файлов по команде злоумышленника, что позволяет при необходимости превратить ограниченный контроль в полный.

Пример. В последнее время backdoor-функционал стал характерной чертой червей. Например, Email-Worm.Win32.Bagle.at использует порт 81 для получения удаленных команд или загрузки троянов, расширяющих функционал червя.

Есть и отдельные трояны типа backdoor. Троян Backdoor.win32.Wootbot.gen использует IRC-канал для получения команд от "хозяина". По команде троян может

загружать и запускать на выполнение другие программы, сканировать другие компьютеры на наличие уязвимостей и устанавливать себя на компьютеры через обнаруженные уязвимости.

- ***Анонимные smtp-сервера и прокси*** — трояны, выполняющие функции почтовых серверов или прокси и использующиеся в первом случае для спам-рассылок, а во втором для заметания следов хакерами.

Пример. Трояны из семейства Trojan-Proxy.Win32.Mitglieder распространяются с различными версиями червей Bagle. Троян запускается червем, открывает на компьютере порт и отправляет автору вируса информацию об IP-адресе зараженного компьютера. После этого компьютер может использоваться для рассылки спама

- ***Утилиты дозвона*** — сравнительно новый тип троянов, представляющий собой утилиты dial-up доступа в Интернет через дорогие почтовые службы. Такие трояны прописываются в системе как утилиты дозвона по умолчанию и влекут за собой огромные счета за пользование Интернетом.

Пример. Trojan.Win32.Dialer.a при запуске осуществляет дозвон в Интернет через платные почтовые службы. Никаких других действий не производит, в том числе не создает ключей в реестре, т. е. даже не регистрируется в качестве стандартной программы дозвона и не обеспечивает автозапуск.

- ***Модификаторы настроек браузера*** — трояны, которые меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна браузера, имитируют нажатия на баннеры и т. п.

Пример. Trojan-Clicker.JS.Pretty обычно содержится в html-страницах. Он открывает дополнительные окна с определенными веб-страницами и обновляет их с заданным интервалом

- ***Логические бомбы*** — чаще не столько трояны, сколько троянские составляющие червей и вирусов, суть работы которых состоит в том, чтобы при определенных условиях (дата, время суток, действия пользователя, команда извне) произвести определенное действие: например, уничтожение данных

Пример. Virus.Win9x.CIH, Macro.Word97.Thus

Другие вредоносные программы

Кроме вирусов, червей и троянов существует еще множество других вредоносных программ, для которых нельзя привести общий критерий. Однако среди них можно выделить небольшие группы. Это в первую очередь:

- **Условно опасные программы**, то есть такие, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:
  - **Riskware** (сокращение от англ. Risk Software - опасное программное обеспечение) - вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернет, утилиты восстановления забытых паролей и другие.
  - Рекламные утилиты (adware), (сокращение от англ. Advertisement Software - рекламное программное обеспечение) - условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается, и программы начинают работать в обычном режиме. Проблема adware кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, что для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже

после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме. Однако среди adware-программ есть и вполне заслуживающие доверия - например, клиент ICQ.

- **Pornware** (порнографическое программное обеспечение) - к этому классу относятся утилиты, так или иначе связанные с показом пользователям информации порнографического характера. На сегодняшний день это программы, которые самостоятельно дозваниваются до порнографических телефонных служб, загружают из Интернет порнографические материалы или утилиты, предлагающие услуги по поиску и показу такой информации. Отметим, что к вредоносным программам относятся только те утилиты класса pornware, которые устанавливаются на компьютер пользователя несанкционированно - через уязвимость в операционной системы или браузера или при помощи троянов. Обычно это делается с целью насильственного показа рекламы платных порнографических сайтов или служб.

- **Хакерские утилиты** (от англ. жарг. hack - рубить, кромсать) обычно называют людей, способных проникнуть в чужую компьютерную - К этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit) и другие подобные утилиты. То есть такие специфические программы, которые обычно используют только хакеры.

- **Злые шутки (**сокращение от англ. Risk Software) - опасное программное обеспечение - программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений о, например, форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений целиком и полностью отражает фантазию автора.

Ущерб от вредоносных программ

Черви и вирусы могут осуществлять все те же действия, что и трояны (см.предыдущий пункт). На уровне реализации это могут быть как отдельные троянские компоненты, так и встроенные функции. Кроме этого, за счет массовости, для вирусов и червей характерны также другие формы вредоносных действий:

- **Перегрузка каналов связи** — свойственный червям вид ущерба, связанный с тем, что во время масштабных эпидемий по Интернет-каналам передаются огромные количества запросов, зараженных писем или непосредственно копий червя. В ряде случаев, пользование услугами Интернет во время эпидемии становится затруднительным. Примеры: Net-Worm.Win32.Slammer

- **DDoS атаки** — благодаря массовости, черви могут эффективно использоваться для реализации распределенных атак на отказ в обслуживании (DDoS атак). В разгар эпидемии, когда зараженными являются миллионы и даже десятки миллионов компьютеров, обращение всех инфицированных систем к определенному Интернет ресурсу приводит к полному блокированию этого ресурса. Так, во время атаки червя MyDoom сайт компании SCO был недоступен в течение месяца. Примеры: Net-Worm.Win32.CodeRed.a - не совсем удачная атака на http://www.intuit.ru/department/security/viruskasper/3/www.whitehouse.gov, Email-Worm.Win32.Mydoom.a - удачная атака на http://www.intuit.ru/department/security/viruskasper/3/www.sco.com

- **Потеря данных** — более характерное для вирусов, чем для троянов и червей, поведение, связанное с намеренным уничтожением определенных данных на компьютере пользователя. Примеры: Virus.Win9x.CIH - удаление стартовых секторов дисков и содержимого Flash BIOS, Macro.Word97.Thus - удаление всех файлов на диске C:, Email-Worm.Win32.Mydoom.e - удаление файлов с определенными расширениями в зависимости от показателя счетчика случайных чисел

- **Нарушение работы ПО** — также более свойственная вирусам черта. Из-за

ошибок в коде вируса, зараженные приложения могут работать с ошибками или не работать вовсе. Примеры: Net-Worm.Win32.Sasser.a - перезагрузка зараженного компьютера

- **Загрузка ресурсов компьютера** — интенсивное использование ресурсов компьютера вредоносными программами ведет к снижению производительности как системы в целом, так и отдельных приложений. Примеры: в разной степени - любые вредоносные программы

Заключение:

Таким образом, в лекции были рассмотрены следующие вопросы:

1. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов.
2. Классификация компьютерных вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов.

На самостоятельной подготовке прочитать материалы из рекомендуемой литературы. Найти в Интернете материалы о сигнатуре известных вирусов.

КАНДИДАТ ТЕХНИЧЕСКИХ НАУК ПОЛКОВНИК
_____Е. ВОРОБЬЕВ

«_____» _____ 200_ г.