ЛЕКЦИЯ №19

КОМПЬЮТЕРНЫЕ ВИРУСЫ. АНТИВИРУСНОЕ ПО

Первые исследования **саморазмножающихся искусственных конструкций** проводились в середине прошлого столетия. В работах фон Неймана, Винера и других авторов дано определение и проведен математический анализ конечных автоматов, в том числе и самовоспроизводящихся. Термин «**компьютерный вирус**» появился позднее - официально считается, что его впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США.

Пандемия **первого IBM-PC вируса «Brain».** Вирус, заражающий 360Кб дискеты, практически мгновенно разошелся по всему миру. Причиной такого «успеха» являлась скорее всего неготовность компьютерного общества к встрече с таким явлением, как компьютерный вирус. Вирус был написан в Пакистане братьями Basit и Amjad Farooq Alvi, оставившими в вирусе текстовое сообщение, содержащее их имена, адрес и телефонный номер. Как утверждали авторы вируса, они являлись владельцами компании по продаже программных продуктов и решили выяснить уровень пиратского копирования в их стране. К сожалению, их эксперимент вышел за границы Пакистана. Интересно, что вирус «Brain» являлся также и первым стелс-вирусом - при попытке чтения зараженного сектора он «подставлял» его незараженный оригинал

В пятницу 13-го мая 1988-го года сразу несколько фирм и университетов нескольких стран мира «познакомились» с вирусом «Jerusalem» - в этот день вирус уничтожал файлы при их запуске. Это, пожалуй, один из первых MS-DOS-вирусов, ставший причиной настоящей пандемии - сообщения о зараженных компьютерах поступали из Европы, Америки и Ближнего Востока. Название, кстати, вирус получил по месту одного из инцидентов - университета в Иерусалиме.

Ноябрь 1988: повальная эпидемия сетевого вируса Морриса (другое название - Internet Worm). Вирус заразил более 6000 компьютерных систем в США (включая NASA Research Institute) и практически парализовал их работу. По причине ошибки в коде вируса он, как и вирус-червь «Cristmas Tree», неограниченно рассылал свои копии по другим компьютерам сети и, таким образом, полностью забрал под себя ее ресурсы. Общие убытки от вируса Морриса были оценены в 96 миллионов долларов.

Июнь1998: эпидемия вируса «Win95.CIH», ставшая сначала массовой, затем глобальной, а затем повальной - сообщения о заражении компьютерных сетей и домашних персональных компьютеров исчислялись сотнями, если не тысячами. Начало эпидемии зарегистрировано на Тайване, где неизвестный хакер заслал зараженные файлы в местные Интернет-конференции. Оттуда вирус пробрался в США, где по недосмотру зараженными оказались сразу несколько популярных Web-серверов - они распространяли зараженные вирусом игровые программы. Скорее всего, именно эти зараженные файлы на игровых серверах и послужили причиной повальной эпидемии вируса, не ослабевавшей в течении всего года. По результатам рейтингов «популярности» вирус «подвинул» таких вирусных суперзвезд, как «Word.CAP» и «Excel.Laroux». Следует обратить внимание также на опасное проявление вируса: в зависимости от текущей даты вирус стирал Flash BIOS, что в некоторых случаях могло привести к необходимости замены материнской платы.

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 компьютерного вируса - набор команд (программных или иных), который производит и распространяет свои копии в компьютерных системах и/ или компьютерных сетях и преднамеренно выполняет некоторые действия, нежелательные для законных пользователей системы или специально написанная, небольшая по размерам программа, которая может приписывать себя к другим программам т. е. “заражать” их, а также выполнять различные нежелательные действия в компьютере.

Свойства вирусов:

1) способность к саморазмножению и эволюции;
2) высокая скорость распространения;
3) избирательность поражённых систем (каждый вирус поражает определённые системы и группы);
4) способность “заражать” “незаражённые” системы;
5) трудность борьбы с вирусами;
6) увеличивается быстрота появлений модификаций и новых поколений вирусов.

Признаки “заражённости”:

1) необычная, странная работа компьютера (частые самопроизвольные перезагрузки);
2) некоторые программы не работают или работают неверно;
3) компьютер часто “зависает”;
4) работа существенно замедляется;
5) на экран выводятся посторонние сообщения;
6) искажается содержание файлов;
7) появление не существовавших ранее “странных” файлов;
8) не загружается ОС.

Действия вируса над файлами.

Вирус может:

1) испортить файл т.е. исказить его содержание. Это тексты программ и документов, файлы баз данных или электронных таблиц.
2) “заразить” файл, т. е. внедриться, приписаться к нему. Такой файл является источником вируса.

КЛАССИФИКАЦИЯ ВИРУСОВ

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы;
- деструктивные возможности.

1. По **СРЕДЕ ОБИТАНИЯ** вирусы можно разделить на:

- файловые;
- загрузочные;
- макро;
- сетевые.

Файловые вирусы либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы). На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной операционной системы: командные файлы (BAT), загружаемые драйверы (SYS, в том числе специальные файлы IO.SYS и MSDOS.SYS) и выполняемые двоичные файлы (EXE, COM). Существуют вирусы, поражающие исполняемые файлы

других операционных систем – семейство Windows 9x, на ядре Windows NT (Windows 2000, Windows XP, Windows 2003, Windows Vista, 7, 8, 8.1, 10), OS/2, MacOS.

Длиной файлового вируса считается длина тела вируса (коды+данные+стек вируса, если есть). В большинстве случаев она равна минимальному приращению длин файлов при их заражении. Выделяют следующие свойства файловых вирусов:

1) место внедрения в файл (начало, конец, середина);
2) метод заражения (использование функций FindFirst, FindNext, перехват обращений ОС к файлам и др.);
3) способ внедрения в оперативную память – для резидентных вирусов (в обычную память по фиксированному адресу, в дисковый буфер, в область данных DOS, в таблицу векторов, используя прерывания DOS int 13h, int 21h, int 27h, в видеопамять и др.
4) длина кода и др.

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. При инфицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор (или MBR) в какой-либо другой сектор диска (например, в первый свободный). «Brain», «Ping-Pong», «Stoned», «Hare», «Azusa», «March6».

Для загрузочных вирусов в качестве длины принимается полная длина тела вируса, т.е. число занимаемых вирусом секторов., умноженное на число байт в секторе.

Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макро-вирусы для Microsoft Word, Excel и остальных программ MS Office. Существуют также макро-вирусы, заражающие документы Ami Pro и базы данных Microsoft Access. Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

К **сетевым** относятся **вирусы**, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Наибольшую известность приобрели сетевые вирусы конца 1980-х, их также называют сетевыми червями (worms). К ним относятся вирус Морриса, вирусы «Cristmas Tree» и «Wank Worm&».

Существует большое количество сочетаний - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс и полиморфик-технологии. Другой пример такого сочетания - сетевой макро-вирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

2. Заражаемая **ОПЕРАЦИОННАЯ СИСТЕМА** (вернее, ОС, объекты которой подвержены заражению) является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS - DOS, Windows, Win95/NT, OS/2 и т.д. Макро-вирусы заражают файлы форматов Word, Excel, MS Office. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

3. Среди **ОСОБЕННОСТЕЙ АЛГОРИТМА РАБОТЫ** вирусов выделяются следующие пункты:

- резидентность;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.

РЕЗИДЕНТНЫЙ вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

В многозадачных операционных системах время «жизни» резидентного DOS-вируса также может быть ограничено моментом закрытия зараженного DOS-окна, а активность загрузочных вирусов в некоторых операционных системах ограничивается моментом инсталляции дисковых драйверов ОС.

Использование **СТЕЛС-алгоритмов** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ — запрет вызовов меню просмотра макросов. Один из первых файловых стелс-вирусов — вирус «Frodo», первый загрузочный стелс-вирус — «Brain».

САМОШИФРОВАНИЕ и **ПОЛИМОРФИЧНОСТЬ** используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы (polymorphic) - это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Достигается это двумя основными способами - шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса.

Различные НЕСТАНДАРТНЫЕ ПРИЕМЫ часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС (как это делает вирус «ЗАРАЗА»), защитить от обнаружения свою резидентную копию (вирусы «TPVO», «Trout2»), затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т.д.

4. По **ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ** вирусы можно разделить на:

- безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия. Ведь вирус, как и всякая программа, имеет ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков (например, вполне безобидный на первый взгляд вирус «DenZuk» довольно корректно работает с 360K дискетами, но может уничтожить информацию на дискетах большего объема). До сих пор попадаются вирусы, определяющие «COM или EXE» не по внутреннему формату файла, а по его расширению. Естественно, что при несовпадении формата и расширения имени файл после заражения оказывается неработоспособным. Возможно также «заклинивание» резидентного вируса и системы при использовании новых версий DOS, при работе в Windows или с другими мощными программными системами. И так далее.

Примечание: к "**вредным программам**", помимо вирусов, относятся также троянские кони (логические бомбы), хакерские утилиты скрытого администрирования удаленных компьютеров ("backdoor"), программы, "ворующие" пароли доступа к ресурсам Интернет и прочую конфиденциальную информацию; а также "intended" -вирусы, конструкторы вирусов и полиморфик-генераторы.

МЕТОДЫ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

- общие средства защиты информации;
- профилактические меры;
- специализированные программы;
- аппаратные средства.

Общие средства будут рассмотрены позднее в лекции по «компьютерной безопасности».

Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и утери каких-либо данных.

· Обязательно делайте регулярное резервное копирование.

· Покупайте дистрибутивные копии программного обеспечения у официальных продавцов.

· Создайте системный диск. Запишите на него антивирусные программы. Защитите диск от записи.

· Периодически сохраняйте файлы, с которыми ведется работа, на внешний носитель, например, на flash-карту или оптические диски.

· Проверяйте перед использованием все диски, особенно flash-диски. Не запускайте непроверенные файлы, в том числе полученные по компьютерным сетям.

· Ограничьте круг лиц, допущенных к работе на конкретном компьютере.

· Периодически проверяйте компьютер на наличие вирусов. При этом пользуйтесь свежими версиями антивирусных программ с актуальными антивирусными базами.

Антивирусные программы

Современные антивирусные программы представляют собой программные многофункциональные комплексы, в которые входят следующие модули:

- программа монитор;
- программа-сканер;
- обновление антивирусных баз;
- создание «аварийной» дискеты и др.

Мониторы являются резидентными модулями, обычно они помещаются в оперативную память после загрузки операционной системы, находятся в памяти во время сеанса работы и отслеживают все действия пользователя и операции, выполняемые операционной системой, с дисками и памятью. При обнаружении подозрительного файла монитор выдает сообщение. К недостаткам можно отнести значительный объем занимаемой стандартной памяти, что может замедлять работу ПК.

Сканеры запускаются в работу пользователем и позволяют выбрать область сканирования (диск, папку), и параметры сканирования. Обычно сканеры по окончании работы генерируют отчет, записываемый в текстовый файл.

Все программы обнаруживают фиксированный набор известных вирусов, содержащийся в их вирусной базе (в настоящее время (2009 г.) около 1800 тыс. известных вирусов).

Аппаратные средства

Представляют собой интерфейсные платы, устанавливаемые в каждом отдельном ПК. Обеспечиваю защиту от вируса на аппаратном уровне, поэтому конкретный вид вируса в данном случае не важен. Недостатком является высокая стоимость и невозможность работы в компьютерных сетях.

ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ ПРИ ОБНАРУЖЕНИИ ВИРУСА

1) выключить компьютер, чтобы прекратить разрушающее действие вируса;
2) загрузить ОС с эталонной системной дискеты (защищенной от записи) или загрузочного диска;
3) просканировать компьютер на наличие вируса любой имеющейся в наличии программой. Избавиться от вирусов, если возможно;
4) если избавиться не удаётся, сделать резервную копию целых файлов и отформатировать диск. Последнее действие нежелательно;

ТИПЫ ВРЕДОНОСНЫХ ПРОГРАММ ПО КЛАССИФИКАЦИИ КАСПЕРСКОГО

К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Сетевые черви

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и т. д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений.

Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

Классические компьютерные вирусы

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том

случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например бэкдор-процедуру или троянскую компоненту уничтожения информации на диске.

Троянские программы

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.