КОМПЬЮТЕРНЫЕ ВИРУСЫ

АНТИВИРУСЫ

Ученик 8 А класса
Власенко Максим

ИСТОРИЯ ПОЯВЛЕНИЯ ВИРУСОВ

- Мнений по поводу даты рождения первого компьютерного вируса очень много. Мне доподлинно известно только одно: на машине Беббиджа его не было, а на Univac 1108 и IBM-360/370 они уже были ("Pervading Animal" и "Christmas tree"). Таким образом, первый вирус появился где-то в самом начале 70-х или даже в конце 60-х годов, хотя "вирусом" его никто еще не называл.
- Поговорим о новейшей истории: "Brain", "Vienna", "Cascade" и далее. Те, кто начал работать на IBM-PC аж в середине 80-х, еще не забыли повальную эпидемию этих вирусов в 1987-89 годах. Буквы сыпались на экранах, а толпы пользователей неслись к специалистам по ремонту дисплеев (сейчас все наоборот: винчестер сдох от старости, а валят на неизвестный передовой науке вирус). Затем компьютер заиграл чужеземный гимн "Yankee Doodle", но чинить динамики уже никто не бросился - очень быстро разобрались, что это - вирус, да не один, а целый десяток.
- Так вирусы начали заражать файлы. Вирус "Brain" и скачущий по экрану шарик вируса "Ping-pong" ознаменовали победу вируса и над Boot-сектором. Все это очень< не нравилось пользователям IBM-PC, и - появились противоядия. Первым отечественным антивирусом был ANTI-KOT: это легендарный Олег Котик выпустил в свет первые версии своей программы, которая уничтожала целых 4 (четыре) вируса (американский SCAN) появился у нас в стране несколько позднее. К сожалению, ANTI-KOT определяет вирус "Time" ("Иерусалимский") по комбинации "MsDos" в конце файла, а некоторые другие антивирусы эти самые буквы аккуратно прицепляют ко всем файлам с расширением COM или EXE.
- Следует обратить внимание на то, что истории завоевания вирусами России и Запада различаются между собой. Первым вирусом, стремительно распространившимся на Западе был загрузочный вирус "Brain", и только потом появились файловые вирусы "Vienna" и "Cascade". В России же наоборот, сначала появились файловые вирусы, а годом позже - загрузочные.
- Время шло, вирусы плодились. Все они были чем-то похожи друг на друга, лезли в память, цеплялись к файлам и секторам, периодически убивали файлы, дискеты и винчестеры. Одним из первых "откровений" стал вирус "Frodo.4096" - первый из известных файловых вирусов-невидимок (стелс). Этот вирус перехватывал INT 21h и, при обращении через DOS к зараженным файлам, изменял информацию таким образом, что файл появлялся перед пользователем в незараженном виде. Но это была только надстройка вируса над MS-DOS. Не прошло и года, как электронные тараканы полезли внутрь ядра DOS (вирус-невидимка "Beast.512"). Идея невидимости продолжала приносить свой плоды и далее: летом 1991 года пронесся, кося компьютеры как бубонная чума, вирус "Dir_II".

ЧТО ТАКОЕ ВИРУС? И ИХ КЛАССИФИКАЦИЯ

- **КОМПЬЮТЕРНЫЕ ВИРУСЫ** — разновидность самовоспроизводящихся компьютерных программ , которые распространяются, внедряя себя в исполняемый код других программ или в документы специального формата, содержащие макрокоманды, такие, как WORD и EXCEL. Многие вирусы вредят данным на заражённых компьютерах, хотя иногда их единственной целью является лишь заражение как можно большего количества компьютеров.

- В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, сетевые черви), по поражаемым операционным системам и платформам (DOS,WINDOWS,UNIX, LINUX, JAVA и другие), по технологиям используемым вирусом (полиморфные вирусыВ настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, сетевые черви), по поражаемым операционным системам и платформам (DOS,WINDOWS,UNIX, LINUX, JAVA и другие), по технологиям

ПРОДОЛЖЕНИЕ

- По способу заражения файловые вирусы (вирусы, внедряющие свой код в исполняемые файлы: командные файлы, программы, драйверы, исходный код программ и др.)разделяют на: перезаписывающие;
- паразитические;
- вирусы-звенья;
- вирусы-черви;
- компаньон-вирусы;
- а так же вирусы, поражающие исходные тексты программ и компоненты программного обеспечения (VCL, LIB и др.).

Вирусы и их способ действия

Перезаписывающие вирусы

- Вирусы данного типа записывают свое тело вместо кода программы, не изменяя названия исполняемого файла, вследствие чего исходная программа перестает запускаться. При запуске программы выполняется код вируса, а не сама программа.

Вирусы-компаньоны

- Компаньон-вирусы, как и перезаписывающие вирусы, создают свою копию на месте заражаемой программы, но в отличие от перезаписываемых не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.
  Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном каталоге Windows, используя тот факт, что этот каталог является первым в списке PATH, и файлы для запуска Windows в первую очередь будет искать именно в нем. Данными способом самозапуска пользуются также многие компьютерные червиВозможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном каталоге Windows, используя тот факт, что этот каталог является первым в списке PATH, и файлы для запуска Windows в первую очередь будет искать именно в нем. Данными способом самозапуска пользуются также многие компьютерные черви и троянские программы.

Файловые черви

- Файловые черви создают собственные копии с привлекательными для пользователя названиями (например Game.exe, install.exe и др.) в надежде на то, что пользователь их запустит.

Вирусы-звенья

- Как и компаньон-вирусы, не изменяют код программы, а заставляют операционную систему выполнить собственный код, изменяя адрес местоположения на диске зараженной программы, на собственный адрес. После выполнения кода вируса управление обычно передается вызываемой пользователем программе.

Паразитические вирусы

- Паразитические вирусы — это файловые вирусы изменяющие содержимое файла добавляя в него свой код. При этом зараженная программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы. Код вируса выполняется перед, после или вместе с программой, в зависимости от места внедрения вируса в программу.

компьютеры пользователей для рассылки спамаСейчас основной канал распространения вирусов — электронная почта. Хакеры и спамеры используют зараженные компьютеры

пользователей для рассылки спама или DDoS-атак.

- BRAIN ВИРУСЫ-Первая эпидемия 1987 была вызвана вирусом Brain (также известен как Пакистанский вирус), который был разработан братьями Амджатом и Базитом Алви (Amdjat и Basit Faroog Alvi) в 1986 и был обнаружен летом 1987. По данным **McAfee**, вирус заразил только в США более 18 тысяч компьютеров. Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев. Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру. Вирус Brain являлся также и первым стелс-вирусом — при попытке чтения зараженного сектора он «подставлял» его незараженный оригинал.
- Вторая эпидемия, берущая начало в Лехайском университете (США), разразилась в ноябре 1987. В течение нескольких дней этот вирус уничтожил содержимое нескольких сот дискет из библиотеки вычислительного центра университета и личных дискет студентов. За время эпидемии вирусом было заражено около четырех тысяч компьютеров.
- Последняя вирусная эпидемия разразилась перед самым Новым годом, 30 декабряПоследняя вирусная эпидемия разразилась перед самым Новым годом, 30 декабря 1987Последняя вирусная эпидемия разразилась перед самым Новым годом, 30 декабря 1987. Её вызвал вирус, обнаруженный в Иерусалимском Университете (Израиль). Хотя существенного вреда этот вирус не принес, он быстро распространился по всему миру.
- В пятницу 13 мая 1988 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.

Червь Морриса

- В 1988В 1988 Робертом Моррисом-младшим был создан первый массовый сетевой червь. 60000-байтная программа, разрабатывалась с расчётом на поражение операционных систем UNIXВ 1988 Робертом Моррисом-младшим был создан первый массовый сетевой червь. 60000-байтная программа, разрабатывалась с расчётом на поражение операционных систем UNIX Berkeley 4.3, SUN. Вирус изначально разрабатывался как безвредный и имел целью лишь скрытно проникнуть в вычислительные системы, связанные сетью ARPANET и остаться там необнаруженным. Вирусная программа включала компоненты, позволяющие раскрывать пароли, существующие в инфицируемой системе, что, в свою очередь, позволяло программе маскироваться под задачу легальных пользователей системы, на самом деле занимаясь размножением и рассылкой копий. Вирус не остался скрытым и полностью безопасным, как задумывал автор, в силу незначительных ошибок, допущенных при разработке, которые привели к стремительному неуправляемому саморазмножению вируса.
- По самым скромным оценкам инцидент с червём Морриса стоил свыше 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая стоимость этих затрат оценивается в 96 миллионов долларов (в эту сумму, также, не совсем обосновано, включены затраты по доработке операционной системы). Ущерб был бы гораздо больше, если бы вирус изначально создавался с разрушительными целями.
- Червь Морриса поразил свыше 6200 компьютеров. В результате вирусной атаки большинство сетей вышло из строя на срок до пяти суток. Компьютеры, выполнявшие коммутационные функции, работавшие в качестве файл-серверов или выполнявшие другие функции обеспечения работы сети, также вышли из строя. 4 маяЧервь Морриса поразил свыше 6200 компьютеров. В результате вирусной атаки большинство сетей вышло из строя на срок до пяти суток. Компьютеры, выполнявшие коммутационные функции,

DATACRIME и «AIDS»

- В 1989 широкое распространение получили вирусы DATACRIME, которые начиная с 12 октября разрушали файловую систему, а до этой даты просто размножались. Эта серия компьютерных вирусов начала распространяться в Нидерландах, США и Японии в начале 1989 г. и к сентябрю поразила около 100 тысяч ПЭВМ только в Нидерландах (что составило около 10 % от их общего количества в стране). Даже фирма IBM отреагировала на эту угрозу, выпустив свой детектор VIRSCAN, позволяющий искать характерные для того или иного вируса строки (сигнатуры) в файловой системе. Набор сигнатур мог дополняться и изменяться пользователем.
- В 1989 году появился первый «троянский конь» AIDS. Вирус делал недоступными всю информацию на жестком диске и высвечивал на экране лишь одну надпись: «Пришлите чек на $189 на такой-то адрес». Автор программы был арестован в момент обналичивания чека и осужден за вымогательство. Также был создан первый вирус, противодействующий антивирусному программному обеспечению — The Dark Avenger. Он заражал новые файлы, пока антивирусная программа проверяла жесткий диск компьютера.

АНТИВИРУСЫ

- СЕЙЧАС СУЩЕСТВУЕТ БОЛЕЕ ДЕСЯТКА АНТИВИРУСОВ ТАКИХ КАК:NORTON,КАСПЕРСКИЙ,AVG,Dr Web И Т.Д
- ОНИ ПУТЁМ СКАНИРОВАНИЯ СИСТЕМЫ НАХОДЯТ НЕПОНЯТНЫЕ ВИРУСЫ ИЛИ ПОДОЗРИТЕЛЬНЫЕ ПРОГРАММЫ.А ПОСЛЕ С РАЗРЕШЕНИЯ ПОЛЬЗОВАТЕЛЯ УНИЧТОЖАЮТ ИХ.