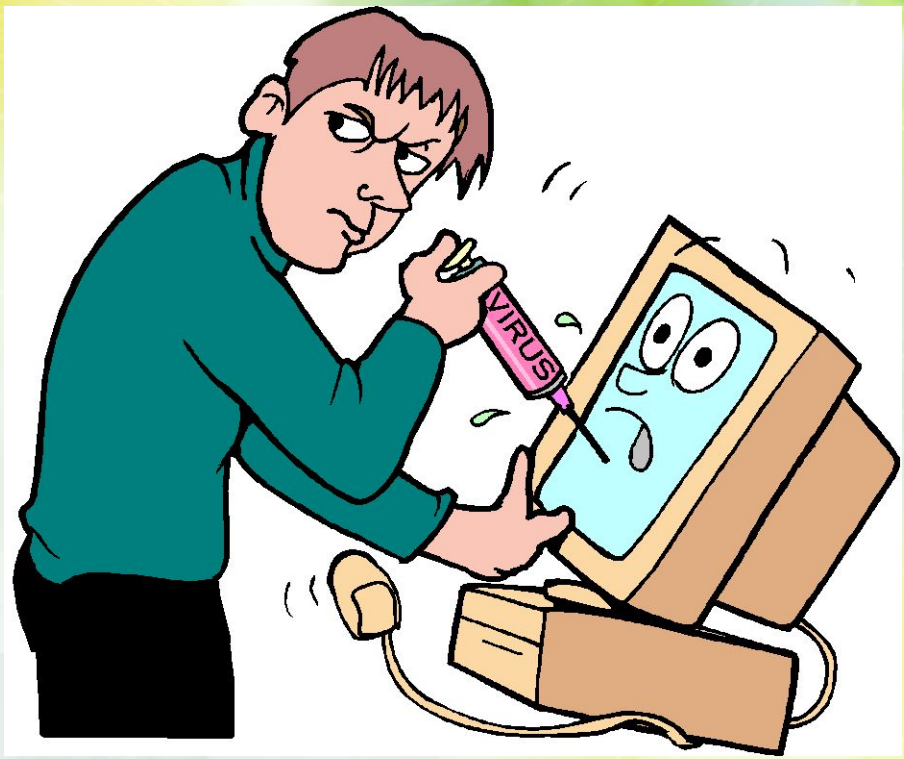
ГБОУ СПО №36 КДПИ им. К. Фаберже

Операционные системы и среды

История развития компьютерных вирусов

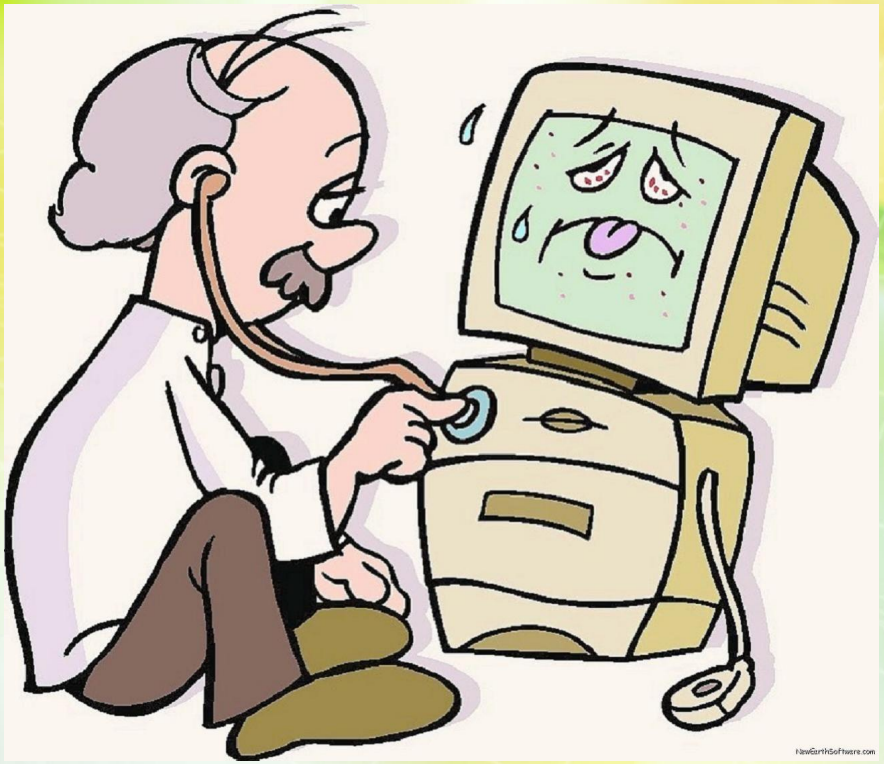
История появления и эволюции компьютерных вирусов, сетевых червей, троянских программ зародилась в 1980-х годах. Примитивные вирусы постепенно превращались в сложные технологические разработки, осваивали новые ниши, проникали в компьютерные сети. Идея вируса, заражающего другие программы и компьютеры, за двадцать лет трансформировалась в криминальный бизнес.

Будучи изначально творчеством вирусописателей-исследователей, компьютерные вирусы стали оружием в руках интернет-преступников.



Одновременно происходило зарождение и становление индустрии антивирусной.

Появившись в конце 1980-х, первые антивирусные разработки получили большую популярность, через 10 лет став обязательным к использованию программным обеспечением.



Этапы развития

Вирусы 1970-1975х годов

В начале 1970-х годов в прототипе современного интернета — военной компьютерной сети APRANET — был обнаружен вирус Creeper, который перемещался по серверам под управлением операционной системы Tenex.

Creeper был в состоянии самостоятельно войти в сеть через модем и передать свою копию удаленной системе. На зараженных системах вирус обнаруживал себя сообщением: «I'M THE CREEPER : CATCH ME IF YOU CAN», которое выводилось на дисплей или на принтер.

Для удаления вируса была написана первая антивирусная программа Reeper, которая аналогичным образом распространялась по сети, удаляла обнаруженные копии Creeper и затем самоликвидировалась.

Другие компьютерные легенды гласят, что также в начале 1970-х на мейнфреймах этого времени появляется программа, получившая название «Кролик» (Rabbit). Эта программа клонировала себя, занимала системные ресурсы и таким образом снижала производительность системы. Достигнув определенного уровня распространения на зараженной машине «Кролик» нередко вызывал сбой в её работе.

Скорее всего «Кролики» не передавались от системы к системе и являлись сугубо местными явлениями — ошибками или шалостями системных программистов, обслуживавших компьютер.

Другой инцидент произошел на системе Univac 1108 с игрой Pervading Animal. При помощи наводящих вопросов игра пыталась определить имя животного, задуманного играющим. В программе была предусмотрена возможность самообучения: если ей не удавалось отгадать задуманное человеком название, игра предлагала модернизировать себя и ввести дополнительные наводящие вопросы.

Модифицированная игра записывалась поверх старой версии, а также копировалась и в другие директории — для того, чтобы сделать результат работы доступным и другим пользователям. В результате, через некоторое время все директории на диске содержали копии Pervading

В те времена такое поведение программы вряд ли могло понравиться инженерам и менеджерам компаний, и через некоторое время был запущена «программа-охотник» (Hunter).

Это была новая версия игры, целью которой было заменить все копии своей предшественницы, а затем удалить и себя саму.

Однако позднее все решилось гораздо проще: для компьютеров Univac была выпущена новая версия операционной системы, в которой изменениям подверглась структура файловой системы, и игра потеряла возможность размножаться.

Вирусы 1980-1986х годов

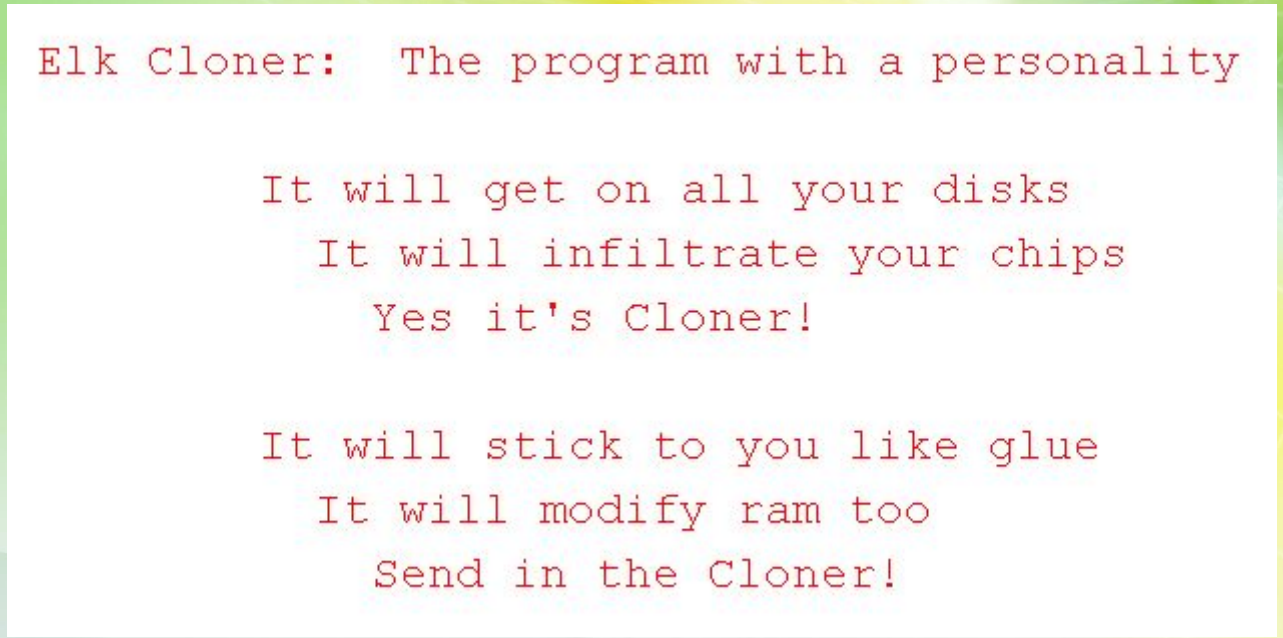
Компьютеры становятся всё более и более популярными. Появляется всё больше и больше программ, авторами которых являются не фирмы-производители программного обеспечения, а частные лица. Развитие телекоммуникационных технологий даёт возможность относительно быстро и удобно распространять эти программы через серверы общего доступа BBS (Bulletin Board System).

«Глобальная сеть» серверов BBS становится популярной и в результате привлекает внимание программистов-хулиганов. Появляется большое количество разнообразных «троянских коней» — программ, не имеющих способности к размножению, но при запуске наносящих системе какой-либо вред.

Apple II, разработанный в 1977, стал одним из наиболее успешных персональных компьютеров того времени.

В результате своей массовости он стал жертвой первого документально зафиксированного компьютерного вируса — некто Richard Skrenta, один из миллионов пользователей Apple II, догадался разработать для этого компьютера саморазмножающуюся программу-вирус.

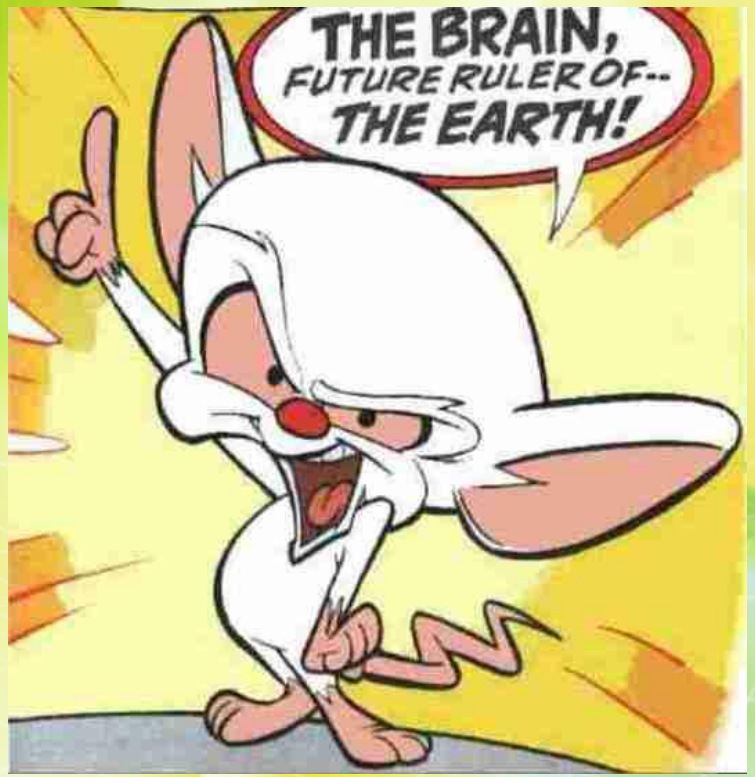
Вирус, получивший название Elk Cloner, записывался в загрузочные секторы дискет, к которым обращалась ОС компьютера. Проявлял себя вирус весьма многосторонне: переворачивал изображение на экране, заставлял мигать текст, выводил сообщение:



Фред Коэн, родоначальник компьютерной вирусологии того времени, на семинаре по компьютерной безопасности в Лехайском университете (США) демонстрирует на системе VAX 11/750 вирусоподобную программу, способную внедряться в другие объекты.

Годом позже, на 7-й конференции по безопасности информации, он дает научное определение термину «компьютерный вирус» как программе, способной «заражать» другие программы при помощи их модификации с целью внедрения своих копий.

Зарегистрирована первая глобальная эпидемия вируса для IBM-совместимых персональных компьютеров. Вирус Brain, заражающий загрузочные сектора дискет, в течение нескольких месяцев распространился практически по всему миру.



Причина такого «успеха» заключалась в полной неподготовленности компьютерного общества к встрече с таким явлением, как компьютерный вирус: антивирусных программ просто не было, а пользователи, в свою очередь, ничего не знали о новом компьютерном бедствии.

Вирус Brain был написан в Пакистане 19-летним программистом Баситом Фаруком Алви (Basit Farooq Alvi) и его братом Амжадом (Amjad).

Они оставили в вирусе текстовое сообщение, содержащее их имена, адрес и телефонный номер. Помимо заражения загрузочных секторов и изменения меток дискет на фразу «(c) Brain» вирус ничего не делал: он не оказывал никакого побочного воздействия и не портил информацию.

Вирус Brain являлся также и первым «вирусом-невидимкой». При обнаружении попытки чтения зараженного сектора диска вирус незаметно подставлял его незараженный оригинал.

В том же году немецкий программист Ральф Бюргер (Ralf Burger) открыл возможность создания программой своих копий путем добавления своего кода к исполняемым MS-DOS-файлам формата COM.

Опытный образец программы, получившей название Virdem и имевшей такую способность, был представлен Бюргером в декабре 1986, в Гамбурге, на форуме компьютерного андеграунда Chaos Computer Club, который в то время собирал хакеров, специализировавшихся на взломе VAX/VMS-систем.

Вирусы 1999 года

В январе разразилась глобальная эпидемия почтового интернет-червя Happy99 (также известного как Ska). По сути, это был первый современный червь, открывший новый этап в развитии вредоносных программ. Он использовал для своего распространения программу MS Outlook, являющуюся корпоративным стандартом в США и во многих странах Европы.

26 марта: глобальная эпидемия почтового червя Melissa — первого макро-вируса для MS Word, сочетавшего в себе также и функциональность интернет-червя. Сразу же после заражения системы он считывал адресную книгу почтовой программы MS Outlook и рассылал свои копии по первым 50 найденным адресам. В автоматизированных системах документооборота письма с червём обрабатывались без участия человека — в результате эпидемия Melissa моментально достигла своего пика и нанесла ощутимый ущерб компьютерным системам мира: такие гиганты индустрии, как Microsoft, Intel, Lockheed Martin были вынуждены временно отключить свои корпоративные службы электронной поч

Вирусы 2005 года

Тенденции второй половины 2004 года сохранились и в последующих 2005 и 2006 годах. «Громких» инцидентов практически не происходит, но зато двукратно растёт число разнообразных троянских программ, которые распространяются самыми разными способами: через интернет-пейджеры, веб-сайты, при помощи сетевых червей или традиционной электронной почты. При этом растёт «популярность» именно сетевых не-почтовых червей, которые проникают на компьютеры, используя различные дыры в программном обеспечении. Продолжали появляться новые вирусы и троянские программы для мобильных платформ, особенно часто — для операционной системы Symbian.

Происходят изменения и в антивирусной индустрии. Корпорация Microsoft активно готовится к выходу на антивирусный рынок и покупает сразу две антивирусные компании. 8 февраля 2005 объявляет о покупке компании Sybari, а 20 июля объявлено о покупке FrontBridge Technologies

Спасибо за внимание