**1. История вредоносных программ**

Мнений по поводу рождения первого компьютерного вируса очень много. Точно известно только одно: на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, вирусов не было, а на Univax 1108 и IBM 360/370 в середине 1970-х годов они уже были.

Несмотря на это, сама идея компьютерных вирусов появилась значительно раньше. Отправной точкой можно считать труды Джона фон Неймана по изучению самовоспроизводящихся математических автоматов. Эти труды стали известны в 1940-х годах. А в 1951 г. знаменитый ученый предложил метод, который демонстрировал возможность создания таких автоматов. Позднее, в 1959 г., журнал "Scientific American" опубликовал статью Л.С. Пенроуза, которая также была посвящена самовоспроизводящимся механическим структурам. В отличие от ранее известных работ, здесь была описана простейшая двумерная модель подобных структур, способных к активации, размножению, мутациям, захвату. Позднее, по следам этой статьи другой ученый - Ф.Ж. Шталь - реализовал модель на практике с помощью машинного кода на IBM 650.

Необходимо отметить, что с самого начала эти исследования были направлены отнюдь не на создание теоретической основы для будущего развития компьютерных вирусов. Наоборот, ученые стремились усовершенствовать мир, сделать его более приспособленным для жизни человека. Ведь именно эти труды легли в основу многих более поздних работ по робототехнике и искусственному интеллекту. И в том, что последующие поколения злоупотребили плодами технического прогресса, нет вины этих замечательных ученых.

 В 1962 г. инженеры из американской компании Bell Telephone Laboratories - В.А. Высотский, Г.Д. Макилрой и Роберт Моррис - создали игру "Дарвин". Игра предполагала присутствие в памяти вычислительной машины так называемого супервизора, определявшего правила и порядок борьбы между собой программ-соперников, создававшихся игроками. Программы имели функции исследования пространства, размножения и уничтожения. Смысл игры заключался в удалении всех копий программы противника и захвате поля битвы.

 На этом теоретические исследования ученых и безобидные упражнения инженеров ушли в тень, и совсем скоро мир узнал, что теория саморазмножающихся структур с не меньшим успехом может быть применена и в несколько иных целях.

### 2. Первые вирусные эпидемии

К 1987 году получили широкое распространение сравнительно дешевые компьютеры IBM PC, что привело к резкому увеличению масштаба заражения компьютерными вирусами. Именно в 1987 вспыхнули крупные эпидемии компьютерных вирусов.

#### Brain

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 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 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. 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 мая 1990 г. суд присяжных признал Морриса виновным. Он был приговорен к условному заключению сроком на два года, 400 часам общественных работ и штрафу размером 10 тыс. долларов.

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.