



Вирусные эпидемии.

Самый первый массовый вирус.



Brain - Разработанный Братьями Алви из Пакистана в 1986 году. Молодые программисты открыли собственную фирму по разработке ПО, однако конкуренты бесконечно воровали их наработки через незащищенную сеть. Тогда братья решили написать простую программу: при попытке украсть информацию с их компьютеров, операционная система злоумышленников заражалась тем самым Brain. Он не мешал работе с устройством, однако уничтожал всю информацию на флоппи-дискетах, которые вставляли в считыватель зараженного компьютера. При запуске ОС на экране выводилась контактная информация молодых людей – адрес и телефоны.

На тот случай,
если кто то не
знает что такое
флоппи-
дискета

```

PC Tools Deluxe V6.22      Disk View/Edit Service
Path=A:
      Absolute sector 0000000, System BOOT

Displacement  Hex codes  ASCII value
0000(0000)  FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20  -0J04; 01 0
0016(0010)  20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F  Welcome to
0032(0020)  20 74 69 65 20 44 75 6E 67 65 6F 6E 20 20 20 20  the Dungeon
0048(0030)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050)  20 28 63 23 20 31 39 38 36 20 42 51 73 69 74 20  (c) 1986 Basit
0096(0060)  26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74  & Amjad (put) Lt
0112(0070)  64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20  d.
0128(0080)  20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20  BRAIN COMPUTER
0144(0090)  53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49  SERVICES..730 NI
0160(00A0)  5A 41 43 20 42 4C 4F 43 48 20 41 4C 4C 41 4D 41  2AM BLOCY ALLAMA
0176(00B0)  20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20  TGBAL TOWN
0192(00C0)  20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52  LANOB
0208(00D0)  45 2D 50 41 48 49 53 54 41 4E 2E 2E 50 48 4F 4E  E-PAKISTAN..PHON
0224(00E0)  45 2D 30 34 33 30 37 39 31 2C 34 34 33 32 34 38  E :430791,443249
0240(00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20  ,288530.

Home=begin of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name

```

Вирус, предназначенный для одного маленького города в Пакистане, внезапно вышел за пределы страны. В 1987 году он заразил 18 тыс. компьютеров в США.

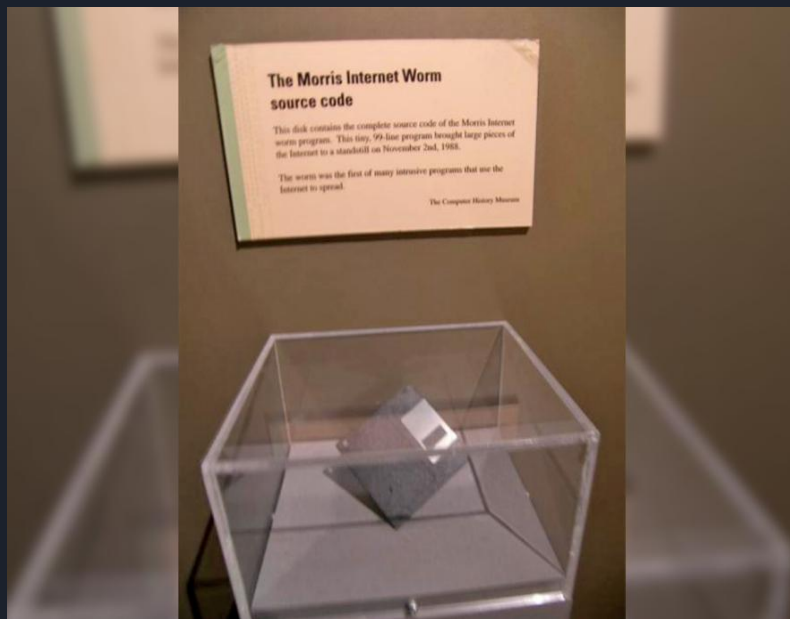
Больше всего пострадал Лехайский университет – там было уничтожено содержимое нескольких сотен дискет с важной информацией.



Сетевой червь Морриса.

1988 год стал знаковым для развития IT-индустрии. Был запущен первый сетевой вирус – **Morris worm**. Его в «локалку» Массачусетского технологического института загрузил студент Роберт Моррис. Однако быстро программа вышла из под контроля – в первый же день она поразила более шести тысяч узлов ARPANET (тогдашнего аналога Интернета), через неделю червем был забит весь сетевой трафик.

Вирус подбирал пароли к различным сервисам пользователей сети, забивал их оперативную память бесполезными процессами, которые ветвились каждые три секунды, и попросту выводил компьютеры из строя. Быстро справиться с червем не смогли даже лучшие компьютерные эксперты страны. В результате сумма ущерба составила почти \$100 млн.



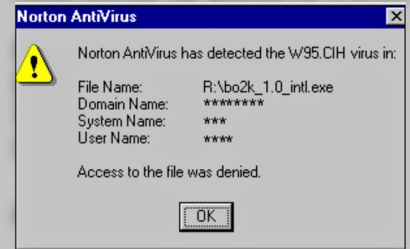
Спецслужбы США не смогли сразу отыскать Морриса, и вряд ли бы у них это получилось, если бы отец автора вируса не работал в Агентстве национальной безопасности. Моррис-старший узнал о том, что в атаке, о которой говорит вся Америка, виноват его сын и попросил Роберта сдаться полиции. На суде злоумышленника осудили на 3 года условно, \$10 тыс. штрафа и несколько сотен часов общественных работ. Это был первый в истории приговор за киберпреступление. Кстати, дискета Морриса с исходным кодом программы до сих пор хранится в музее науки в Бостоне как один из главных экспонатов.

Тайваньский Чернобыль.

22-летнему Чэню Инхао из Тайваня было довольно скучно учиться в университете Датун в Тайбэе. Он существенно опережал программу, поэтому пока его однокурсники делали домашние задания, Чэнь писал короткие коды, ставя себе различные задачи. Так в 1998 году появился вирус **СИН** – по инициалам создателя. Это безобидная на первый взгляд программа весом 1 килобайт при запуске не производила никаких манипуляций с ОС, лишь закладывая небольшую «логическую бомбу». 26 апреля (годовщина взрыва на **АЭС в Чернобыле**, отсюда второе название) все зараженные системы Windows 95/98 уничтожали данные с жестких дисков и повреждали содержимое микросхем BIOS, что делало компьютер непригодным для использования.

По разным оценкам, вирус, который Чэнь хотел запустить лишь в своем университете, достиг 500 тыс. компьютеров по всему миру, включая Россию. Распространялся он, в основном, за счет веб-серверов с компьютерными играми. Китаец получил серьезный выговор от университета, но не попал в тюрьму – в законодательстве Тайваня не было статей о киберпреступлениях.

Вирус «Чернобыль» можно встретить и до сих пор. У него немного изменилась оболочка, но код все еще срабатывает именно 26 апреля.

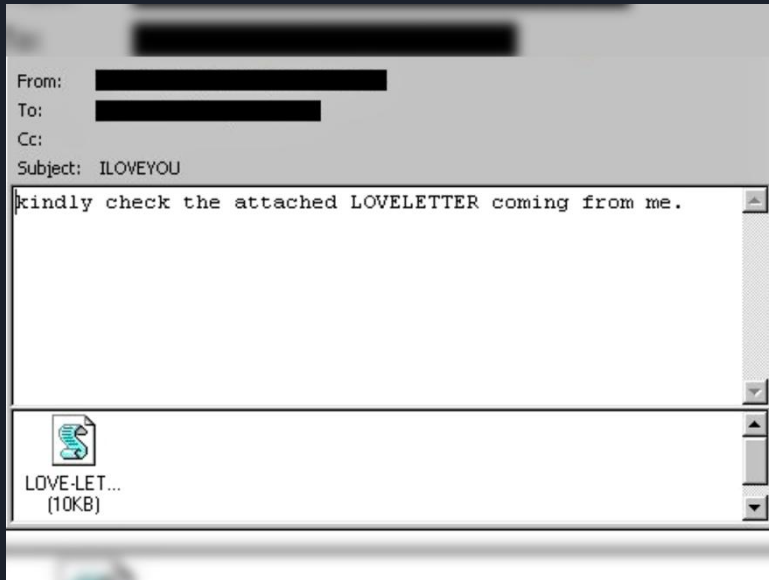




Мелисса.Вирус-любовник.

1999 год ознаменовался первой масштабной волной заражения через почтовые сервисы и спам-рассылку. Вирус **Melissa** затронул не только обычных пользователей, но и многих компьютерных гигантов, таких как Intel и Microsoft. Изначально вирус от имени некой Мелиссы присылал странный файл с подписью «очень важная информация». При открытии приложения компьютер заражался, и рассылка шла уже от его имени. Большинство пользователей без раздумий открывали приложения от своих родственников и коллег, таким образом становясь еще одним звеном в цепочке распространения вредоносного ПО. Ущерб составил около \$100 млн.

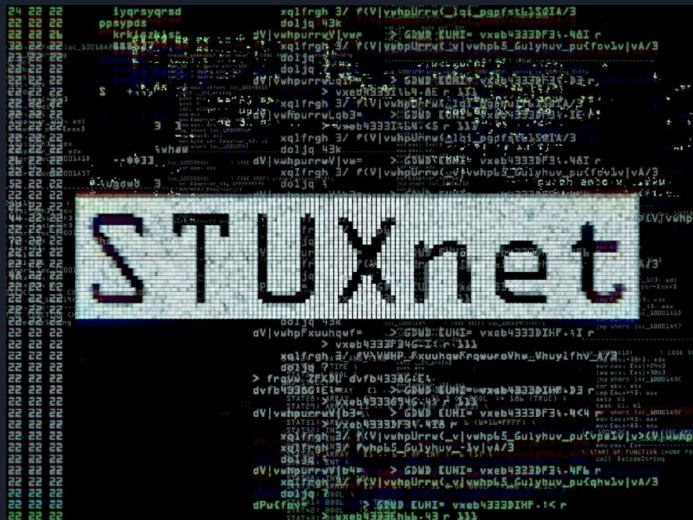
Продолжение эпопеи с почтовыми вирусами не заставило себя ждать. Уже в 2000 году злоумышленники создали похожую программу, которая на этот раз играла на эмоциях людей. От имени коллег и родственников вирус отправлял сообщение «I love you» и приложение – love-letter, которое и заражало компьютер. Дальше все происходило по схеме Melissa. Эпидемия **Iloveyou** стала одной из самых массовых в истории – заражено было 10% от всех имевшихся на тот момент на планете компьютеров. Ущерб от украденных паролей составил \$5,5 млрд. Создатели – филиппинцы Ренел Рамонс и Онел де Гузман – также не понесли наказания за свои действия, ведь в их стране законодательством не предусмотрены наказания за распространение вирусов.



Вирус как оружие



В 2010 году мировую общественность поразила находка эксперта по информационной безопасности из Беларуси Сергея Уласеня. Он обнаружил вирус, который способен не только заражать операционные системы, но и внедряться в промышленные аппараты, установленные на производствах, в аэропортах, на электростанциях. На зараженной этим вирусом АЭС, например, могла выйти из строя система охлаждения, что неминуемо привело бы к взрыву. Вирус назывался «**Win32/Stuxnet**» и был классифицирован как «боевой», то есть применяемый для шпионажа и диверсий.



Программа вызвала ряд международных скандалов. Страны поочередно обвиняли друг друга в распространении вируса. Одна из многих теорий: это сделали спецслужбы Израиля, чтобы подорвать ядерную промышленность Ирана. Согласно другой, во всем виноват президент США Барак Обама и АНБ. Распространяется ПО через флеш-накопители и запускается автоматически. По большинству стран мира на оборонных и промышленных предприятиях прошла лекция по компьютерной безопасности для сотрудников: флешки извне не приносить, личные устройства в рабочие компьютеры не вставлять.

Хочется Плакать



Хакерская атака программой **WannaCry** началась 12 мая и уже успела поразить, по разным данным, от 200 до 300 тысяч компьютеров в 150 странах. Код, написанный злоумышленниками, находит уязвимость в операционной системе Windows, шифрует все данные на компьютере, а за разблокировку просит «выкуп» – около \$500.

До сих пор достоверно неизвестно, кто стоит за этой программой: спецслужбы США, агенты КНДР или пресловутые российские хакеры. Однако это далеко не первая поистине масштабная эпидемия компьютерного вируса в истории человечества. «МИР 24» собрал самые известные примеры киберугрозы.



Список использованных ресурсов:

<https://mir24.tv>

wikipedia



СПАСИБО

ЗА

ВНИМАНИЕ