Компьютерные вирусы

Кукота Анастасия **1/1**л

Предвидение вирусов

.
Термин «компьютерный вирус» был впервые использован в 1973 году в фантастическом фильме Westworld.

Сейчас существуют, навреное, миллионы вирусов, распространяющихся через интернет всякими путями – файловые раздачи, e-mail, сайты. Когда всё связано со всем, вирусы распространяются быстро.
А вот начиналось это довольно медленно - первые вирусы распространялись с дискетами и переносились на них между компьютерами.

С чего всё началось

В 1987 году появился первый вирус, который заражал IBM PC-совместимые компьютеры под управлением MS-DOS, — Brain. Вирус должен был «наказать» местных «пиратов», ворующих ПО у их фирмы. В программе значились имена, адреса и телефоны братьев. Однако неожиданно для всех Brain вышел за пределы Пакистана и заразил тысячи компьютеров по всему миру.
В том же году появился вирус Jerusalem, запрограммированный на удаление зараженных файлов по пятницам 13-го.

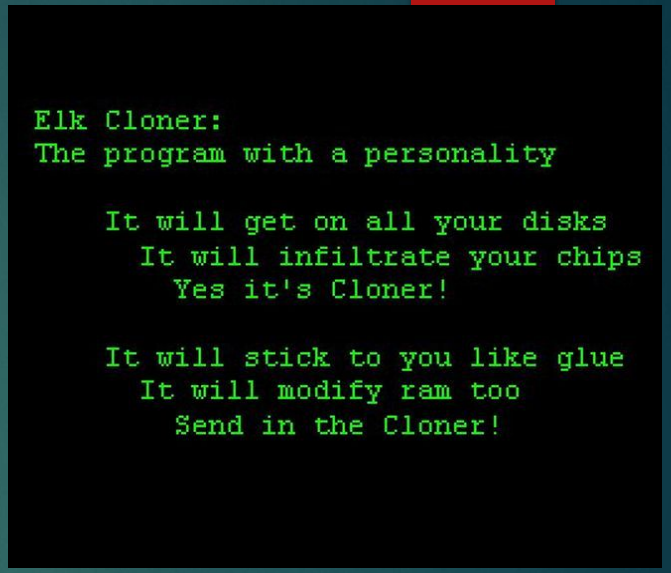
2 ноября 1988 года, студент Корнельского университета Роберт Моррис запустил программу-червь, которая сохранилась в истории под именем своего разработчика. Червь Морриса стал первым сетевым червем, успешно распространившимся и одной из первых известных программ, эксплуатирующих такую уязвимость, как переполнение буфера. За каких-то полтора часа ему удалось заразить около 6 тыс. машин.

В 1989 году создано антивирусное программное обеспечение для IBM PC. В этом же году появился первый вирус типа «троянский конь» — AIDS и стала более популярна услуга ремонт компьютеров на дому. Вирус делал недоступной всю информацию на жестком диске компьютера и высвечивал на экране лишь одну надпись: «Пришлите чек на 189 долл. на ??? адрес :))». Автор программы был осужден за вымогательство.

В 1990 году компьютерный журнал PC Today разослал подписчикам зараженную дискету. Вирус называемый AIDS Information Trojan- троянская программа, распространявшейся в составе пакета с базой данных о заболевании синдромом приобретенного иммунодефицита (СПИД). Как программа, так и база данных были записаны на дискете, которая были разослана 20 тысячам подписчиков. После записи на винчестер она действительно начала выдавать информацию по обещанной тематике. Однако затем (после 90 загрузок системы) троянец шифровал имена всех файлов на диске, делал их невидимыми и оставлял на диске всего один читаемый файл - требование перечислить сумму в 378 долларов на счет некоей фирмы в Панаме. В этом случае пользователю якобы будет выслана программа, которая произведёт удаление вирусов с компьютера. Джозеф Попп - автор "троянца", был пойман и приговорен к тюремному заключению.

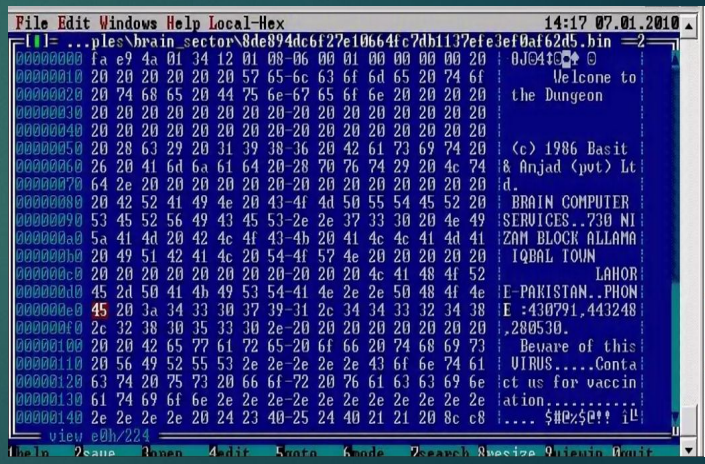
Самые известные

ELK CLONER
В 1981 году Ричард Скрента написал один из первых загрузочных вирусов для ПЭВМ Apple II — ELK CLONER.[4] Он обнаруживал своё присутствие сообщением, содержащим небольшое стихотворение. Из-за отсрочки появления программу сразу нельзя было заметить, что улучшало шансы на распространение. Программа добралась и до компьютера учителя, обвинившего его в проникновении к нему в кабинет. Эпидемия продолжалась несколько недель.



Вирус загрузочного сектора Brain

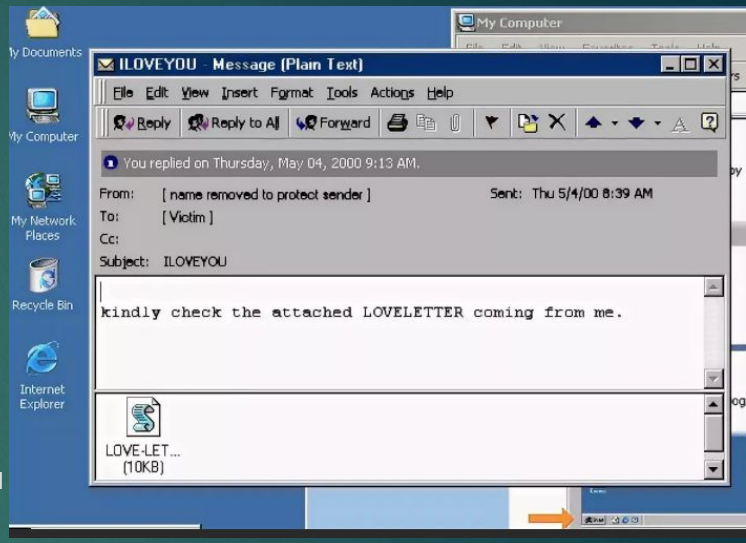
Brain, первый вирус для IBM-совместимых компьютеров, появился в 1986 году – он заражал пятидюймовые дискеты. Как сообщает Securelist, вирус был написан двумя братьями – Баситом и Амджадом Фаруком Алви, которые держали компьютерный магазин в Пакистане. Братьям надоело, что покупатели нелегально копировали купленное у них ПО, и они создали этот вирус, которые заражал загрузочные сектора дискет. Brain заодно оказался и первым вирусом-невидимкой: при обнаружении попытки чтения зараженного сектора диска вирус незаметно подставлял его незараженный оригинал. Также он записывал на дискету фразу «(c) Brain», но при этом не портил никаких данных.



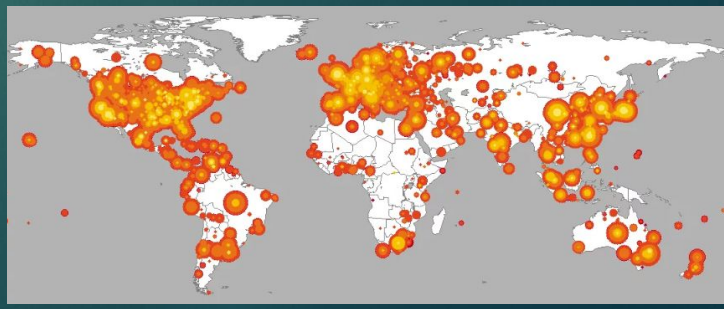
Самые известные

Вирус ILoveYou

В начале 21 века появился надежный высокоскоростной интернет-доступ, и это изменило методы распространения вредоносных программ. Теперь они не были ограничены дискетами и могли очень быстро распространяться через электронную почту. Одна из самых серьезных эпидемий новой эры была вызвана червем ILoveYou, который появился 4 мая 2000 г.



Червь Code
Червь Code Red был так называемым бестелесным червем – он существовал только в памяти и не предпринимал попыток заразить файлы в системе. Используя брешь в системе безопасности Microsoft Internet Information Server, в 2011 году червь всего за несколько часов распространился по всему миру и вызвал хаос, внедряясь в протоколы обмена информацией между компьютерами.
Зараженные компьютеры в итоге были использованы для проведения атаки на веб-сайт Белого дома США.



Глобализация вирусов

Начиная с 1990 года проблема вирусов начинает принимать глобальный размах.
Во второй половине 1990 года появились два стелс-вируса — Frodo и Whale. Оба вируса использовали крайне сложные стелс-алгоритмы, и к тому же применял несколько уровней шифровки и антиотладочных приёмов.

Начинают открываться конференции по вопросам написания вирусов, на проблему противостояния вирусам были вынуждены обратить внимание крупные компании.
1992 год известен как год появления первых конструкторов вирусов для PC — VCL (для Amiga конструкторы существовали и ранее), а также готовых полиморфных модулей (MtE, DAME и TPE) и модулей шифрования. Начиная с этого момента, каждый программист мог легко добавить функции шифрования к своему вирусу.

В 1993 году появляется всё больше вирусов, использующих необычные способы заражения файлов, проникновения в систему и т. д.
Выходят новые версии вирусных генераторов, а также появляются новые (PC-MPC и G2). Счёт известных вирусов уже идёт на тысячи. Антивирусные компании разрабатывают ряд эффективных алгоритмов для борьбы с полиморфными вирусами, однако сталкиваются с проблемой ложных срабатываний.

Весной 1994 был обнаружено SrcVir, семейство вирусов, заражающих исходные тексты программ (C и Pascal). В июне 1994 года началась эпидемия OneHalf.
В 1995 году появляется несколько достаточно сложных вирусов (NightFall, Nostradamus, Nutcracker). Появляются первый «двуполый» вирус RMNS и BAT-вирус Winstart. Широкое распространение получили вирусы ByWay и DieHard2 — сообщения о заражённых компьютерах были получены практически со всего мира. В феврале 1995 года случился инцидент с beta-версией Windows 95, все диски которой оказались заражены DOS-вирусом Form.

Будущее вирусов

На протяжении уже более 60 лет компьютерные вирусы находятся в сфере коллективного человеческого сознания. То, что однажды было лишь кибер-вандализмом и кибер-хулиганством, быстро превратилось в киберпреступление.

Быстро развиваются черви, троянцы и вирусы. Хакеры мотивированы и умны, они всегда стремятся тестировать на прочность системы и код, расширять границы доступных им методов и изобретать новые способы заражения.

В будущем киберпреступники, вероятно, будут чаще взламывать личные данные, базы данных крупных компаний и терминалы. Эти вирусы будет сложно обнаружить, тяжело удалить – они будут обходить все известные механизмы защиты.