Эволюция компьютерного вируса

...

Проектная работа Артемьева Александра 9Б по информатике

Цель работы:

1.Первые самовоспроизводящиеся программы.

2.ELK CLONER.

3. Brain и Jerusalem.

4. DATACRIME и AIDS.

5. Глобализация проблемы вирусов.

6.Кибероружие и кибершпионские программы.

7. Как бороться с вирусами на компьютере.

Первые самовоспроизводящиеся программы

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения **Джон фон Нейман**, который в 1951 году предложил метод создания таких механизмов. Первой публикацией, посвящённой созданию самовоспроизводящихся систем, является статья Л. С. Пенроуз в соавторстве со своим отцом, нобелевским лауреатом по физике Р. Пенроузом, о самовоспроизводящихся механических структурах, опубликованная в 1957 году американским журналом Nature.[1] В этой статье, наряду с примерами чисто механических конструкций, была приведена некая двумерная модель подобных структур, способных к активации, захвату и освобождению. По материалам этой статьи Ф. Ж. Шталь (F. G. Stahl) запрограммировал на машинном языке ЭВМ IBM 650 биокибернетическую модель, в которой существа двигались, питаясь ненулевыми словами. При поедании некоторого числа символов существо размножалось, причём дочерние механизмы могли мутировать. Если кибернетическое существо двигалось определённое время без питания, оно погибало.

ELK CLONER

В 1981 году Ричард Скрента написал один из первых загрузочных вирусов для ПЭВМ Apple II — ELK CLONER. Он обнаруживал своё присутствие сообщением, содержащим небольшое стихотворение:
ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS

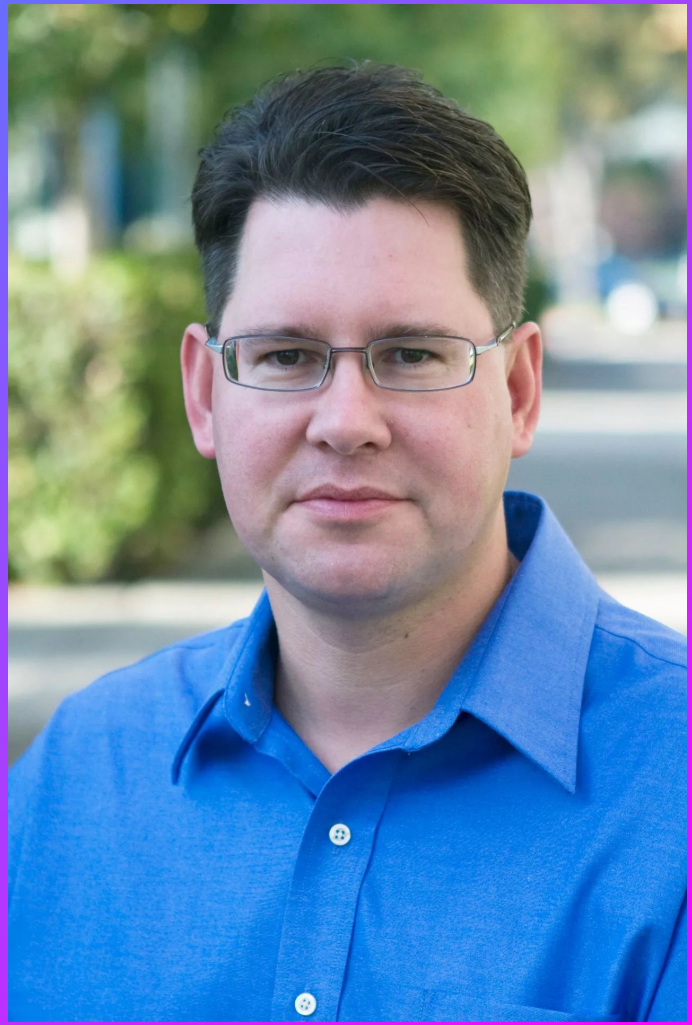
IT WILL INFILTRATE YOUR CHIPS

YES, IT'S CLONER

IT WILL STICK TO YOU LIKE GLUE

IT WILL MODIFY RAM, TOO

SEND IN THE CLONER!



Brain и Jerusalem

Первая эпидемия 1987 года была вызвана вирусом Brain (от англ."мозг"), который был разработан братьями Амджатом и Базитом Алви 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 тысячи компьютеров по всему миру. Вирус Brain являлся также и первым стелс-вирусом — при попытке чтения заражённого сектора он «подставлял» его незаражённый оригинал.

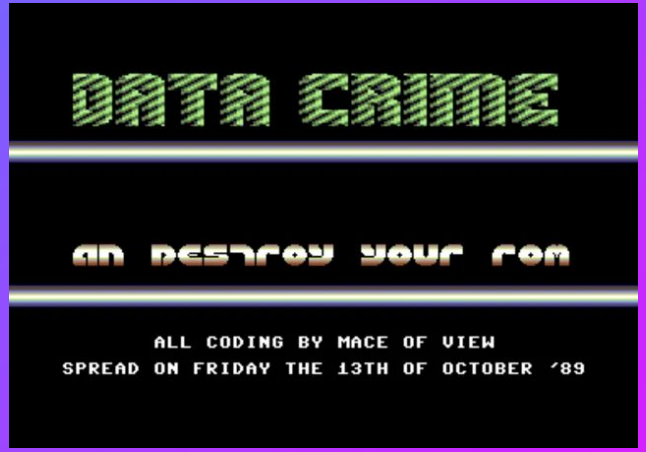
В пятницу 13 мая 1988 сразу несколько фирм и университетов нескольких стран мира «познакомились» с вирусом Jerusalem — в этот день вирус уничтожал файлы при их запуске. Это, пожалуй, один из первых MS-DOS-вирусов, ставший причиной настоящей пандемии — сообщения о заражённых компьютерах поступали из Европы, Америки и Ближнего Востока.

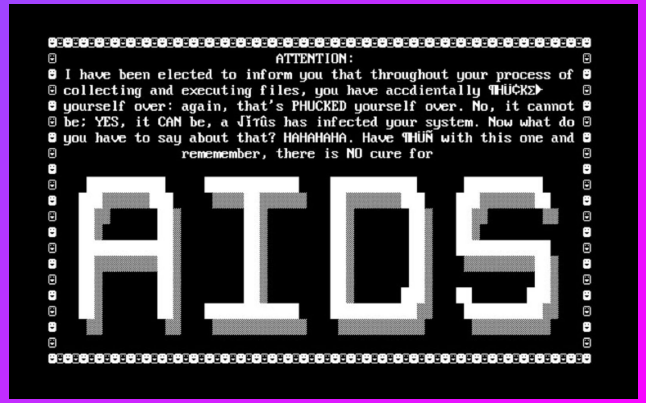
DATACRIME и AIDS

В 1989 году широкое распространение получили вирусы DATACRIME, которые начиная с 13 октября и до конца года разрушали файловую систему, а до этой даты просто размножались. Эта серия компьютерных вирусов начала распространяться в Нидерландах, США и Японии в начале 1989 года 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 недоступной всю информацию на жёстком 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 осуждён за вымогательство.

Также был создан первый вирус, противодействующий антивирусному программному обеспечению — The Dark Avenger. Он заражал новые файлы, пока антивирусная программа проверяла жёсткий диск компьютера.





Глобализация проблемы вирусов

Начиная с 1990 года проблема вирусов начинает принимать глобальный размах.

В начале года выходит первый полиморфный вирус — Chameleon. Данная технология была быстро взята на вооружение и в сочетании со стелс-технологией (Stealth) и бронированием (Armored) позволила новым вирусам успешно противостоять существующим антивирусным пакетам. Во второй половине 1990 года появились два стелс-вируса — Frodo и Whale. Оба вируса использовали крайне сложные стелс-алгоритмы, а 9-килобайтный Whale к тому же применял несколько уровней шифровки и антиотладочных приёмов.

В Болгарии открывается первая в мире специализированная BBS, с которой каждый желающий может скачать свежий вирус. Начинают открываться конференции Usenet по вопросам написания вирусов. В этом же году выходит «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига.

На проблему противостояния вирусам были вынуждены обратить внимание крупные компании — выходит Symantec Norton Antivirus.

Начало 1991 года отмечено массовой эпидемией полиморфного загрузочного вируса Tequila. Летом 1991 появился первый link-вирус, который сразу же вызвал эпидемию.

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. Кроме того, в конце 1992 появился первый вирус для Windows 3.1 — WinVer.

В 1993 году появляется всё больше вирусов, использующих необычные способы заражения файлов, проникновения в систему и т. д. Основными примерами являются: PMBS, работающий в защищённом режиме процессора Intel 80386. Shadowgard и Carbuncle, значительно расширившие диапазон алгоритмов компаньон-вирусов. Cruncher — использование принципиально новых приёмов сокрытия своего кода в заражённых файлах.

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.

Кибероружие и кибершпионские программы

«Flame»

В мае 2012 года Лаборатория Касперского обнаружила вредоносную программу «Flame», вирусные аналитики охарактеризовали её «самым сложным кибер-оружием из ранее созданных», поразившим от 1000 до 5000 компьютеров по всему миру. Вредоносный код «Flame» во многом превзошёл «Stuxnet»: размером — около 20 мегабайт, количеством библиотек и дополнительных плагинов — более 20-ти, базой данных SQLite3, различными уровнями шифрования, использованием редкого для создания вирусов языка программирования LUA. Как считают вирусные аналитики Лаборатории Касперского, разработка этой вредоносной программы началась более 5 лет тому назад и она проработала на заражённых компьютерах Ближнего Востока не менее двух лет. Детальный анализ вредоносной программы позволил исследователям установить, что её разработка началась ещё в 2008 году и активно продолжалась вплоть до момента обнаружения в мае 2012 года. Кроме того, выяснилось, что один из модулей платформы Flame был использован в 2009 году для распространения червя Stuxnet.

«NetTraveler».

В июне 2013 года «Лаборатория Касперского» объявила о раскрытии новой кибершпионской сети, получившей название NetTraveler и затронувшей более 350 компьютерных систем в 40 странах мира. Атаке подверглись государственные и частные структуры, в том числе правительственные учреждения, посольства, научно-исследовательские центры, военные организации, компании нефтегазового сектора, а также политические активисты. Россия оказалась в числе наиболее пострадавших стран, заняв вторую строчку в рейтинге государств, испытавших на себе наиболее заметные последствия операции NetTraveler. Согласно результатам расследования, проведенного экспертами «Лаборатории Касперского», кампания шпионажа стартовала ещё в 2004 году, однако пик её пришелся на период с 2010 по 2013 гг. В последнее время в сферу интересов атакующих входили такие отрасли, как освоение космоса, нанотехнологии, энергетика, в том числе ядерная, медицина и телекоммуникации. Помимо всего прочего, аналитики «Лаборатории Касперского» обнаружили, что 6 жертв операции NetTraveler ранее пострадали от «Красного октября». Тем не менее прямых связей между организаторами NetTraveler и «Красного октября» найдено не было. В сентябре 2013 года эксперты «Лаборатории Касперского» обнаружили сразу две кампании кибершпионажа, направленные на южнокорейские промышленные, научно-исследовательские, оборонные и государственные организации. Первая кампания строилась на базе троянца Kimsuky, который обладал таким функционалом, как слежение за нажатием клавиш, составление и кража списка файлов во всех каталогах, удаленное управление компьютером и хищение документов формата HWP, повсеместно используемого в южнокорейских госучреждениях в составе пакета Hancom Office. Улики, обнаруженные экспертами «Лаборатории Касперского», дают возможность предполагать наличие «следа» Северной Кореи. Среди целей атакующих были южнокорейские университеты, занимающиеся изучением международных отношений и разработкой государственной оборонной политики, национальная логистическая компания и группы политических активистов.

Как бороться с вирусами на компьютере

1.Проверьте настройки своего компьютера. У вас как минимум должен быть установлен файервол, а также должен быть надежный антивирус свежей версии.
2.Установите надежный антивирус. Знайте, что на новые компьютеры ставить дополнительные антивирусные программы может быть не нужно, поскольку во многих случаях они выпускаются со встроенными антивирусными функциями, которые работают лучше сторонних приложений.
3.Делайте резервные копии и храните их в удаленном месте. Это может быть облако или удаленный жесткий диск в сети.
4.Не нажимайте на все подряд. В интернете полно баннеров и всплывающей рекламы, которая сделана так, чтобы привлечь внимание пользователя и заставить его нажать на ссылку.
5.Знайте, что некоторые всплывающие окна могут быть фальшивыми. Некоторые всплывающие окна имитируют работу надежных антивирусов.

Спасибо за внимание