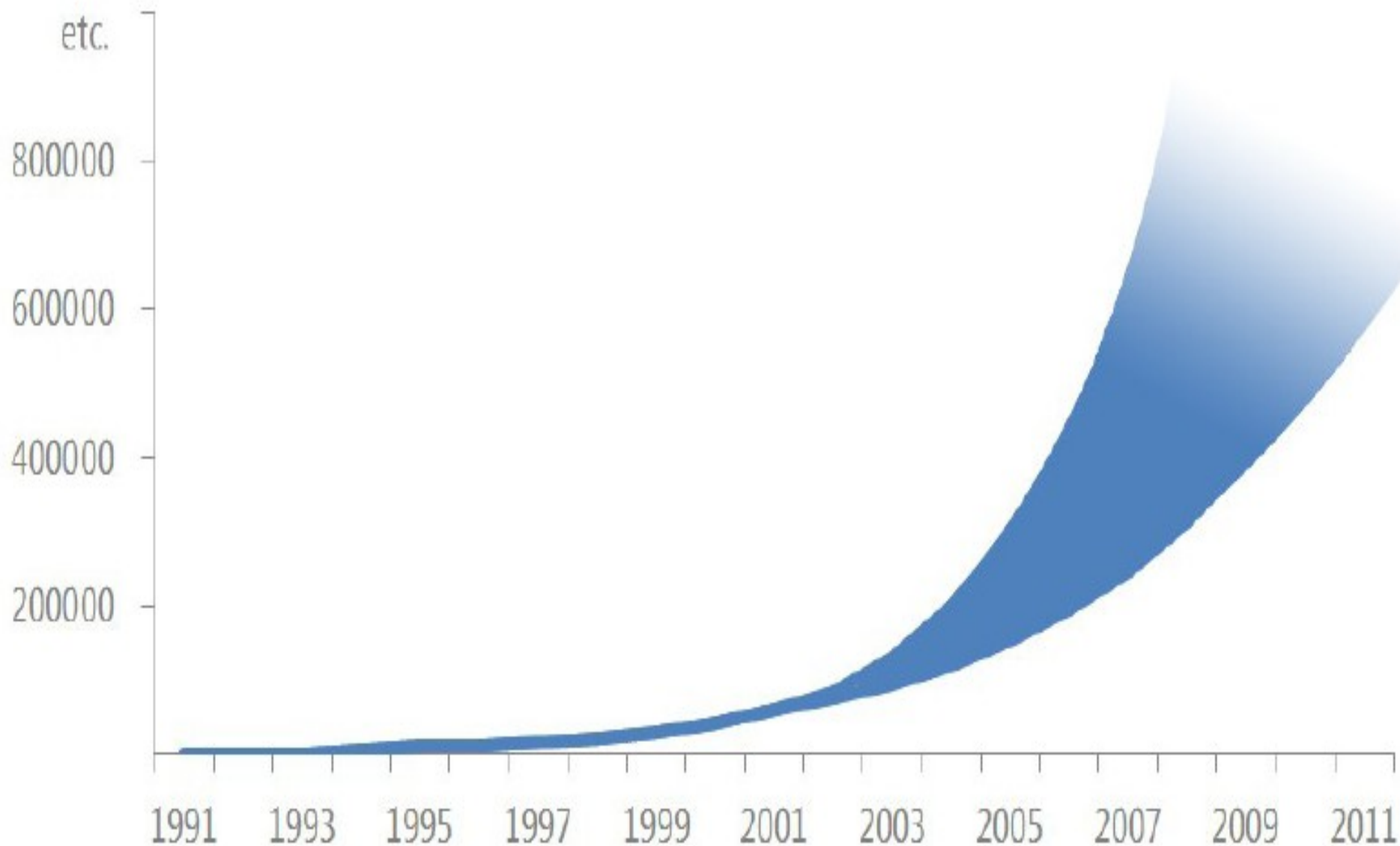


COMPUTER SECURITY

MALWARE

Willy Sudiarto Raharjo

Teknik Informatika
Universitas Kristen Duta Wacana



http://download.microsoft.com/download/1/A/7/1A76A73B-6C5B-41CF-9E8C-33F7709B870F/Microsoft_Security_Intelligence_Report_Special_Edition_10_Year_Review.pdf

Malicious Software Attacks

- Malware: damaging/annoying attack software that enters a computer system without the owner's knowledge
- Classification
 - Infecting malware
 - Infect a computer system with destructive software
 - Concealing malware
 - Hiding from user and doing something nasty in the background

Infecting Malware

■ Virus

- Self-replicating program that produces its own code by attaching copies to other executables
- Need a “carrier”
 - Documents/program
 - User
- Launched when carrier is executed by the users
 - Downloading email attachment
 - File sharing via USB flash drive loaded using autorun.inf

[Home](#) | [News](#) | [comment & features](#) | [arts & entertainment](#) | [Sport](#)

[General News](#) | [local news](#) | [Student news](#) | [Academic News](#) | [Student Politics](#) | [National Politics](#)

Virus shuts down Exeter University computer network

Malicious attack forces lecturers to return to more traditional teaching methods

Marcus De Wilde

Wednesday 03 February 2010, The Journal Issue 30

A major computer virus attack at the University of Exeter has sparked warnings at campuses across the country.

The attack on 18 January saw the entire university network temporarily shut down to prevent the virus from spreading.

Stuart Franklin, a spokesman for the University of Exeter, said: "We were attacked by a virus. It was a malicious attack. It is the first time I have known an attack to succeed. It affected everyone, staff and students."

Arthur Clowes, an undergraduate politics and economics student, told *The Journal*: "The attack was so sudden. The IT department had issued a blanket message warning everyone. The network went down and no one knew what had happened."

The attack forced lecturers to abandon electronic whiteboards and projectors and return to more traditional marker pens and blackboards.

Mr Clowes added: "Some of my lecturers have shown themselves to be too dependent on computers. There are those for whom the loss of technology has proved to be no problem while others have struggled without it."

Ian Hill, security manager for Kcom, which oversees the security measures for Exeter internet company Eclipse, said: "Viruses that come out these days we tend to generally refer to as malware."

"It's difficult to say what it was or where it came from. These things are coming out all the time. The virus almost certainly came in either via email or via students browsing affected websites. We do the best we can, but no system is 100 percent secure."

Article tools

- [Print article](#)
- [Increase](#) or [Decrease](#) text size
- Share: [!\[\]\(ebd6bb7e63799a540c476e56de06a0ed_img.jpg\)](#) [!\[\]\(e43afbdc743fd9d9a5a6d3c334ee35c3_img.jpg\)](#) [!\[\]\(7bdb7a0d8bc456bf78d3c87f99586f5c_img.jpg\)](#) [!\[\]\(ac4918d513c8c222db0d525550a16080_img.jpg\)](#) [!\[\]\(371c3e5ec0c5f3fc458fa533d77c7fc7_img.jpg\)](#)
- Show [0 comments](#)

Malware and Spam Rise 70% on Social Networks, Security Report Reveals

Corporate Security at Risk from Social Networks Claim Three Out of Four Businesses

BOSTON--([BUSINESS WIRE](#))--A report published today by IT security and data protection firm [Sophos](#) has revealed an alarming rise in attacks on users of social networks, such as Facebook and Twitter, by cybercriminals.

Sophos's "Social Security" investigation reveals that criminals have increasingly focused attacks on social networking users in the last 12 months, with an explosion in the reports of spam and malware:

- 57% of users report they have been spammed via social networking sites, a rise of 70.6% from last year
- 36% reveal they have been sent malware via social networking sites, a rise of 69.8% from last year

"Computer users are spending more time on social networks, sharing sensitive and valuable personal information, and hackers have sniffed out where the money is to be made," said Graham Cluley, senior technology consultant for Sophos. "The dramatic rise in attacks in the last year tells us that social networks and their millions of users have to do more to protect themselves from organized cybercrime, or risk falling prey to identity theft schemes, scams, and malware attacks."

72% of Firms Worried Workers Behavior on Social Networks is Putting Their Business at Risk

Sophos surveyed more than 500 organizations*, and discovered that 72% are concerned that employee behavior on social networking sites exposes their businesses to danger, and puts corporate infrastructure – and the sensitive data stored upon it – at risk.

The "Social Security" survey is just one part of Sophos's 2010 Security Threat Report, which explores current and emerging computer security trends. It reveals that criminals identify potential victims on social networks, and then attack them, both at home and at work. In Sophos's opinion, many Web 2.0 sites are concentrating too much on growing their marketshare at the expense of properly defending their existing users from Internet threats.

Facebook – The Most Feared Social Network?

Survey respondents were also asked which social network they believed posed the biggest security risk, with 60% naming Facebook:

- 1. Facebook: 60%
- [2. MySpace: 18%](#)
- 3. Twitter: 17%
- 4. LinkedIn: 4%

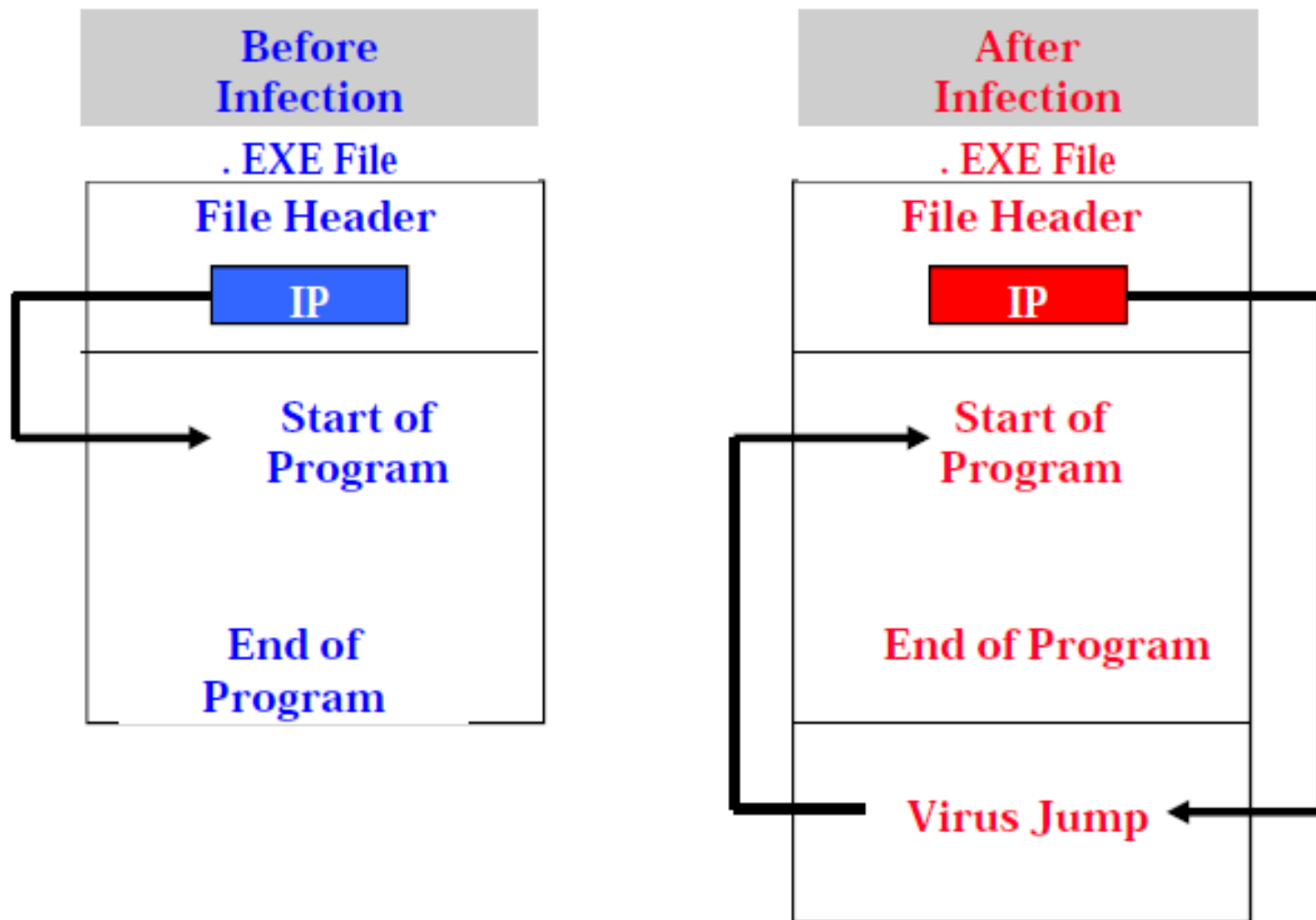
"We shouldn't forget that Facebook is by far the largest social network – and you'll find more bad apples in the biggest orchard," explained Cluley. "The truth is that the security team at Facebook works hard to counter threats on their site – it's just that policing 350 million users can't be an easy job for anyone. But there is no doubt that simple changes could make Facebook users safer. For instance, when Facebook rolled-out its new recommended privacy settings late last year, it was a backwards step, encouraging many users to share their information with everybody on the Internet."

"Targeted attacks against companies are in the news at the moment, and the more information a criminal can get about your organization's structure, the easier for them to send a poisoned attachment to precisely the person whose computer they want to break into"

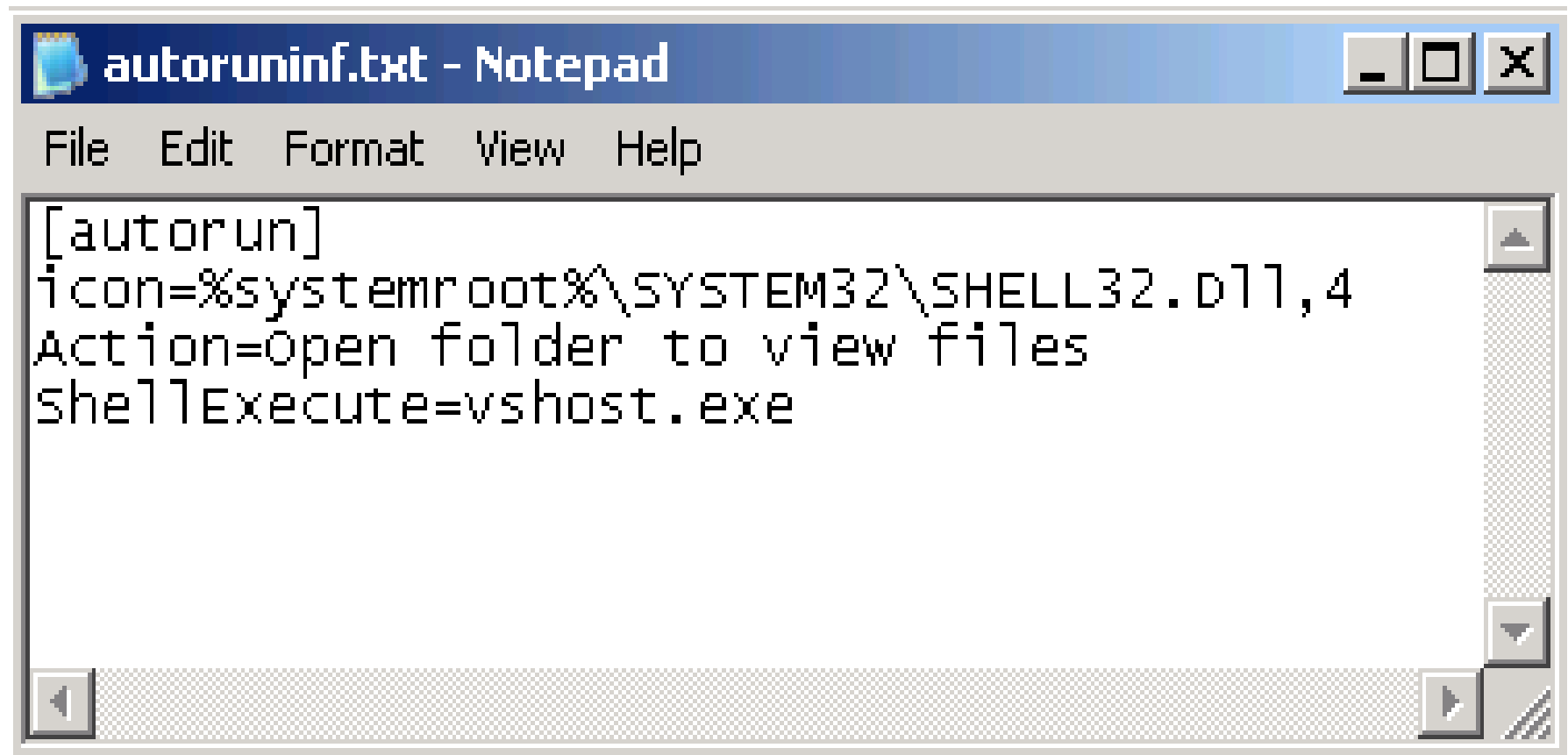
Types of Computer Viruses

- File infector
 - Infect program executables files (.COM, .EXE)
- Resident
 - Loaded into RAM and interrupt functions executed by users
- Boot
 - Infects the MBR of a hard drive (eg. CIH)
- Macro
 - Written in macro script language (eg. VBA)
 - Mostly used in Office application (MS. Office)

File Infection



Autorun.inf

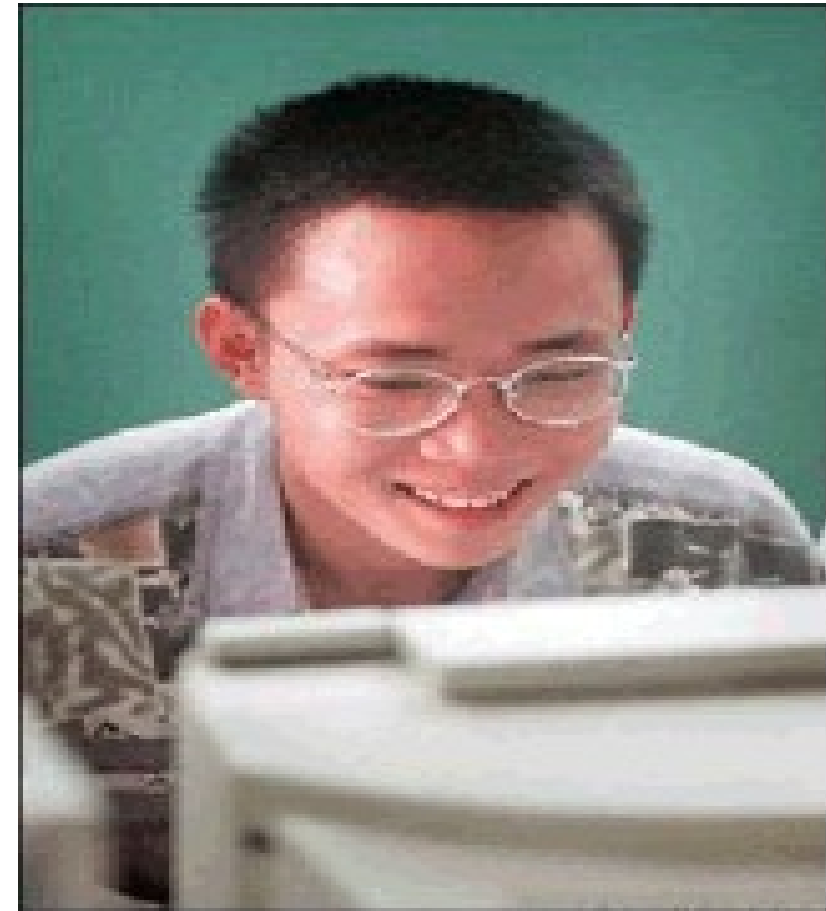
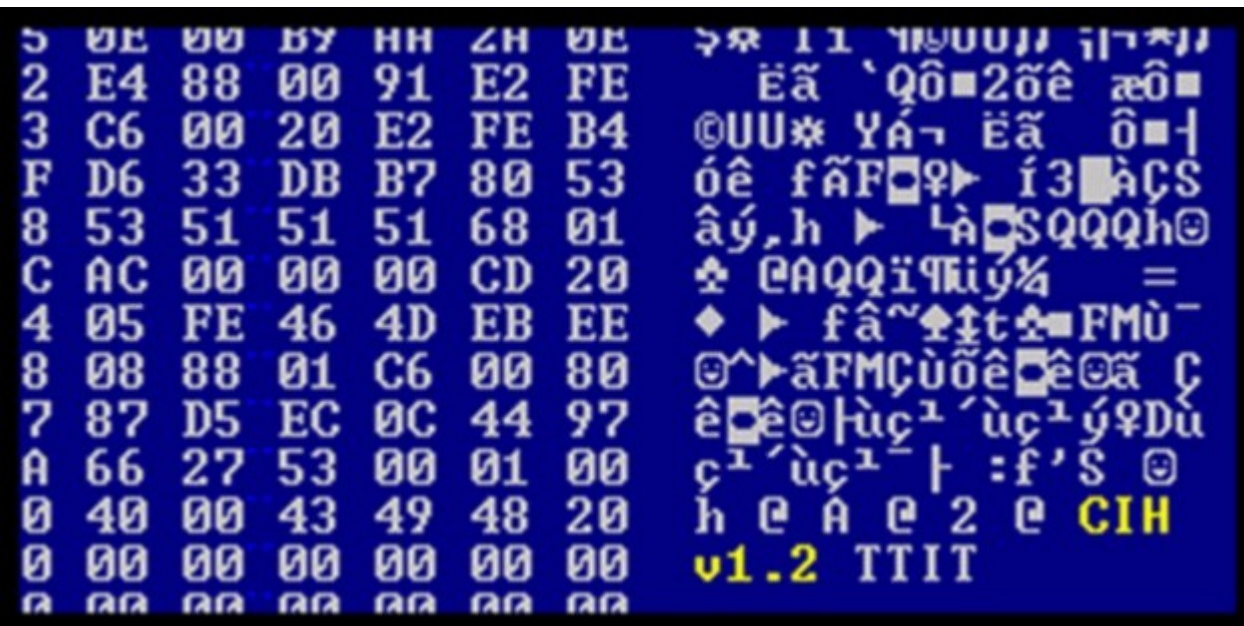


The image shows a classic Windows Notepad window. The title bar at the top reads "autoruninf.txt - Notepad" and includes standard minimize, maximize, and close buttons. Below the title bar is a menu bar with the options "File", "Edit", "Format", "View", and "Help". The main text area contains the following text:

```
[autorun]
icon=%systemroot%\SYSTEM32\SHELL32.DLL,4
Action=Open folder to view files
shellExecute=vshost.exe
```

The text is displayed in a monospaced font. The window also features a vertical scrollbar on the right and a horizontal scrollbar at the bottom.

CIH (Chernobyl)



Macro Virus



Virus Indication

Indications of a virus attack:

- Programs take longer to load than normal
- Computer's hard drive constantly runs out of free space
- Files have strange names which are not recognizable
- Programs act erratically
- Resources are used up easily

How Does Virus Attacks?

Stealth Virus:

- Can hide from anti-virus programs

Polymorphic Virus:

- Can change their characteristics with each infection

Cavity Virus:

- Maintains same file size while infecting

Tunneling Virus:

- They hide themselves under anti-virus while infecting

Camouflage Virus:

- Disguise themselves as genuine applications of user

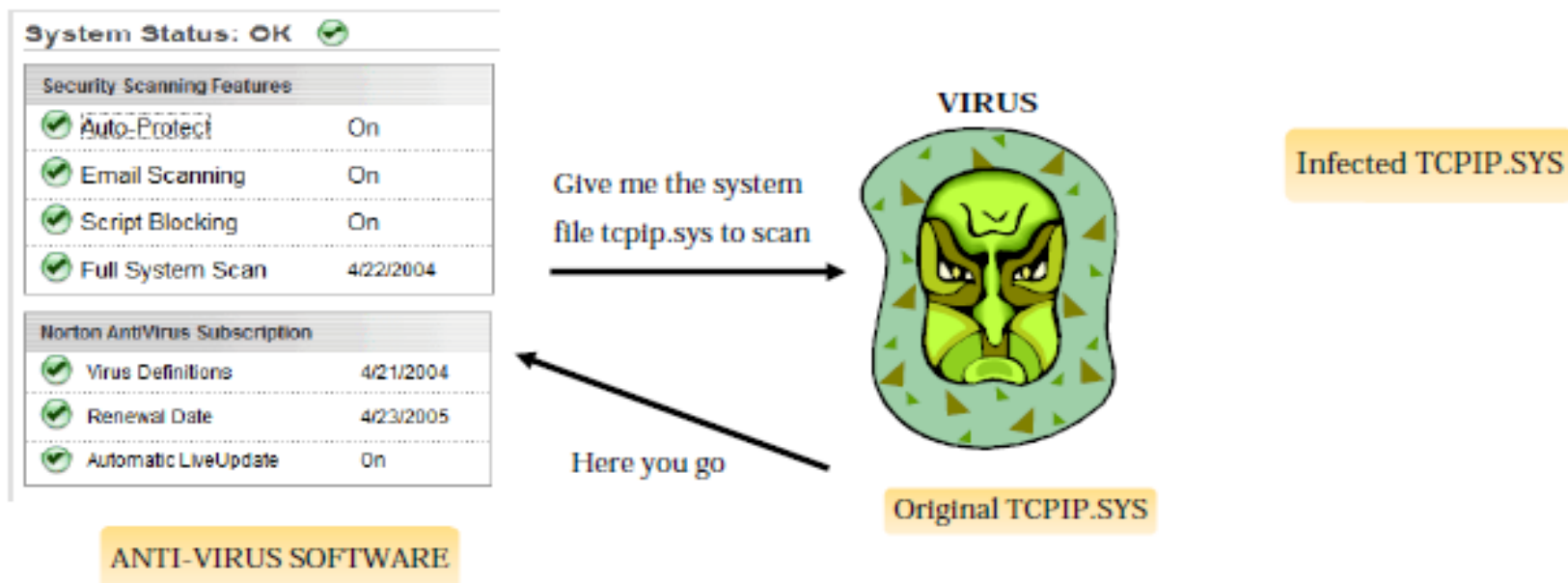


Stealth Virus

These viruses evade anti-virus software by intercepting its requests to the operating system

A virus can hide itself by intercepting the anti-virus software's request to read the file and passing the request to the virus, instead of the OS

The virus can then return an uninfected version of the file to the anti-virus software, so that it appears as if the file is "clean"



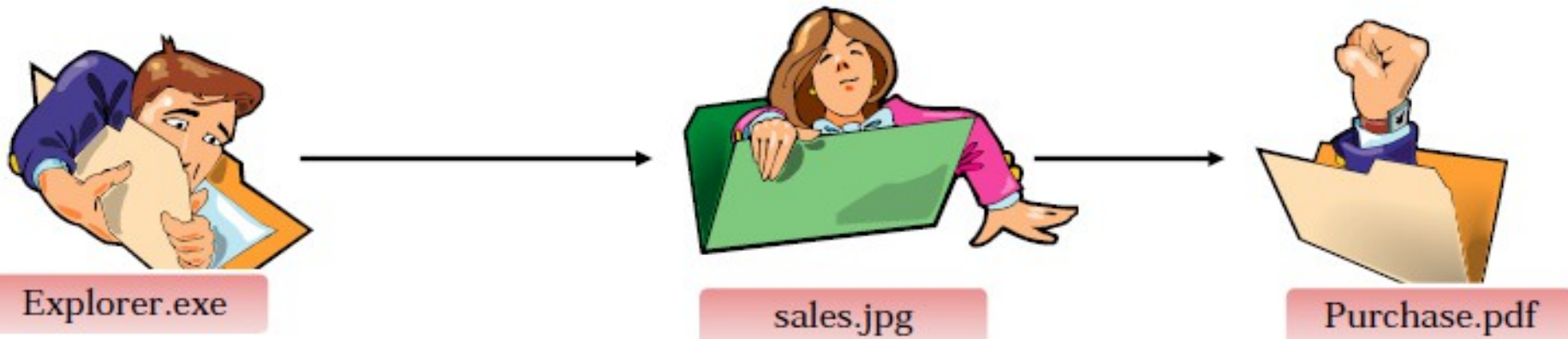
Self-Modification

Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for *virus signatures*

A signature is a characteristic byte-pattern that is part of a certain virus or family of viruses

Self-modification viruses employ techniques that make detection by means of signatures difficult or impossible

These viruses modify their code on each infection (each infected file contains a different variant of the virus)

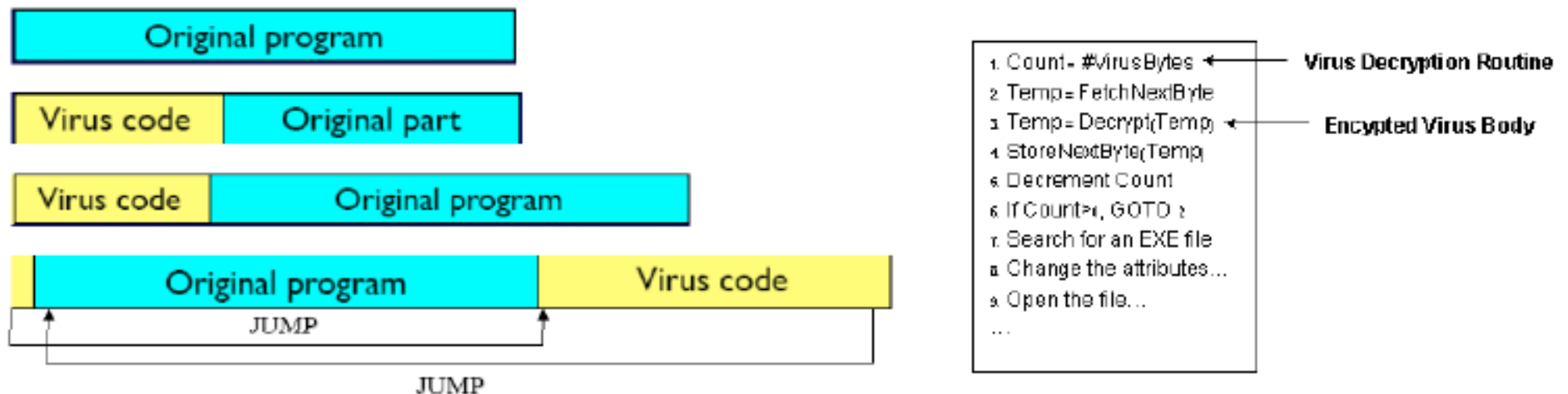


Polimorphic Virus

A well-written polymorphic virus therefore has no parts that stay the same on each infection

To enable polymorphic code, the virus has to have a polymorphic engine (also called *mutating engine* or *mutation engine*)

Polymorphic code is a code that mutates while keeping the original algorithm intact

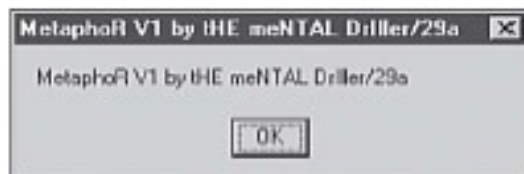


Metamorphic Virus

Metamorphic viruses rewrite themselves completely each time they are to infect new executables

Metamorphic code is a code that can reprogram itself by translating its own code into a temporary representation, and then back to normal code again

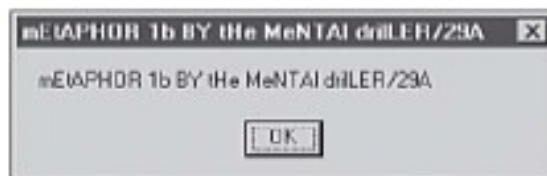
For example, W32/Simile consisted of over 14000 lines of assembly code, 90% of it is part of the metamorphic engine



a.) Variant A



c.) The "Unofficial" Variant C



b.) Variant B

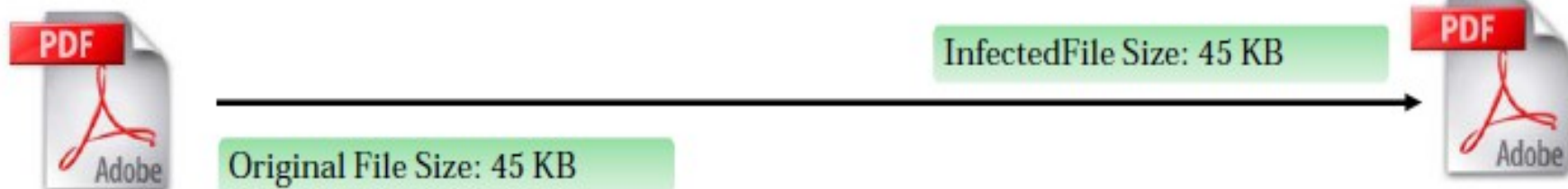


d.) The .D variant (which was the "official" C of the original author)

Cavity Virus

Cavity Virus overwrites a part of the host file that is filled with a constant (usually nulls), without increasing the length of the file, but preserving its functionality

Sales & Marketing Management is the leading authority for executives in the sales and marketing management industries. The suspect, Desmond Turner, surrendered to authorities at a downtown Indianapolis fast-food restaurant

[illegible]

Sparse Infector Virus

Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose lengths fall within a narrow range



By infecting less often, such viruses try to minimize the probability of being discovered



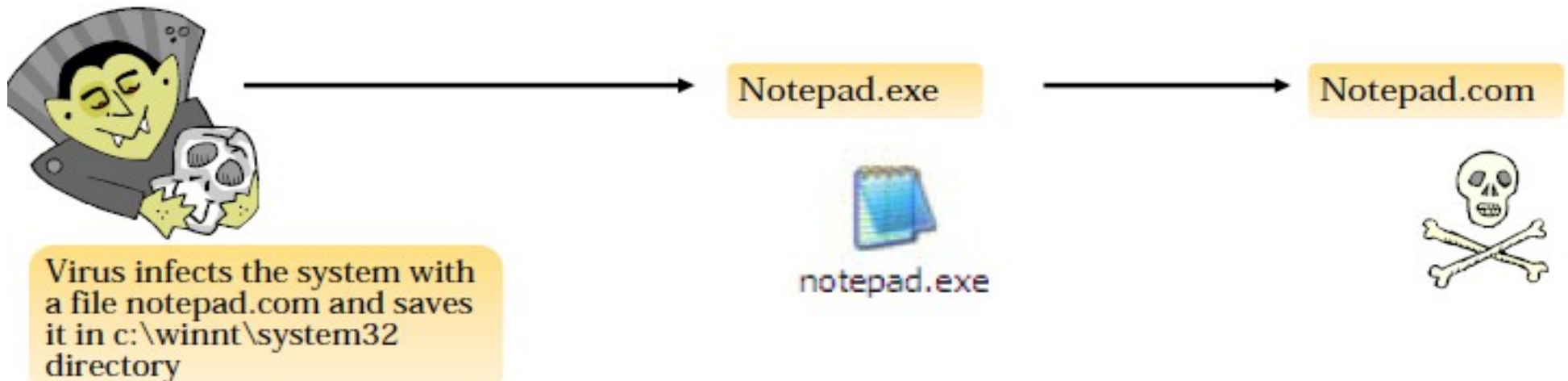
Wake up on 15th of every month and execute code



Companion Virus

A Companion virus creates a companion file for each executable file the virus infects

Therefore a companion virus may save itself as notepad.com and every time a user executes notepad.exe (good program), the computer will load notepad.com (virus) and therefore infect the system



File Extension Virus

File extension viruses change the extensions of files

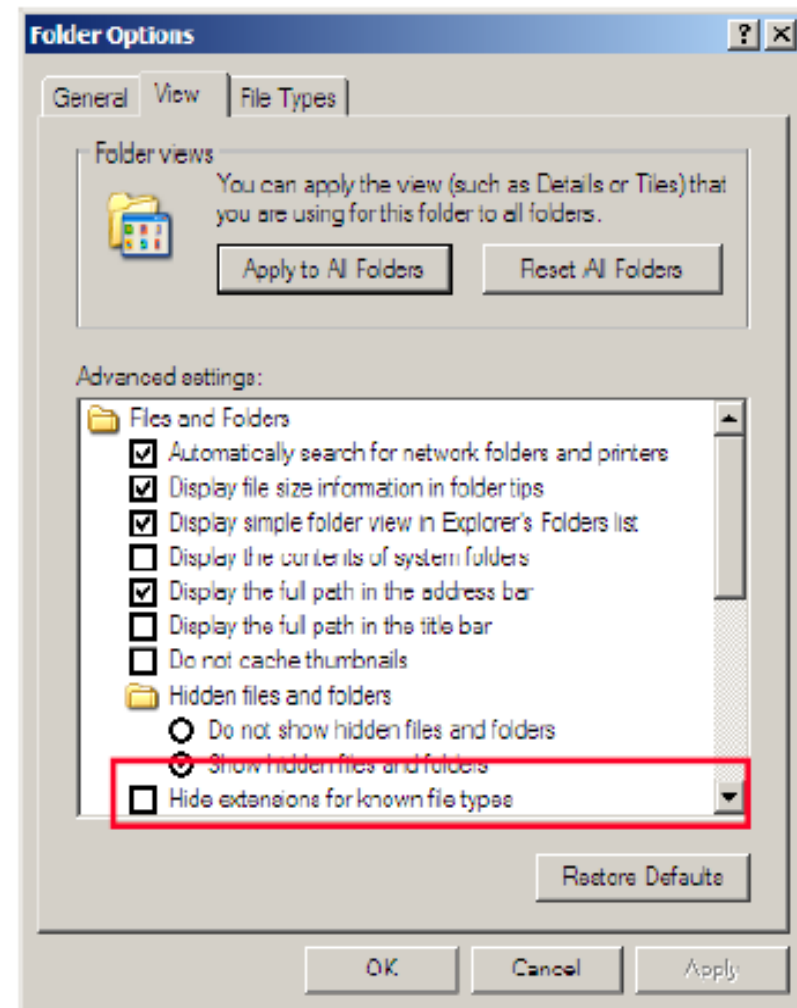
.TXT is safe as it indicates a pure text file

With extensions turned off if someone sends you a file named BAD.TXT.VBS you will only see BAD.TXT

If you've forgotten that extensions are actually turned off, you might think this is a text file and open it

This is really an executable Visual Basic Script virus file and could do serious damage

Countermeasure is to turn off "Hide file extensions" in Windows



Worms

Worms are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer whereas a worm does not

There is a difference between general viruses and worms

A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs

A worm spreads through the infected network automatically but a virus does not

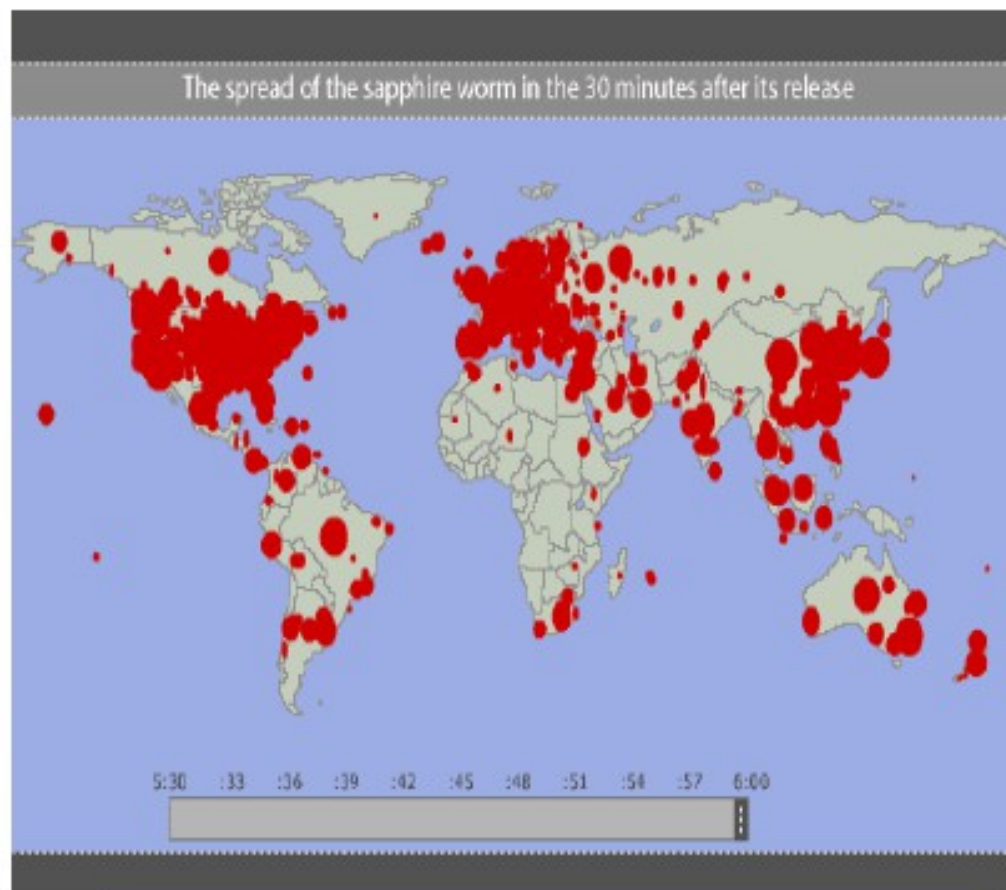


Slammer Worm

The Slammer worm (also known as the Sapphire worm) was the fastest worm in history—it doubled in size every 8.5 seconds at its peak

From the time it began to infect hosts (around 05:30 UTC) on Saturday, Jan. 25, 2003, it managed to infect more than 90 percent of the vulnerable hosts within 10 minutes using a well-known vulnerability in Microsoft's SQL Server

Slammer eventually infected more than 75,000 hosts, flooded networks across the world, caused disruptions to financial institutions, ATMs, and even an election in Canada



Source:

<http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/slammermapnoflash.html>

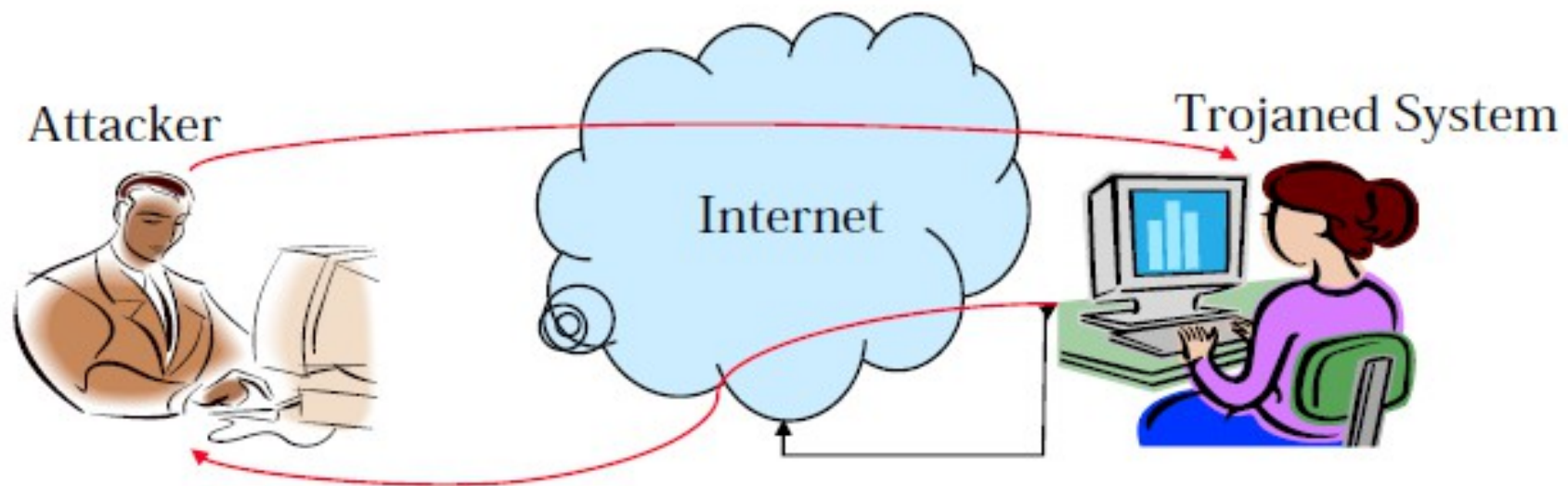
Concealing Malware

- Trojan Horses

A Trojan is a small program that runs hidden on an infected computer

With the help of a Trojan, an attacker gets access to stored passwords in the Trojaned computer and would be able to read personal documents, delete files and display pictures, and/or show messages on the screen





An attacker gets access to the Trojaned system as the system goes online

By the access provided by the Trojan, the attacker can stage different types of attacks

How Do Trojans Gets In?

Instant Messenger applications

IRC (Internet Relay Chat)

Attachments

Physical access

Browser and email software bugs

NetBIOS (FileSharing)

Fake programs

Untrusted sites and freeware software

Downloading files, games, and screensavers from Internet sites

Legitimate "shrink-wrapped" software packaged by a disgruntled employee



Anti Virus

- Signature Scanning

- Using virus database to scan for virus' fingerprints
- Depends on how often you update your database
- Not able to detect newly created virus

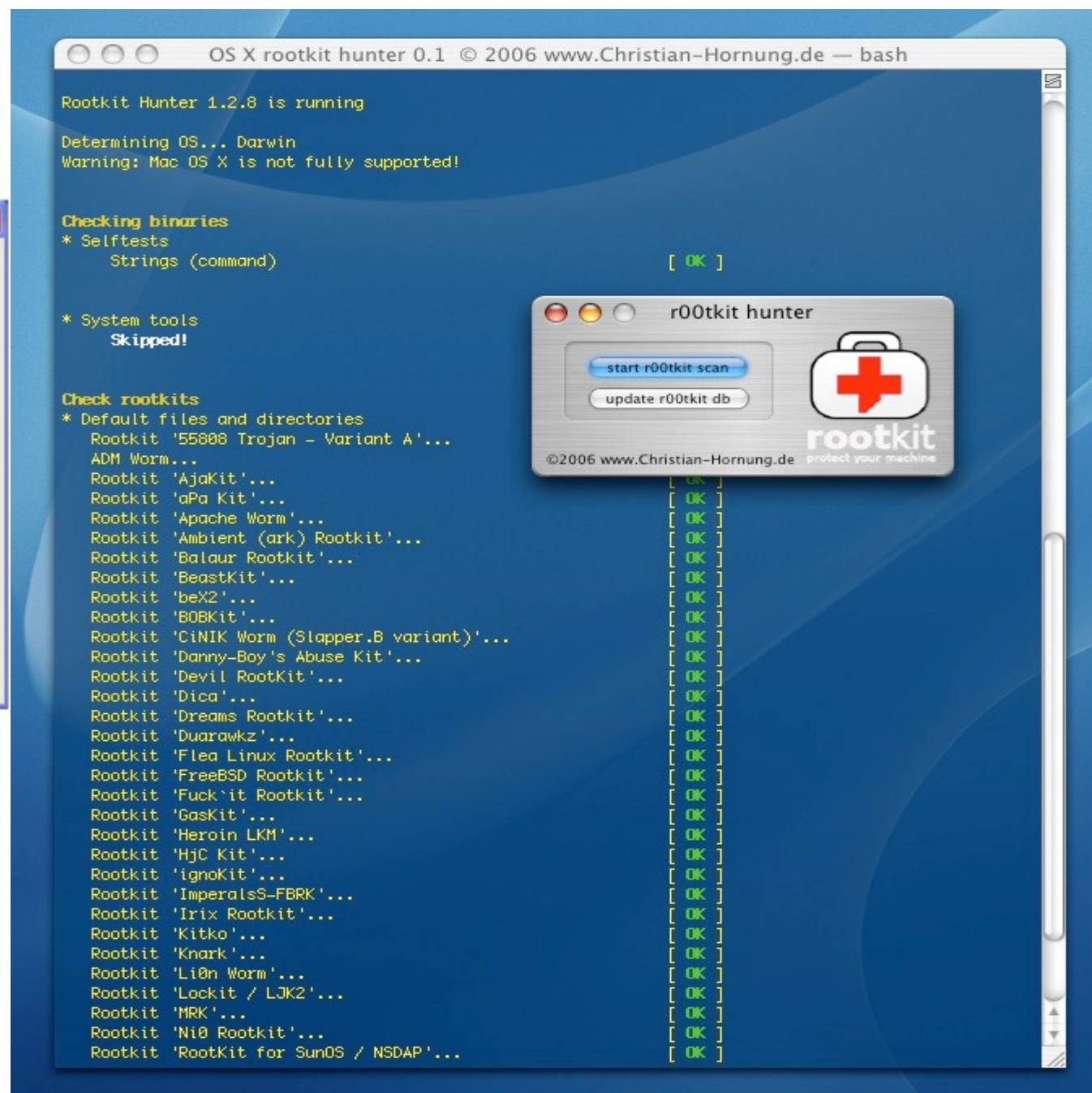
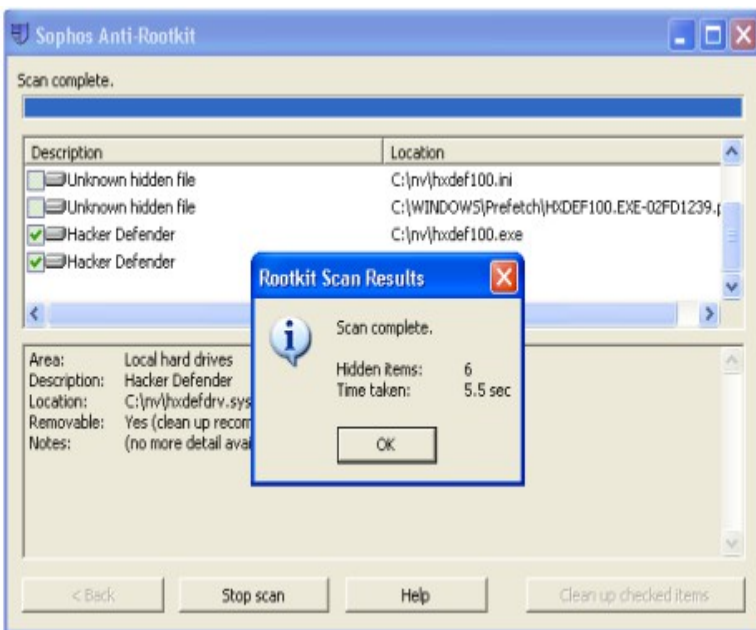
- Heuristic Scanning

- Scans for instructions not found on normal application
- Employs weight-based and/or rule-based systems

<http://www.symantec.com/connect/ja/articles/heuristic-techniques-av-solutions-overview>

Rootkits

- Set of software tools which hides the presence of other type of malicious software
- Replacing OS commands with modified version
- Users can no longer trust their computer
- Solution:
 - Boot from clean CD/DVD or flash drive, not from hard drive
 - Format your system and restore all your data from backups



Logic Bomb

- Computer program that is active when triggered by event
- Difficult to detect until it's triggered
 - Normally embedded in large computer programs



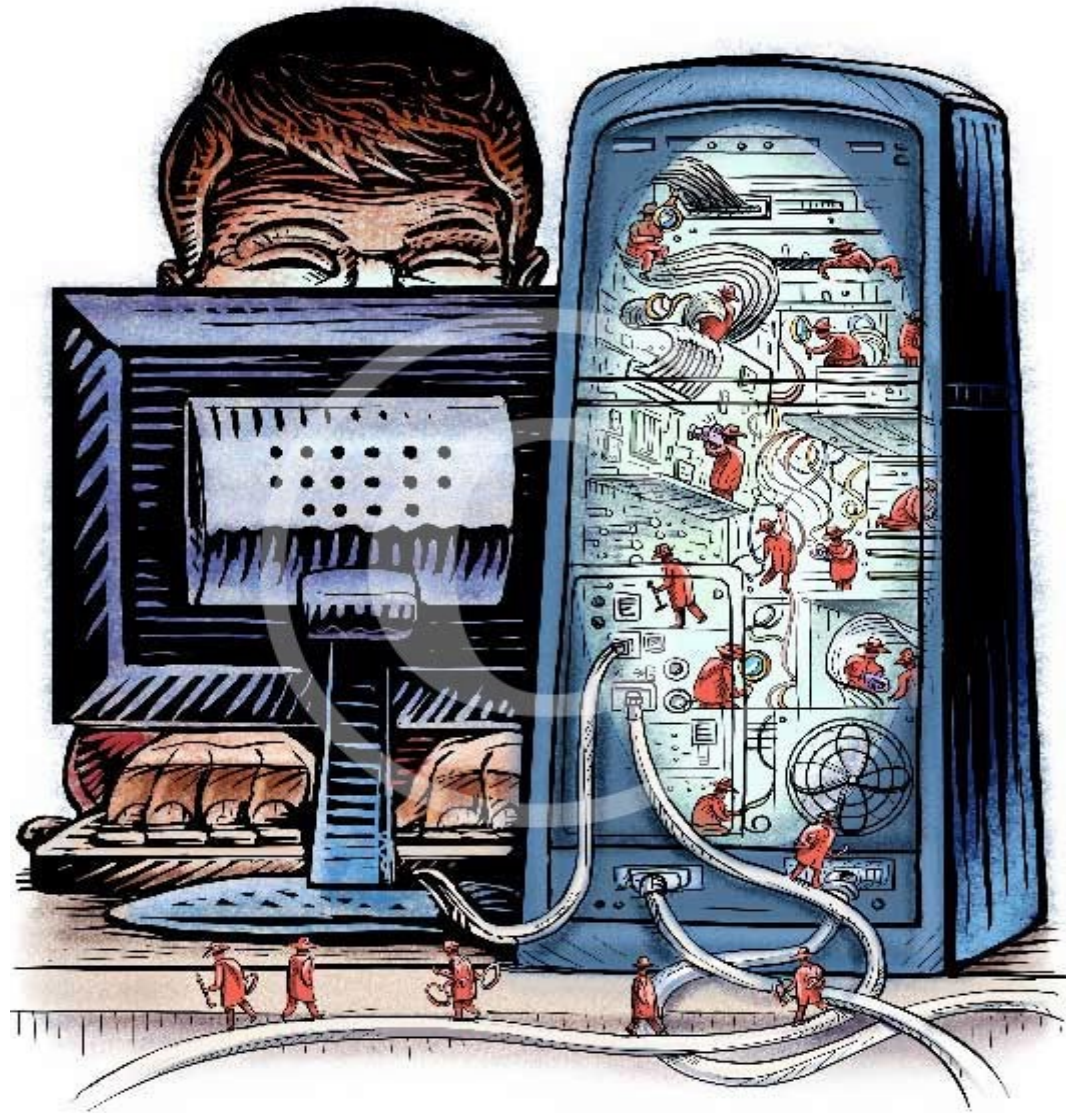
Zombie dan Botnets

- Infected computer under remote control by attacker
- Collections of zombie: botnets
- What can they do:
 - (D)DoS attack
 - Manipulate online pooling
 - Spreading malware



Spyware

- Does not replicate
- Tracking software
 - Advertisements
 - Personal information
 - Web browsing activity
- User are not aware of their existence

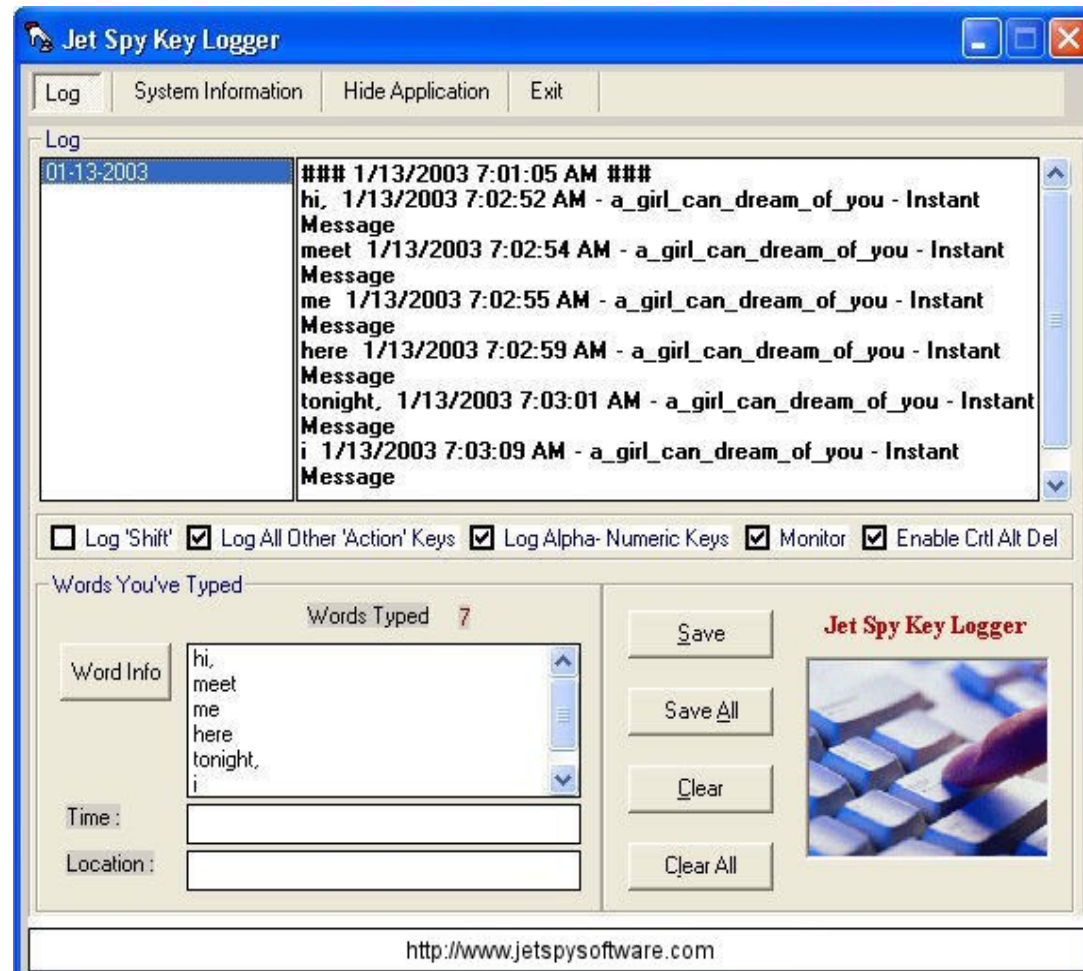


KeyLogger

- Monitors each keystroke a user types on keyboard
- Information retrieved or transmitted to remote location

Types:

- Hardware keylogger
- Software keylogger



Keyboard Keylogger

