# 4.4 The anatomy of a virus

**A Study this diagram and read the text below. Highlight all words you don’t understand.**

A biological virus is a very small, simple organism that infects living cells, known as the host, by attaching itself to them and using them to reproduce itself. This often causes harm to the host cells. 5

Similarly, a computer virus is a very small program routine that infects a computer system and uses its resources to reproduce itself. It often does this by patching the operating system to enable it to de-10

tect program files, such as COM or EXE files. It then copies itself into those files. This sometimes causes harm to the host computer system.

When the user runs an infected program, 15

it is loaded into memory carrying the virus. The virus uses a common programming technique to stay resident in memory. It can then use a reproduction routine to infect other programs. This process continues until the computer is switched off.

The virus may also contain a payload that remains dormant until a trigger event activates it, 20

such as the user pressing a particular key. The payload can have a variety of forms. It might do something relatively harmless such as displaying a message on the monitor screen or it might do something more destructive such as deleting files on the hard disk.

When it infects a file, the virus replaces the first instruction in the host program with a command that changes the normal execution sequence. This type of command is known as a JUMP 25

command and causes the virus instructions to be executed before the host program. The virus then returns control to the host program which then continues with its normal sequence of instructions and is executed in the normal way.

To be a virus, a program only needs to have a reproduction routine that enables it to infect other programs. Viruses can, however, have four main parts. A misdirection routine that ena-30

bles it to hide itself; a reproduction routine that allows it to copy itself to other programs; a trigger that causes the payload to be activated at a particular time or when a particular event takes place; and a payload that may be a fairly harmless joke or may be very destructive. A program that has a payload but does not have a reproduction routine is known as a Trojan.

**B Answer the following questions about the text on the previous page.**

**1 What is the function of the JUMP instruction?**

This command causes the virus instructions to be executed before the host program. Whenever it infects a file, the virus replaces the first instruction in the host program with a com25 mand which changes the normal execution process.

**2 What are the main parts of the virus code?**

The virus hides itself with a misdirection routine. This allows it to copy itself everywhere. The virus is equipped with a trigger causing the activation at a particular time or even when a specific task is running.

**3 What is the last act of the virus?**

The virus shuts down the computer.

**4 How are computer viruses like biological viruses?**

Mostly a virus is well hidden and reproduces itself.

**5 What is the effect of a virus patching the operating system?**

The virus detects files such as DOM’s or EXE’s. Then it copies itself into these files and produces errors in the operating system.

**6 Why are some viruses designed to be loaded into memory?**

They are using a common programming technique to last inside the memory. Equipped with a reproduction routine, it infects other programs and does this so until the computer powers off.

**7 What examples of payload does the writer provide?**

There are several types of viruses. Some types do relatively harmless things such as changing the background or displaying a message. The other types do things in the destructive way, like deleting files or sending anonymous data.

**8 What kind of programs do viruses often attach to?**

DOM or EXE files.

**9 Match each virus routine to its function.**

Routine Function

**1** misdirection **a** does the damage

**2**  reproduction **b** attaches a copy of itself to another program

**3** trigger **c** hides the presence of the code

**4** payload **d** decides when and how to activate the payload

1 – c, 2 – b, 3 – d, 4 - a

**10 How does a Trojan differ from a virus?**

A Trojan is a payload program without a reproduction routine.

**C Fill in the gaps. Use the words from the list below but don’t change them. Use each word only once. There are some words you don’t need.**

compromise dismissed infiltrated prosecute corrupted dormant infringement scam crucial Encryption launch spreading Decryption ftp padlock stalking disguised https replicates tamper trigger

1 On a certain date a launch routine is activated which makes keys beep when pressed and corrupts files.

2 When an infected program is run, the boot sector is corrupted which causes the disk content to be overwritten and data to be lost.

3 A secure website can be recognized in two ways: the address bar shows the letters https and a closed padlock is displayed at the bottom of the screen.

4 This program displays a message when it detects spyware and other unwanted software that may compromise your privacy or damage your computer.

5 Security is crucial when you send confidential information online.

6 When buying a book online and typing in your credit card number, your data could be copied if one of the intermediary computers is corrupted by hackers.

7 Encryption changes data into a secret code so that only someone with a key can read it.

8 A worm replicates itself and sends a copy to everyone in an address book.

9 A Trojan horse is disguised as a useful program; it may affect data security.

10 In 1988 the Union Bank of Switzerland lost almost £32 million to hackers. As a result, N. Whitely was arrested in connection with virus spreading.

11 A virus can remain dormant until a trigger event activates it, such as the user pressing a particular key.

12 Because of the financial crisis, Siemens dismissed another 120 people.