



# Data Recovery Clinic

935 MAIN Street, Suite A-1 , Safety Harbor, FL 34695

866-360-4192

866-360-4192  
727-360-4192 (24/7)  
Fax: 800-675-3967

Data Recovery Clinic  
now has New York Office

826 Broadway \* Suite 9  
NY, NY 10003  
Phone: 212-996-6125

## Introduction to Viruses

### What is a virus?:

It is a program that can enter a computer in many different ways. These programs, or viruses, are special programs in that they can cause unwanted or damaging effects or take advantage of exploits and operating system weakness to cause damage, system instability, or even allow other programs or users to access your network or data files. When a virus enters a computer or network, it will often try to situate itself in a place where it can be activated and distributed, unintentionally, by the user. A virus will not act until it has been run or until certain pre-established conditions have been met, called the "trigger" condition (a specific date, an operation carried out by the user, etc.). In many cases, the effects produced by a virus, called the "virus payload", will not be seen until some time after it has infected the computer. A typical characteristic of viruses is their capacity to reproduce and spread to other files or programs.

### Why are they called "viruses"?:

Computer viruses are called viruses due to their similarities with biological viruses. In the same way as biological viruses enter the body and infect the cells, computer viruses get into the into the computer and infect files. In addition, both types of virus can reproduce themselves and spread, passing the infection from one infected system to others.

The effects produced by a virus can range from catastrophic to simply annoying: they can damage or delete data stored in a computer, cause the infected computer to crash, display on-screen messages, etc.

In addition to propagation and infection techniques, many viruses will also use "evasion" techniques. This means that the virus has techniques or a defense system that makes it difficult to detect it and helps it avoid any action taken against it.

### How do I know if I have got a virus?:

It may appear that you have a virus in your computer, but you cannot be sure that this is the case until it is detected using an antivirus tool (programs that detect and eliminate viruses). Some actions that can be carried out by a virus are obvious enough to be recognized and could include: messages displayed on-screen, operations slowing down, the properties of some files change, files and/or folders disappear, the computer will not start, the content of the infected disk is lost, etc.

Viruses are increasingly sent via e-mail, therefore it is important to delete all suspicious and/or unsolicited messages. However, messages known as hoaxes are e-mail messages that inform you about the existence of a possible virus, but are

Virus [Hard Drive Recov](#)

NOT viruses. If you have any doubt about an email or attachment, DO NOT open it.

### **What do viruses infect?:**

The main target of viruses are files located in storage devices such as hard and floppy disks. They target program files, although other types of files and documents can also be infected. A program is simply a file with an .EXE or .COM extension, which can be run to perform specific operations.

As we have already mentioned, there are viruses designed to infect files that are not programs. However, these documents contain elements known as macros. Macros are small programs that the user can include in certain types of files.

Other elements prone to virus attack are the storage devices themselves. By attacking the places in which files are stored, the damage produced by the virus will affect all of the information they contain.

### **How did viruses arise?:**

In the 60s, some scientists developed a game for programmers called CoreWar. The objective of the game was to introduce some programs in memory that made the other programs run certain instructions. The aim was to saturate the memory and for each program to act independently, carrying out certain actions.

Now, however, it is not a game. Some experts believe that over 1,000 new viruses, trojans, exploits and hoaxes are created and released in the world every year. Many of these are simple programs that are easily stopped by most good anti-virus software. These are typically written by amateur programmers and released as a prank or joke, but have spread further than imagined. A growing number of these, however, are highly sophisticated and cleverly designed programs created by professional "hackers" and are released with the intention to create widespread damage or havoc.

The problem with many of these viruses is that effective prevention, detection and disinfection is often impossible until it has been active for awhile. The "Melissa" virus is a perfect example of how a cleverly written virus can become widespread before effective defensive can be created and distributed.

### **Common Virus Entry Points**

The first question that people often ask themselves is: How did this virus get into my computer, or attack it? Knowing the answer to this question can often prevent infection by protecting the possible virus entry points.

Here are the most common entry points used by viruses:

*Removable disk drives*

*Computer networks*

*Internet*

**Removable Disk Drives:** Disk drives are storage devices on which data is stored in the form of files or documents. These disk drives enable documents to be created on one computer and then used on another. Among these types of storage devices are: floppy disks, CD-ROMs, and Zip and Jaz disks. The last two types are simply special disks with a larger capacity than floppy disks. If any of these are

infected, the other computers on which they are used will be infected. E-mail messages can also be stored in these storage devices, which may also be infected. Floppy disks (or other extractable disks) can store programs, files, Web pages (HTML), e-mail messages with attached files, compressed files, etc. Any of these elements could be infected. Similarly, what is known as the boot sector of the disk could also be infected with a boot virus. Although it still happens, infections produced from floppy disks have decreased significantly to 10%. This means of spreading viruses has given way to much quicker means of propagation, such as e-mail.

Although in general CD-ROM drives can only read the content of a disk but cannot write on them, nowadays it is possible to read and write (record) on a CD-ROM. This, along with the large quantity of information that they can store has led to a large number of infections. In addition, many computers can be booted from a CD-ROM. This option can also lead to an increase in the number of infections.

**Computer Networks:** A network is a group of interconnected computers that makes it easier for groups of people to work together. Each computer that forms part of the network can connect to all other networked machines. Through this system it is possible to transfer information from one computer to another and/or access the information stored in one of them from the rest. If the information (programs, files, documents, etc.) that is accessed or transferred from one computer to another are infected, the computers that accessed this computer, or those involved in the transfer, could also be infected.

The network connections can be local and/or remote, allowing computers and laptops to connect via cable, an Intranet, modem, etc. In short, this means that the network can be accessed from several points. You only need to consider a single computer and the means through which a virus can enter it, then multiply this by the computers in the network and mobile machines (such as laptops) that can connect to this network in order to get an idea of the myriad ways through which viruses can enter a network.

**Internet:** The Internet is becoming an increasingly popular means of obtaining information, sending and receiving files, sending and receiving news, or downloading files. All of these operations are based on transferring information and the interconnection of millions of computers all over the world. This means that as well as data, you may well be receiving a hidden virus. This simple fact alone has allowed virus attacks to grow at an unprecedented rate and has currently made The Internet the biggest virus entry point. Infection via Internet may be produced through a number of different means, including the following:

*E-mail*

*Web pages*

*File transfers (FTP)*

*Downloads*

*Newsgroups*

**E-mail:** Documents and files can be sent and received via e-mail in the form of attachments. These files could be infected. When an e-mail message is opened and the file it contains is run or opened, the computer that has received the message will become infected. The most important characteristics of infection via e-mail are as follows:

*Increased replication and propagation capacity.* The virus can spread to thousands of computers throughout the world in just a few minutes.

*Storage of messages.* Messages are stored in a special database (for example, PST files), which are difficult to scan using an antivirus program that is not designed specifically for e-mail systems.

*Increased connection capacity.* It is possible to send and receive messages between any types of computers/platforms.

Every day, millions and millions of e-mail messages are exchanged throughout the world. The time that it takes to reach the recipient is minimal. In addition, an e-mail message can be sent to a large number of recipients at the same time. This makes e-mail particularly popular with virus authors: It is an extremely fast way of spreading and reaching a large number of recipients. In addition, viruses can nowadays produce an infection and have the capacity to send themselves to other computers without the affected user realizing. In this case, the recipients of the virus could be all of the people included in the e-mail Address Book of the infected computer.

In most cases, infections transmitted via e-mail are not carried out when the message is opened, but on opening or running an infected file included in it. There are exceptions, however. Some viruses, the minority, can carry out their infection when the mail message is opened (without the attached file needing to be executed).

In order to avoid infection via e-mail, the following advice should be considered:

*Install an antivirus product that is designed to scan e-mail.*

*Do not open suspicious files, messages from unknown senders, messages which contain strange texts, etc.*

*Do not run or open files included in suspicious mail messages.*

*If you think a message may be infected, delete it and inform the sender.*

**Web Pages:** The majority of pages visited in Internet are text files or images written in a language known as HTML. However, they may also contain programs known as ActiveX controls and Java Applets. These may be infected and therefore infect the visitor to that page. If one of these pages includes a virus in HTML code that includes sections of dynamic code (which executes programs, or carries out certain operations), you could become infected simply by visiting the page. When browsing Web pages, any flaws in your browser can be exploited through ActiveX Controls, Java Applets, HTML code and/or JavaScript, as well as through other methods. All of these can enable viruses to 'sneak' into a computer.

**File Transfers (FTP):** The term FTP stands for File Transfer Protocol. Through this protocol it is possible to place documents (upload) on any computer in the world or copy files from any computer to your own (download). When a file is downloaded, it is copied directly from a certain place to your computer. The downloaded files

could, of course, contain a virus that would infect your computer. Some of the most common operations carried out by users on the Internet are downloading programs (shareware), documents, etc.; in addition to downloading software from specific sites. For this reason, it is very important that you only download files from sites that offer guarantees.

**Downloads:** although downloading files from Internet is similar to file transfer (FTP), it is not the same. Through FTP you can upload as well as download files, whereas through downloads you can only obtain files (which will be copied from a website to your computer). Although in general, these downloads are safe and virus free, it is possible that the downloaded file could be infected. There are some sites that are specially prepared for downloading software or IT utilities.

**News or Newsgroups:** Through this service it is possible to debate a topic with anyone in the world or receive e-mails featuring the latest information on a topic of your choice. These newsgroups work in a similar way to a notice board. Users post their comments, doubts, or notes about certain topics and other users can respond, give their opinion, clear up doubts, etc. These messages could contain an infected document that could install a virus in your system. With newsgroups you run the same risk of virus infection as you do with e-mail. When you connect to a newsgroup, files containing the recent articles are downloaded (in the same way as e-mail). These files could also be infected.

### **Where Do Viruses Hide?**

Viruses make use of a number of different places in order to 'hide' from antivirus products and use different techniques to do so. These hiding places include the following:

**Main memory:** In this case the virus is automatically placed in the main memory (RAM memory) where it waits for a program to be run (a file with an EXE or COM extension) in order to infect it. This type of virus is known as a resident virus.

**Documents containing macros:** In general, non-program files are not infected by any type of virus. However, there are certain types of documents (files) that users can create or use in their day-to-day activities that contain what are known as macros. A macro is a set of instructions or operations that another program can carry out. These macros form part of documents (text, spreadsheet or database documents), and as they are programs they can be infected by viruses (Macro viruses).

**Boot sector (Boot and Master Boot):** The boot sector of a floppy or hard disk contains information on the characteristics and contents of the disk. When we refer to the boot sector of a floppy disk, we use the term BOOT, whereas the term MASTER BOOT (MBR - Master Boot Record) is used to refer to the same section of a hard disk. This section of a disk may also contain a program that makes it possible to boot (start) the computer. Some viruses, known as Boot viruses, infect this program, thereby ensuring that they are run every time the computer is booted from the infected disk.

Files attached to e-mail messages: E-mail is being used on an ever-increasing scale as a way of exchange files. These files (attached files or attachments) accompany the text message that is sent and could be infected. Users generally do not suspect that these files could contain a virus, but on opening the message and the attached file they could get a nasty surprise.

Internet Web Pages: Web pages that are visited while browsing the Internet are files that in theory should not be infected, as they are text documents (containing text, images and sound). However, they may contain other components known as Java Applets or ActiveX Controls, which are programs that give the web page a more dynamic appearance, better services and features. Like all other programs, they may be infected and thereby infect users that visit pages containing these components.

### **Symptoms of Infection**

This section will classify and describe each of the symptoms that may be noticed when a virus, worm or Trojan carries out its infection or is activated in a computer.

[File Recovery Tool](#)

We are going to start by establishing criteria for classifying the level of damage that viruses could carry out in your computer:

No damage. In this case, viruses do not carry out any action after infecting the computer. The objective of these viruses is usually to propagate and infect other elements and/or computers (they send themselves by e-mail, IRC or through a network).

Minimum damage. They only carry out actions that annoy the user, without affecting data integrity or other areas of the computer (display messages on screen, animations, etc).

Moderate/slight damage. In this case, there may be slight changes to files or loss of data, but the actions will never be totally destructive (some files or part of their content may disappear). The actions carried out by the virus will be repairable.

Serious damage. Loss of large quantities of data and/or files. However, it will be possible to recover part of the data, although the process may be rather complicated and tedious.

Very serious damage/irreparable. In this case, all of the data that the infected disk drives contain may be lost (including network drives). The structure of each disk drive may also be lost (at least the structure of the main drive), because a virus has reformatted it. This damage is very difficult to repair and is in some cases irreparable. In addition, other memory systems will also be attacked such as the RAM, CMOS and BIOS, as well as boot systems and system files.

Unpredictable damage. This damage is usually caused by Trojans. Trojans are programs that can be handled remotely (from another computer) by the person that is launching the attack (attacker or hacker). This type of program is becoming more and more complex and has more attack utilities and functions. Through the client program -in the attacker's computer-, the server program -in the victim's computer- and a connection through the communications port of the victim's computer, the attacker can carry out any action in the victim's computer.

Some of the symptoms or effects that could be observed in a computer, when a virus has carried out its infection or when it has been activated (depending on the trigger conditions), are as follows:

Note: it is important to bear in mind that the symptoms described below may be due to causes other than viruses.

Slow down. The computer operates much more slowly than usual. It takes a lot longer to open applications or programs. Even the operating system takes longer to carry out simple operations that do not usually take so long.

Run /Open. When you try to start a certain program or open a specific file, it will not run or open.

Disappearance of files and folders. The files stored in certain directories (usually those which belong to the operating system or certain applications), have disappeared because the virus has deleted them. Entire directories and folders may also disappear.

A Trojan called Backdoor/Acid.1.0 pretends to delete files from the Windows folder

Impossible to access the content of files When a file is opened an error message may be displayed or it may simply be impossible to open it. A virus could have modified the File Allocation Table resulting in the loss of the addresses which are the starting point for locating files.

Unexpected or unusual error messages. Dialog boxes display absurd, humorous, spiteful or aggressive messages, which do not appear under normal circumstances.

A message displayed by a worm called W32/Music

Decrease in memory and hard disk space The free space on the hard disk significantly decreases. This could indicate that a virus has infected a large number of files and that it is spreading throughout the computer. When a program is run, a message appears indicating that there is not sufficient memory to do so (although this is not true and there are few programs open).

Defective Sectors. A message informs you that there are errors on part of the disk that you are working with and a file cannot be saved or it is not possible to perform

a certain operation.

**Change in the file properties** The virus modifies some or all of the characteristics of the file that it infects. As a result, you will notice that the date/time associated with the file (when it was created or last modified) is incorrect, its properties have been modified, the size has changed (when this should not have happened), etc.

**Operating System errors** When certain operations are carried out - normal and supported by the operating system in other situations - error messages are displayed, other unsolicited actions are carried out or nothing happens.

**Duplicate files** If there is a file with an EXE extension and another with the same name but with a COM extension (also a program), the file with the COM extension will be a virus. Viruses do this because if there are two files with the same name the operating system will always run the file with the COM extension first.

**Renamed files.** A virus will have changed the names of the files that it has infected and/or other specific files.

**Problems starting the computer.** The computer will not start, or does not start up in the usual way. It is advisable to start the computer using a system or boot disk and scan all areas of the computer using an antivirus in command-line.

**Computer blocks.** In situations in which there are few programs open (or none) and there is not a heavy load on the system, the system blocks (it 'crashes') and prevents you from working. It is necessary to use the key combination CTRL+ALT+SUPR in order to remove the task that has blocked or to restart the computer.

**The computer shuts down/restarts.** Whilst you are working with the computer as usual and without carrying out any strange operations, the computer automatically shuts down and restarts. Obviously everything that has not been saved will be irretrievably lost.

**The program shuts down.** Whilst you are working with an application or program it shuts down even though you have not performed any unexpected operations or done anything that could produce this action.

**The CD-ROM tray opens and closes.** The tray of the CD-ROM drive opens and closes without user intervention. This action is very typical of Trojans.

The keyboard and/or mouse do not work correctly When you use the keyboard, it does not write what you want or it carries out operations that do not correspond to the keys that you have pressed. In addition the mouse pointer moves around the screen independently, without you moving it (or when you do, it carries out unusual activities).

Sections of windows disappear. Certain sections (buttons, menu options, texts, etc.) that should appear in a particular window have disappeared and are not displayed. In addition, in windows in which nothing should appear, strange icons or unusual content appears (for example in the Windows taskbar, next to the system clock).

Icono displayed on the task bar by a worm called W32/Navidad.DB

If you have noticed any of these symptoms in your computer, it is advisable to scan it using a good antivirus solution that is completely up to date. You can download either of the two antivirus solutions from the links below:

[Panda Antivirus Titanium](#)

[Panda Antivirus Platinum](#) [What is a Virus?](#)

[Entry Points](#)

[Where Do Viruses Hide?](#)

[Types of Virus](#)

[Symptoms of Infection](#)

[Techniques Used By Viruses](#)

[Antivirus Techniques](#)

[Start](#)

[Techniques used by Viruses](#)

Each one of the many thousands of existing viruses uses different techniques both to carry out their infection routine and to conceal their presence from the eyes of users. These techniques change and evolve over time, as do the techniques used by antivirus programs to detect them. This section focuses on the most common mechanisms used by viruses:

[Stealth](#)

[Tunneling](#)

[Self-encryption](#)

[Polymorphism](#)

[Armoring](#)

**Stealth:** Viruses that use this method in order to conceal their presence from the eyes of users in order not to raise suspicion and to trick them into believing that nothing untoward has happened. This technique is mostly used by resident viruses, although it may also be used by other types. In addition, there are several types of stealth techniques; 'stealth' is a generic term for this kind of technique. However, antivirus programs also use special anti-stealth techniques in order to detect this type of virus.

When a virus infects a file, it leaves a series of tell-tale signs such as an increase in the size of the infected file, changes in the file's date and time stamps, sections of file code marked as being defective, reduction of available memory, etc. This type of virus makes sure that these traces cannot be seen by the user. To do this, it checks all requests made by the operating system for information related to these characteristics, intercepting them and offering false information instead of the real data. The viruses that use stealth techniques usually carry out certain actions so that their effects are not evident. These actions include the following:

The size of the file will increase when it is infected, as the virus is inserted inside it. However, this type of virus prevents the new file size from being displayed in order not to arouse suspicion.

When they infect a file, they do not modify the date or the time. This means that they will not assign the file to show the date and time the file was last modified (when the infection was carried out).

If they go memory resident, they usually place themselves over the first 640 Kbytes.

If the viruses are capable of over-writing write-protected sections of a disk, they prevent write-protect error messages from appearing.

**Tunneling:** This is a technique specifically designed to prevent the correct use of the permanent (resident) antivirus protection installed on a computer. While the permanent antivirus protection works to detect the presence of viruses in the system, this type of virus works against it. The antivirus analyzes all file operations performed on the computer by intercepting the actions the operating system carries out. However, if the virus intercepts these requests first, the antivirus will not detect the presence of the malicious code. Fortunately, antivirus techniques have been developed that permit the detection of viruses that use this technique.

The tunneling system is quite complicated, as the microprocessor must be put in step-by-step mode and work with interrupts. In addition, this type of virus is capable of obtaining the memory address in which the operating system services are originally located. This allows it to use these types of services without intercepting those used by other programs.

**Self-encryption:** antivirus programs search for strings of characters (known as the virus signatures) which all viruses have. Viruses therefore use a technique known as self-encryption, which enables them to take on a different appearance each time they infect (polymorphic). This means that the virus will use a specific string to carry out one infection and a different one in the next. In addition, they encode or encrypt their strings to make it more difficult for the antivirus program to detect them. However, the viruses that use this technique always use the same encryption routine (or algorithm), which makes it possible for antivirus programs

to detect them.

To summarize, using an encryption key and a series of mathematical operations, the virus can encrypt itself. This makes it difficult for the virus to be decrypted in order to be scanned and/or detected. The virus can also decrypt itself. In general they use the same key for encryption and decryption.

**Polymorphism:** Based on the self-encryption technique, polymorphic viruses encrypt their code in a different way with each infection they carry out (their signature changes from one infection to the next). If this were the only thing they were capable of, we would be referring to viruses that use encryption. However, these viruses also encrypt the way (routine or algorithm) in which their signature is encrypted. This means that a polymorphic virus is capable of creating different variants of itself from one infection to the next, changing its "shape" with each infection. The encryption operations are usually carried out through XOR (OR-Exclusive) operations, where  $a \text{ XOR } b = a'b + ab'$ .

In order to detect this type of virus, antivirus programs use decryption simulation techniques. The antivirus programs try to locate the viruses by searching for their signature or pattern (string of characters unique to each virus). If the virus is encrypted and its encryption changes every time it infects, it will be very difficult to detect.

However, the virus cannot completely encrypt itself, as it needs to keep part of its code (not encrypted) in order to decrypt itself. This section is used by antivirus programs to detect polymorphic viruses. In order to do this, the antivirus program will try to locate the routine or algorithm that allows the virus to automatically decrypt itself.

**Armoring:** Through this technique, viruses prevent their code from being examined. In order to find out more about a virus, analysts look into files using special programs called Debugger, which allow them to examine each line of the virus code in the original language it was written in. Viruses that use the 'Armoring' technique make it impossible for their code to be read.

To sum up, a virus prevents its code from being examined, by making it impossible to disassemble or trace it. This is where the name 'armoring' comes from. However, there are antivirus programs that use heuristic techniques to detect this type of virus.

What is a Virus?

Entry Points

Where Do Viruses Hide?

Types of Virus

Symptoms of Infection

Techniques Used By Viruses

## Antivirus Techniques

### Start

## Antivirus Techniques

As the techniques used by viruses evolve and are studied in depth in virus labs all around the world, antivirus programs are incorporating increasingly advanced technology that makes it possible to detect viruses and protect users against these menaces. The following are the most used:

String search

Deductive search

Exceptions

Heuristic scan

Permanent protection (Resident)

Vaccination

Research

**Strings search:** Every virus contains a string of characters that uniquely and unequivocally identifies them (as if it were their fingerprint). This is known as the virus signature. Antivirus programs include a file known as the Virus Signature File, which contains all of the strings that correspond to each virus that they can detect. This means that when an antivirus scans in search of viruses, what it is doing is looking for these strings in the files it has been instructed to scan. If a file does not contain any of these strings, then it is considered to be virus-free, whereas if the antivirus detects one of the strings in a file it informs the user that it may be infected.

This means that the antivirus programs must search for these strings in small specific sections of the file. They must also be aware that there may be two variants of the same virus with the same string or that new viruses may appear and whose strings are still not known. This makes it important for antivirus programs to combine the 'string search' technique, with other more accurate techniques.

**Deductive search:** As at times the string search mentioned above may not be completely reliable, antivirus programs also use other techniques. One of them, which is very similar to the string search, is the deductive search. This involves observing certain properties in each file that is scanned. There are certain properties that infected files will always have. When the deductive search detects one of them, it will confirm that the file is infected. This type of search takes the internal structure of the files that it scans into account, the date, the time and the attributes of the file (read-only, write, system, hidden, etc.).

**Exceptions:** An alternative to the string search and the deductive search method is to search for exceptions. When a virus uses a different string (signature) from one infection to another it becomes difficult to detect by means of the string search

method. If this happens, the antivirus program will search for a specific virus.

Heuristic scan: When there is no information available to permit the detection of a new or unknown virus, the Heuristic technique is used. This consists of scanning files and gathering a series of data from them (size, date and time of creation, etc.). This information is studied by the antivirus program which, depending on the results obtained, concludes whether a file may harbor a potential virus or not.

Due to its large scanning capabilities and suspicion of strange situations, this type of antivirus technique could result in false alarms that refer to possible viruses, when they do not actually exist. This is due to the fact that this technique examines sections of the file that have unusual characteristics or carry out unusual functions.

Some antivirus programs include the option to carry out a scan using this technique if the user requires it. If this is the case, the antivirus program will carry out its usual scans and will then apply the heuristic scan in the following way:

It accesses the code of the program to be scanned.

It runs it step-by-step. In other words, it runs each line of code, one by one.

It detects possible activity that, in theory, the program being scanned should not carry out, or modifications that the file being scanned should not have.

If it detects suspicious activity, it alerts the user. It informs the user that it could contain a virus or that there are significant or unusual changes to the file being scanned.

To sum up, this type of scan can detect both known and unknown viruses. This is because the scan is not based on the characteristics of a particular virus but on the characteristics that all viruses have in common (all viruses use similar groups of techniques that can be detected).

It is advisable to be cautious with the results of the heuristic scan. This means that you should consider what you are going to do as a consequence. There are some antivirus applications (such as Panda Antivirus Titanium) that allow you to send suspicious files to be examined by experts (Virus Laboratory). If a heuristic scan detects a suspicious file, through Panda Antivirus Titanium you can send it to Panda Software, so that it can be examined. You will quickly receive a reply and the corresponding solution if necessary.

Permanent protection (Resident): Although it is not a technique as such, the majority of antivirus programs offer this feature. Whilst the computer is switched on, the antivirus program will scan all of the files involved in all of the operations

carried out (in the system and via Internet). The antivirus places its scan program in memory, and when files are opened, closed or run etc, the program will scan them. When a virus is detected, a warning is displayed and you are offered the possibility of disinfecting the virus. If nothing out of the ordinary is found, the scan process continues.

Therefore, it could be said that the permanent protection constantly observes everything, without user intervention. This significantly reduces the risk of infection, as the antivirus program constantly scans any area of the computer which is carrying out operations and prevents infected files or programs from being run.

Although it is always advisable to have the permanent protection enabled, there are antivirus programs that give the user the option of enabling or disabling it. In addition, the characteristics of this protection can also be configured (elements to be scanned, action to be taken if a virus is detected, elements that should not be scanned, the antivirus alerts, etc).

**Vaccination:** By means of this technique, the antivirus program stores information on the characteristics of each files that has been scanned (the files are vaccinated). If in subsequent scans a difference is detected between the information stored and the current file information, the antivirus program will inform the user of this difference. This technique helps the file to be reconstructed, if it has been infected.

There are two types of vaccine:

**Internal (inoculation).** The information is stored within the file itself, which means that when it is executed it automatically checks for any changes.

**External.** Information is stored in a specially created file, which the program uses to check against the information obtained in the current scan.

**Research:** There are viruses that may get into the memory of the computer (RAM) and activate themselves. These viruses may not be detected by the normal memory scan. The research mechanism consists of 'provoking' the virus into attempting to carry out an infection. Through this mechanism, new viruses can be discovered and the tricks that they use to carry out their infection can be identified. Therefore, the virus can be detected. If a virus is detected, the antivirus program will have to consider what actions it should carry out and how it should do it.

What is a Virus?

Entry Points

Where Do Viruses Hide?

Types of Virus  
Symptoms of Infection  
Techniques Used By Viruses  
Antivirus Techniques

### **Antivirus Techniques**

As the techniques used by viruses evolve and are studied in depth in virus labs all around the world, antivirus programs are incorporating increasingly advanced technology that makes it possible to detect viruses and protect users against these menaces. The following are the most used:

[Undelete File](#)

String search  
Deductive search  
Exceptions  
Heuristic scan  
Permanent protection (Resident)  
Vaccination  
Research

String search: Every virus contains a string of characters that uniquely and unequivocally identifies them (as if it were their fingerprint). This is known as the virus signature. Antivirus programs include a file known as the Virus Signature File, which contains all of the strings that correspond to each virus that they can detect. This means that when an antivirus scans in search of viruses, what it is doing is looking for these strings in the files it has been instructed to scan. If a file does not contain any of these strings, then it is considered to be virus-free, whereas if the antivirus detects one of the strings in a file it informs the user that it may be infected.

This means that the antivirus programs must search for these strings in small specific sections of the file. They must also be aware that there may be two variants of the same virus with the same string or that new viruses may appear and whose strings are still not known. This makes it important for antivirus programs to combine the 'string search' technique, with other more accurate techniques.

Deductive search: As at times the string search mentioned above may not be completely reliable, antivirus programs also use other techniques. One of them, which is very similar to the string search, is the deductive search. This involves observing certain properties in each file that is scanned. There are certain properties that infected files will always have. When the deductive search detects one of them, it will confirm that the file is infected. This type of search takes the internal structure of the files that it scans into account, the date, the time and the attributes of the file (read-only, write, system, hidden, etc.).

Exceptions: An alternative to the string search and the deductive search method is to search for exceptions. When a virus uses a different string (signature) from one infection to another it becomes difficult to detect by means of the string search

method. If this happens, the antivirus program will search for a specific virus.

Heuristic scan: When there is no information available to permit the detection of a new or unknown virus, the Heuristic technique is used. This consists of scanning files and gathering a series of data from them (size, date and time of creation, etc.). This information is studied by the antivirus program which, depending on the results obtained, concludes whether a file may harbor a potential virus or not.

Due to its large scanning capabilities and suspicion of strange situations, this type of antivirus technique could result in false alarms that refer to possible viruses, when they do not actually exist. This is due to the fact that this technique examines sections of the file that have unusual characteristics or carry out unusual functions.

Some antivirus programs include the option to carry out a scan using this technique if the user requires it. If this is the case, the antivirus program will carry out its usual scans and will then apply the heuristic scan in the following way:

It accesses the code of the program to be scanned.

It runs it step-by-step. In other words, it runs each line of code, one by one.

It detects possible activity that, in theory, the program being scanned should not carry out, or modifications that the file being scanned should not have.

If it detects suspicious activity, it alerts the user. It informs the user that it could contain a virus or that there are significant or unusual changes to the file being scanned.

To sum up, this type of scan can detect both known and unknown viruses. This is because the scan is not based on the characteristics of a particular virus but on the characteristics that all viruses have in common (all viruses use similar groups of techniques that can be detected).

It is advisable to be cautious with the results of the heuristic scan. This means that you should consider what you are going to do as a consequence. There are some antivirus applications (such as Panda Antivirus Titanium) that allow you to send suspicious files to be examined by experts (Virus Laboratory). If a heuristic scan detects a suspicious file, through Panda Antivirus Titanium you can send it to Panda Software, so that it can be examined. You will quickly receive a reply and the corresponding solution if necessary.

Permanent protection (Resident): Although it is not a technique as such, the majority of antivirus programs offer this feature. Whilst the computer is switched on, the antivirus program will scan all of the files involved in all of the operations

carried out (in the system and via Internet). The antivirus places its scan program in memory, and when files are opened, closed or run etc, the program will scan them. When a virus is detected, a warning is displayed and you are offered the possibility of disinfecting the virus. If nothing out of the ordinary is found, the scan process continues.

Therefore, it could be said that the permanent protection constantly observes everything, without user intervention. This significantly reduces the risk of infection, as the antivirus program constantly scans any area of the computer which is carrying out operations and prevents infected files or programs from being run.

Although it is always advisable to have the permanent protection enabled, there are antivirus programs that give the user the option of enabling or disabling it. In addition, the characteristics of this protection can also be configured (elements to be scanned, action to be taken if a virus is detected, elements that should not be scanned, the antivirus alerts, etc).

**Vaccination:** By means of this technique, the antivirus program stores information on the characteristics of each files that has been scanned (the files are vaccinated). If in subsequent scans a difference is detected between the information stored and the current file information, the antivirus program will inform the user of this difference. This technique helps the file to be reconstructed, if it has been infected.

There are two types of vaccine:

**Internal (inoculation).** The information is stored within the file itself, which means that when it is executed it automatically checks for any changes.

**External.** Information is stored in a specially created file, which the program uses to check against the information obtained in the current scan.

**Research:** There are viruses that may get into the memory of the computer (RAM) and activate themselves. These viruses may not be detected by the normal memory scan. The research mechanism consists of 'provoking' the virus into attempting to carry out an infection. Through this mechanism, new viruses can be discovered and the tricks that they use to carry out their infection can be identified. Therefore, the virus can be detected. If a virus is detected, the antivirus program will have to consider what actions it should carry out and how it should do it.

### **Types of Virus**

Viruses can be classified according to certain characteristics. Depending on these characteristics some viruses belong to a specific group but others could be included in several groups. Some of the criteria considered when classifying viruses are as

follows:

Means through which they carry out their infection.

Techniques they use to infect.

Techniques they use to hide and avoid antivirus programs.

Types of file that they infect.

Place where they hide after infecting.

Platform or operating system that they attack.

Actions that they carry out.

In addition, there are other characteristics used to classify viruses in other groups (means of propagation, trigger condition,... etc).

Although many of them have a very special feature that clearly associates them to one particular virus type, others may fall into several different categories.

Below is a list of groups that classify some of the most common types of viruses:

File Infectors

Resident Viruses

Direct Action viruses

Overwrite viruses

Companion viruses

Boot viruses

Macro viruses

Worms

Trojans (Trojan Horses)

Logic Bombs

Encrypted

Multipartite

Resident

Polymorphic

**File Infectors:** This type of virus infects programs or executable files (files with an EXE or COM extension). When one of these programs is run, directly or indirectly, the virus is activated, producing the damaging effects it is programmed to carry out. The majority of existing viruses belong to this category, and can be classified depending on the actions that they carry out.

**Resident Viruses:** When this type of virus is executed or activated, the first thing it does is check if a series of pre-established conditions have been met (date, time, etc) in order to launch its attack. If these conditions have not been met, the virus will lie in wait in the main memory (RAM memory) for a program to be executed. It will occupy 200 to 5000 Bytes of memory. If an executable file (program) that is not infected is used during one of the operations carried out by the operating system, the virus will infect it. In order to do this, the virus adds its own malicious code to the original file code.

This type of virus can be treated as a file infector virus. When the virus goes memory resident, it will try and remain there until the computer is switched off or restarted (as this type of memory is volatile -its content is lost when the power source is shut off-). Some of these viruses modify the system configuration (in the Windows Registry, for example), in order to ensure that it goes memory resident every time the computer is switched on or restarted.

Once it is resident, it will intercept certain operating system services. These services may be used by the programs whilst they are running. This means that resident viruses could intervene in the operations carried out by the programs that are running at a given time. This result is that the virus can modify the services needed by the program, so that they point to or run parts of the virus code. As a result the resident virus will be run whenever a program needs and accesses the operating system services.

This type of virus can also belong to any of the other above mentioned types. Its main characteristic is that it loads itself into the RAM memory upon execution. Once the virus has gone memory resident it will be able to control and intercept all the programs executions or other actions carried out on by the operating system. This way, it will be able to infect all the files that are opened, closed, renamed or copied,...etc.

Resident virus

These viruses remain memory resident until they somehow disappear from it. Occasionally, it is possible to cancel the process by pressing the CTRL+ALT+SUPR keys simultaneously. As we mentioned before these viruses load themselves into the RAM memory, so they will disappear when the computer is switched off or

rebooted. The reason for this lies in the fact that the RAM memory is volatile (it loses its contents when the power is turned off). However there are certain viruses that manage to load themselves into memory when the computer is started up. These viruses can carry out its ations when the trigger condition is met straight away, or they can remain in memory permanently until the trigger condition is met.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the descriptions of a large number of these viruses.

AntiCMOS AntiEXE Barrotes  
Viernes 13 Babylonia CIH (Chernobyl)

**Direct Action Viruses:** As soon as the virus is executed, it will try to replicate, or reproduce itself. This means that it will create copies of itself. When certain specific conditions are met, the virus will go into action and infect files in the directory or folder that is in use and in the directories that are specified in the AUTOEXEC.BAT file PATH. This batch file is always located in the root directory of the hard disk and carries out certain operations when the computer is booted. Files infected with this type of virus can be disinfected, returning them to their original status.

These viruses can also be considered file infector viruses as they search for files in order to infect them. The reason why these viruses try to replicate is because they are not resident and therefore will not be running in memory. This means that they have to replicate and carry out their actions every day.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Aristotle Intruder W32/HTM.H4  
Trojan/Win32.TPS VBS/ColdApe.A W98/Corvinus.A

**Overwrite Viruses:** This type of virus is characterized by the fact that it does not respect the information contained in the files that it infects, rendering them useless once they have been infected. There are some overwrite viruses that are resident and others that are not. Although they can be disinfected, it is impossible to recover the infected files, meaning that the only alternative is to delete them. This type of virus is a file infector virus.

A notable feature of these viruses is that the size of the files infected by an overwrite virus does not increase, as the virus does not occupy more space than the infected file. This is because the virus places itself over the content of the infected file, it is not added to the content of the file.

The result of an infection by this type of virus is partial or total loss of the content

of the file, which is impossible to recover.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Trivial.37.D Trivial.88.B Trivial.88.D  
Ulodozen

Companion Viruses: companion viruses can be considered file infector viruses as well as resident or direct action. They are known as companion viruses because once they get into the system they "accompany" the other files that already exist. In other words, in order to carry out their infection routines, companion viruses can wait in memory until a program is run (resident viruses) or act immediately by making copies of themselves (direct action viruses).

Unlike overwrite or resident viruses, companion viruses do not modify the files that they infect. When the operating system is working (running programs) the operating system may have to call up a specific program. If there are two executable files with the same name but with different extensions (one with an EXE extension and the other with a COM extension), the operating system will run the COM file first. Companion viruses take advantage of this characteristic of the operating system.

If there is an EXE file with a specific name, the virus will create another executable file with the same name but with a .COM extension, in order to hide itself from the user and avoid arousing suspicion. The file that is created will contain the virus itself. When the operating system finds two files with the same name, it will execute the file with the .COM extension first, thereby executing the virus. Once the virus has been executed, it hands the control back to the operating system so that it can run the original EXE file. This way the user will not know that the virus has carried out its infection. To be more precise, a companion virus will follow the steps below:

It chooses a specific file with an .EXE extension to infect.

It creates a file with the same name but with a .COM extension.

It includes itself in the file with the .COM extension (this will be the virus itself).

It hides the file that it has just created (the .COM file), in order not to arouse suspicion.

From that moment on, whenever the original EXE file is run, the following will happen:

The operating system will try to run the file with the EXE extension.

The operating system will realize that another file with the same name exists, but with a .COM extension.

The operating system will run the file with the .COM extension. This is the virus.

For these reasons, companion viruses may have different formats: :

Companion Viruses in MS-DOS. These viruses take advantage of the MS-DOS command interpreter that runs COM files before EXE files (if there are two files with the same name, one with a .COM extension and another with an EXE).

Companion Viruses in Windows. These viruses work in a similar way to companion viruses in MS-DOS. The only difference is that these viruses do not create a file with a COM extension and with the same name as the victim file. These viruses change the extension of the victim file from EXE to COM. Then, the virus goes memory resident and infects all of the programs that are run.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

DeDouble Little Brother W95/HLLC.4096.C

Boot Virus : This type of virus affects the Boot sector of a floppy or hard disk. This is a crucial part of a disk, in which information on the disk itself is stored together with a program that makes it possible to boot (start) the computer from the disk.

This kind of virus does not affect files, which means that the contents of an infected disk are safe as long as you do not attempt to boot the computer using that disk. If this happens, the virus will infect the computer in the following way:

It hides in a specific sector of the infected disk.

It reserves a place in memory so that no other programs will be able to occupy it.

It copies itself to this zone reserved in the memory.

From this position in the memory, it will intercept the operating system services.

From then on the following will happen:

Whenever an operating system application calls a function to access files, the virus takes control.

It checks if the disk that it accesses is infected. If it is not, it will infect it.

The virus replaces the original boot sector (without infecting it).

It modifies the original boot sector, writing its viral code to it.

By doing this, the virus passes the control to the operating system. Therefore it will seem that nothing has happened. However, the virus will continue to act.

Boot virus infections are usually carried out through floppy disks. The best form of protection against this happening is to write-protect all floppy disks.

If a floppy disk infected with a Boot virus were inserted in the disk drive of a computer, the infection could spread to the hard disk. In this case, the MBR (Master Boot Record) of the hard disk (or of the hard disks) of the computer would be infected. This means that any type of disk (floppy, CD-ROM, Zip, Jazz, etc.) used in the infected computer would also become infected.

These viruses save a copy of the original Boot sector, but each virus may do this in a completely different way. Some will copy them to a specific sector of the disk and mark it as faulty. Others store it in a section of the disk that already contained information (making it impossible to recover this information). Finally, the most aggressive or dangerous overwrite the original boot sector, preventing the computer from being booted using that disk.

The best way of avoiding boot viruses is to ensure that floppy disks are write-protected (whenever you do not need to write on them).

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Anti-Telefónica CMOS.Erase Cruel  
Diablo Empire Form  
Michelangelo Parity Boot Tequila

**Macro Viruses:** Unlike the viruses we have mentioned so far, which infect programs (EXE or COM files) or applications, macro viruses infect the files (documents, workbooks, presentations and/or databases) that are created using certain applications or programs. Each of these file types may incorporate small programs known as macros. A macro is a small program that a user can associate to a file created using certain applications. They do not depend on the operating system, but rather on specific actions carried out by the user of a document containing macros. These mini-programs make it possible to automate series of operations so that they are performed as a single action, thereby saving the user from having to carry them out one by one.

These macros could become infected, this means that they could be the target of viruses (more specifically macro viruses). In this case, when a document containing macros is opened, they will automatically be loaded and may be

executed immediately or when the user decides to do so. The virus will then (or at a later stage) take effect by carrying out the actions it has been programmed to do. Contrary to popular belief, macro viruses are capable of producing great damage and of spreading extremely quickly.

In addition, these viruses can infect the global template (through the macros) that the tools (word processor, spreadsheets, etc.) use. On opening a document, spreadsheet or database with an infected template, the document will become infected. This is the most common method used by macro viruses to spread their infection.

As we have already mentioned, this type of virus affects documents, spreadsheets or workbooks, databases and/or presentations containing macros. Therefore, the target of this type of virus will be files created with tools that allow macros to be used. This means that there is not just one type of macro virus, but one for each tool: Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Access, Corel Draw, Lotus Ami Pro, etc.

Microsoft Word macro viruses

Microsoft Excel macro viruses

Microsoft Access macro viruses.

Microsoft PowerPoint macro viruses

Multipartite Macro viruses

.RTF file macro viruses

Lotus Ami Pro macro viruses.

Corel Draw macro virus.

However, not all programs or tools that allow macros to be used will be targeted by this type of virus. The tools that are attacked by macro viruses have to meet a certain criteria:

The macros can be transported (through any of the regular means of propagation) from one computer to another, as they are included in the infected file (document, spreadsheet, presentation, database, etc.).

The macros created and incorporated in one file can be obtained, included and used in others.

The macros can be automatically run (when a file is opened or closed, for example), without user intervention.

These are the most common types of macro viruses:

Microsoft Word macro viruses. These are the most common viruses nowadays. Their targets are text documents created and edited with Microsoft Word (DOC files). For identification purposes, their names usually include the following prefixes: WM (Word 6.0 and/or Word 95 macro virus), W97M (Word 97 macro virus) or WOOM (Word 2000 macro virus). In addition to the automatic macros, macros can also be created in Visual Basic.

The most common methods of spreading the infection are via the macros

themselves, the Word global template (NORMAL.DOT file) and other types of templates, and the Microsoft Word STARTUP directory.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Bablas Class Lewinsky  
Melissa Marker Elecciones2000

Microsoft Excel macro viruses Their objectives are spreadsheets created and edited with Microsoft Excel (XLS files). For identification purposes, their names usually include the following prefixes: XM (Excel 6.0 and/or Excel 95 macro virus), X97M (Excel 97 macro virus) or X00M (Excel 2000 macro virus). In addition to the automatic macros, macros can also be created in Visual Basic.

The most common methods of spreading the infection are via the macros themselves, and the Microsoft Excel XL START directory.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Barisada Laroux Manalo  
Oblivion Sugar Totaler

Microsoft Access macro viruses. Even though this type of virus is not as common as the two previous ones, they do exist. The main difference with these viruses is that they do not use macros, but rather the Microsoft Access modules. Their targets are databases created and edited with Microsoft Access (MDB files).

Microsoft PowerPoint macro viruses. The targets of these viruses are presentations created and edited with Microsoft PowerPoint (PPT files). The most common methods of spreading their infection include the macros themselves, and the PowerPoint global template.

Multipartite Macro viruses. There are macro viruses whose target is not just one Microsoft Office tool, but several of them (for example, they could attack both Word documents and Excel spreadsheets). To differentiate between these viruses and Word or Excel viruses, the following prefixes are used in descriptions: OM (Office 95 macro virus), O97M (Office 97 macro virus) or O00M (Office 2000 macro virus).

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Cybernet HalfCross Shiver  
Tristate Y2K

.RTF file macro viruses. RTF files can be created with Microsoft Word, but they

cannot contain macros. However, if you had a DOC file (Word document) with macros and you changed its extension to RTF, the macros of the original DOC file will remain. The result would be a so-called "fake RTF".

This strategy is used to give users a sense of false security. Users are aware that RTF files should not contain macros, so they would open it. If the file is a fake RTF, they could get infected -in the same way as if they opened an infected DOC file.

Lotus Ami Pro macro viruses. There are not very many of these viruses at the moment. The target of these viruses is files created and edited with Lotus Ami Pro word processor (SAM text files and SMM files, containing macros and other data).

These viruses search for other files in order to spread themselves.

Corel Draw macro virus. The main target of these viruses is files created or edited with the Corel Draw graphic design tool. To infect the system, they search for Corel Draw script files (CSC files, containing elements that are similar to macros). The virus then finds out if these files contain the line "REM Virus". If they don't, it infects the file.

Link or Directory Viruses: Files are documents that contain the information you are working on (text, databases, spreadsheets, images, sound, etc.) or programs (EXE and COM files) and other elements that make it possible to run programs. In order to organize all this information, directories (or folders) are created, which in turn may contain other directories called subdirectories (or subfolders). The structure of a disk can therefore be seen as a huge filing cabinet, in which files are stored in different drawers (directories or folders). Another way of representing this concept is to think of the hard drive as a desk with many drawers. These drawers are the directories or folders where files are stored, but which could also be divided into smaller sections (subdirectories or folders). In short, files are the content and directories or folders are the containers of the content.

The operating system must always have access to information on the files saved on the computer, including the name of the file in question and where (directory or folder) it is stored. To do this, it assigns the file an address, which is accessed every time you want to use the file.

Link or directory viruses change these addresses in order to infect a particular file. In order to run a program, the operating system will immediately go to the address assigned to this application. However, this type of virus alters the address before the system has had time to find the program. What it does is to change the address (in the FAT) so that it points to where the virus is located, saving the correct address elsewhere. This way, instead of running the target program, you will actually be executing the virus. In short, these viruses work in the following way:

They change the address that indicates where the infected file is. That address will now point to where the virus is.

When you try to execute the file, you will really be executing the virus (since the

file address will now be pointing at the virus).

As this type of virus is capable of modifying the addresses where all the hard disk files are stored, its capacity to infect ALL of them is very real. Link or directory viruses can therefore infect entire disk drives, although they cannot infect network drives or add their code to infected files. If you check an infected disk for errors (using tools like SCANDISK or CHKDSK), a large number of errors will be detected, identifying all the links that have been altered by the virus. However, it would be better not to repair this situation, as this could result in genuine chaos as far as the data storage system is concerned, thereby producing even more damage than the virus itself.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

### Byway

Worms: Worms are different to other viruses since they do not infect other files. Their sole objective is to propagate or spread to other systems as quickly as possible. They do however make use of replication (propagation) techniques. In fact, their objective is to copy themselves and then infect other systems. Their infections or replications usually take place through e-mails, computer networks and Internet IRC Channels. They could also replicate inside the memory of a PC.

When a worm is executed, it continues running until the computer is shut down or rebooted. However, each virus uses different techniques to ensure that it is executed every time the computer is booted and Windows starts. They can do this by changing the Windows Registry, for example.

Worms that focus on infecting other computers, copy the program they use to carry out infections to a particular directory in the infected computer. They do this by propagating through any means that gives them access to other computers (network, e-mail, disk drives, the Internet, etc). The worm could also consist of more than one program. If this is the case, all programs will be subordinate to a main program. This variation is usually called a net worm.

These are the steps that a worm usually follows to infect other systems:

Somebody (usually a hacker), exploiting possible security vulnerabilities within a system or software tool, sneaks the worm into a computer network.

The worm infects the computers it has access to through the security hole.

Once it is in, it copies itself.

After doing that, it tries to infect all computers it can access.

Depending on the language it is written in, the techniques it uses to propagate and other characteristics, worms can belong to several categories:

E-mail worms. these worms usually propagate through e-mail messages, using e-mail client programs.

IRC worms (mIRC and Pirch worms). These are worms that spread through IRC (chat) channels. The most widespread programs used to do this are usually mIRC and Pirch.

VBS (Visual Basic Script) worms. These are worms written or created in Visual Basic Script.

Windows32 worms: these worms spread through the Windows API (functions belonging to a particular Internet protocol).

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Disemboweler ExploreZip Fix2001  
Happy99 I Love You Mandragore  
Navidad Pretty Park The Fly

Trojan Horses (or Trojans): Trojans cannot be considered viruses as such. They take their name from Greek mythology (the famous wooden horse in which Greek soldiers hid so that they could enter the city of Troy undetected and then attack it). Trojans work in a similar way. They seem to be harmless programs which get into a computer through any channel. When that program is executed (they have names or characteristics which trick the user into doing so), they install other programs on the computer which could be harmful.

A Trojan may not activate its effects at first. However, when they are activated (when the trigger conditions are met), files could be deleted, information on the hard drive lost or a backdoor to the system could be opened.

Most Trojans access specific communication ports and leave them open for external access. If this is the case, using a connection (in a local network or through the Internet) somebody could access all the information stored on a computer

(passwords, personal keys, e-mail addresses, etc), send this information to other addresses (other computers, usually the attacker's) and perform any operation without the user's consent.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Asylum Bck/BO.F Crack2000  
DonaldDick Extacis KillCMOS  
MTX Netbus Win32/HLLP

Logic Bombs: These activate and damage an infected system only when one or more condition/s are met. They are not considered viruses as such, since they do not replicate, but rather depend on the actions taken by the user (the user usually copies and/or executes them unintentionally).

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

Restart

Encrypted: Rather than a virus category, this is a technique that viruses could use. A virus could belong to another category and be also encrypted (if it uses this technique). The virus encodes or encrypts itself so that antivirus programs cannot easily detect it. In order to perform these activities, the virus de-encrypts itself and, when it is finished, encrypts itself again.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.

DieHard Explosion-II Elvira  
Flip Junkie TMC

Multipartite: These viruses can carry out many infections and do so using several techniques. Their objectives are any elements that could be infected: files, programs, macros, disks, etc. They are considered rather dangerous due to their capacity to combine many infection techniques and the actions they can carry out.

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find

the description of a large number of these viruses.

Inca Natas One Half  
Pieck Tequila

Polymorphic: These are virus that use a new technique to avoid detection by antivirus programs (they are usually the hardest viruses to find). They change with every infection they carry out. In this way, they create a large number of copies of themselves.

Polymorphic viruses encrypt or encode themselves in a different way (using different algorithms and encryption keys) every time they infect a system. This makes them impossible to find using strings or signature searches (since these are different in every encryption).

Below there is some information about some viruses of this type. If you would like more information, see the list of viruses in the Encyclopedia, where you will find the description of a large number of these viruses.



**Data Recovery Clinic**

**935 MAIN Street, Suite A-1 , Safety Harbor, FL 34695**

**866-360-4192**

**866-360-4192**

**727-360-4192 (24/7)**

**Fax: 800-675-3967**

Data Recovery Clinic  
now has New York Office

826 Broadway \* Suite 9  
NY, NY 10003  
Phone: 212-996-6125

This document was created with Win2PDF available at <http://www.daneprairie.com>.  
The unregistered version of Win2PDF is for evaluation or non-commercial use only.