BinaryHealthcare.com
Industrial Evangelist

First Written : 1996
Last Updated : 17th October 1998

Viruses:
A Theoretical Beginner's Guide

By: Adam Chee W.S

Note: This article is also published at East Carolina University (USA)

Disclaimer

I offer the following information for educational purposes only. I will assume no responsibility for what they are used for. The article is compiled by me (the author) with information from some articles but mostly with ideas and knowledge of my own. I recommend that you be very careful in handling these ideas as well. By downloading any of the following files or using them you accept all responsibility and this disclaimer.

Introduction

Dear reader, the article you are about to read was written in the year 1996 and updated periodically till the year 1998. While some of the information contained is outdated at this point of time, it was technically correct and relevant back then (Believe it or not, I even received an email from the hacker group **2600** for this, just a pity that **Hotmail** junked my mailbox when it got flooded).

So before you email me to complain that new virus types are not covered here etc etc, bear in mind that it was the year 1996, I was 18 years old when I wrote this

=== Start of Article ===

I believe that understanding theory concepts is the only way to truly understand the way how computer works, learn the concepts and evolve from it. That is why this document is only a brief theoretical guide, If you want a Tutorial on how to write a Virus, search the Internet for it or email me, I will try to explain concepts and answer common question on this topic.

Due to the Virus Ethics, I will not "teach" you how to "write" destructive codes; rather I'll give you an overall structure of a virus, how it works and the necessary knowledge to protect yourself against one. In this version, all source code of viruses and their explanation are taken out because I believe that these source codes have been used for purposes other than educational. (That means some morons had compiled it and infected PCs).

The reason why this report is written is:

- To enhance laymen on the concepts of viruses.
- To try to revive the **hacker's ethics** on virus (Yes, there are ethics for Hackers and Virus Coders too)

- To create an awareness on Viruses and Malicious Software

What is a Virus?

Alot of people are not clear or do not know what is the actual definition of a computer virus. The concept of a virus is extremely simple and should be understood by even beginning programmers, literally anybody can write a virus, as *Jim Goodwin* said in an article,

" *We have merely surrounded the virus issue with an air of mystique that makes it appear that there is some magic formula that must be guarded from the crowd of people waiting to write viruses*."

And I agreed with his definition of a virus: **A program that merely copies itself and attaches itself to another program**.

Take note that nowhere in the definition is there any mention of non prompted, secret operations of destructive actions or of spreading across multiple computer installations. A program need not conduct such activity to qualify as a virus!

The minimum criteria for computer virus design is

- Be executable
- Be capable of cloning itself
- Convert other executable objects into viral clones

Take note that computer Viruses usually load and run without user requesting them to; they hide inside normal programs (call *host programs* and run when the host runs)

The problem is that other than viruses, there are other rouge programs out there, and the laymen are also classifying them as viruses. Therefore I'll refer all rouge programs as viruses throughout the rest of the tutorial. However, before we start, I will go through the definitions of a few rouge programs.

- **Bug-ware**
  A lawful computer program designed to do specific sets of function but due to internal logic flaws, they accidentally cause harm to system hardware for software.
- **Trojan Horse**
  A piece of unauthorized code hidden in what appears as a useful program and like a virus, may execute immediately or be link to a certain time or event. A Trojan however does not self-replicate.
- **Chameleons**
  A program that emulates other programs, often used to trick users into revealing passwords or other confidential information by emulating logon procedures.
- **Software bombs**
  The easiest to produce, software bombs simply detonate within moments of their launched with no viral cloning. They explode within impact & blow up data.

- **Time bombs**
  A set of computer instructions enters into a system or a piece of software that are design to go off at a predetermined time. E.g. 1st of April, Friday the 13th …
- **Logic bombs**
  Programs that execute destructive computer commands conditionally depending upon the status of specific environmental variables. E.g. A logic bomb could monitor payroll records in an effort to watch for the dismissal of it's programmer. The logic bomb could be programmed to denote when its programmer's payroll record fails to appear for 3 consecutive weeks.
- **Replicators**
  A program that creates continuously and without end-independent, executable copies of itself until no disk space are left. Also known as **rabbit**.
- **Worms**
  Enters a computer network and leaves messages or recopies itself to use up memory.
- **Trapdoors**
  A program written to provide future access to the system by the programmer.
- **Viruses**
  A program that attaches itself to a legitimate, executable program, then reproduces itself when the program is run.

Some rouge programs are purposely designed to make a program do things you don't expect it to do while other viruses are just an annoyance, perhaps only displaying a "Peace on earth" message. The viruses we're worried about are the ones designed to destroy your files and waste the valuable time you'll spend to repair the damage.

Things Virus can do or have done

- Fill up your computer with garbageware.
- Mess up files
- Mess up the FAT (file allocation table)
- Mess up the boot sector
- Format a disk or a diskette
- Display a message
- Put message into printouts
- Reset a computer
- Slow things down
- Redefine keys
- Lock up keyboard
- Change data in programs or files
- Encrypt or otherwise distort your data
- Physically damage the hard drive and other parts of the machine
- Copy data you have access to for another user who shouldn't have access

Computer Virus Warning signs

- Computer operation seem sluggish

- Programs takes longer than normal to load
- Programs access multiple disk drives where they didn't before
- Programs conduct disk access at unusual times.
- Available disk space decrease rapidly
- The number of available RAM suddenly or steadily decrease
- Memory maps (like DOS MEM command) reveal new TSR (memory-resident) program of unknown origin.
- Normally well-behaved program function abnormally or crash without reason
- Programs encounter errors where they didn't have before
- Programs generate undocumented message (error messages) E.g. Invalid drive specification
- Apparently benign, humorous "pranks" programs mysteriously materialize & nobody admits to installing them. E.g. black holes, bouncing balls, smiley faces starts to appear on screens
- Files mysteriously disappear
- Files are replaced with objects of unknown origin or are replaced with garbled data
- Names, extensions, dates, attributes or data changed on files or directories that have not been modified by users
- Data files or directories of unknown origin appear

Frequently asked questions about Viruses

Q) What is a virus?

A computer virus is simply, a program designed to attach itself to another computer program. Some computer viruses damage the data on your disks by corrupting programs, deleting files, or even reformatting your entire hard disk. Most viruses, however, are not designed to do any serious damage; they simply replicate or display messages.

Q) What viruses can and can't do?

- Computer viruses infect executable program files, such as word processing, spreadsheet, or operating system programs.
- Viruses can also infect disks by attaching themselves to special programs in areas of your disks called boot records and master boot records. These are the programs your computer uses to start up.
- Computer viruses do not damage hardware, such as keyboards or monitors. Though you may experience strange behaviors such as screen distortion or characters not appearing when typed, a virus has, in fact, merely affected the programs that control the display or keyboard. Not even your disks themselves are physically damaged, just what's stored on them. Viruses can only infect files and corrupt data.
- Most viruses stay active in memory until you turn off your computer. When you turn off the computer you remove the virus from memory, but not from the file, files, or disk it has infected. So the next time you use your computer, the virus program is activated again and attaches itself to more programs. A computer virus, like a biological virus, lives to replicate.

- A virus cannot appear all by itself, it has to be written, just like any other program.
- Not all viruses are intentionally harmful - some may only cause minor damage as a side effect - however, there is no such thing as a "harmless" virus.
- Reading plain data from an infected diskette cannot cause an infection. (However, it is not trivial to determine what "plain data" is)
- A write-protected diskette cannot become infected, if the hardware is working properly.
- It used to be the case that a virus could not infect a computer unless it was booted from an infected diskette or an infected program was run on it, but alas, this is no longer true. It is possible for a virus infection to spread, just by the act of reading an infected Microsoft Word document, for example, or through use of Lotus Notes, to name two well-known applications.
- It also used to be the case that a virus could not infect data files or spread from one type of computer to another; a virus designed to infect Macintosh computers could not infect PCs or vice versa, but with the appearance of application viruses this has changed as well - there are now a few viruses that can infect WinWord as well as MacWord.

Q) How does a Virus Spread?

A virus is inactive until the infected program is run or boot record is read. Once the virus is activated, it loads into the computers memory where it can perform a triggered event or spread itself. Disks used in an infected system can then carry the virus to another machine. Programs files can also spread a virus. Data files, however, can not transfer a virus but they can become damaged.

Q) What should I do to protect myself?

Isolating the computer system from contact with outside sources of software is the best way to insure the integrity of the system. This is very difficult for multi-user systems and not a particularly attractive solution if the computer is going to continue be useful over time.

One alternative approach is to detect the existence of malicious or self replicating computer instructions. This requires some knowledge of the target of the attack and the means used by a virus to self-replicate. A generic solution is difficult, but several programs have been developed for identifying certain types of computer instructions that could present risks.

These programs check for extraneous file operations including opens, closes, reads and writes that bypass operating system functions

Another solution is to stop the virus from replication by preventing the rewriting of 'infected' files. Confining programs to libraries on storage devices with 'write disable' hardware is one approach. Many large-scale computer peripheral devices have such a switch, however these features are rarely found on desktop computers. An alternative to a hardware 'write disable' switch is a software 'read only' feature. Unfortunately, these options are found only on mini and mainframe computer operating systems. The "read-only" attribute in MS-DOS is not an effective protection mechanism because File Allocation Tables (FAT) can be changed from user written programs.

Popular microcomputer operating systems allow execution of computer instructions that can directly address and operate storage devices bypassing normal operating system calls. Thus there is a constant exposure of disk storage devices and their file directories to destruction or modification.

Q) How do these virus programs enter a computer system?

Generally, viruses enter a computer system by using an appealing program as a 'host' to harbor the self replicating computer instructions. The host can be one of the operating system tools such as compilers, editors, file utilities or one of the embedded macro languages found in spreadsheets or data base management software, and sometimes even in games.

Distribution of malicious software depends on getting an unsuspecting user to accept a program where visual inspection of the product is difficult, and the author or source can remain anonymous. Public or private conferencing systems, timesharing networks and electronic bulletin boards as well as user group software exchanges and computer "flea markets" meet these requirements.

Q) I'm infected with a virus, what should I Do?

If you have a computer virus or suspect you have one, the first thing to do is: DON'T PANIC!

Most infections are harmless, and even if you have a very destructive virus on hand.

The most important tool in your fight against computer viruses is an uninfected boot diskette! This disk ensures that you can start your system without any virus code in the computer's memory. You can easily create a boot disk if you choose to copy the system files to a disk during formatting or with the DOS command FORMAT A: /S.

After which, simply run any good Anti-Virus program (I recommend F-prot, its free and good) to find the virus and disinfect it.

Reformatting your hard drive is only the last resort if other attempts to remove the virus have failed. If you are unsure of what to do, get someone experienced in clearing a virus to help you.

For more FAQ reading, get the **comp.virus FAQ**

Testing Your Virus Scanner ("Anti-Virus Program")

Any Virus Scanner (Anti-Virus Program) can be tested with a special test file. This is a dummy file which is detected like if it were a virus. This file is known as EICAR Standard Anti-virus Test file (EICAR is the European Institute of Computer Anti-virus Research).

Naturally, the file is not a virus. When executed, EICAR.COM will display the text '**EICAR-STANDARD-ANTIVIRUS-TEST-FILE**' and exit.

To create the EICAR test file, simply use any text editor (like the good old Edit.com found in DOS) to create a file with the following single line in it:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Save the file to any name with COM extension, for example EICAR.COM. Make sure you save the file in standard MS-DOS ASCII format. The file should be 68 bytes long, but might be 70 bytes if the editor puts a CR/LF at the end. Now you can use this file to test what happens when your Virus Scanner encounters a “real” virus, or if you wanna play safe, email me and request for real live Viruses.

Myths about Viruses

1) All purposely-destructive code comes as a virus.

Wrong. Remember, “Trojan horse” is the general term for purposely-destructive code. Very few Trojan horses are actually viruses.

2) All Trojan horses are bad.

Believe it or not, there are a few useful Trojan horse techniques in the world. A “side door” is any command not documented in the user manual, and it’s a Trojan horse by definition. Some programmers install side doors to help them locate bugs in their programs. Sometimes a command may have such an obscure function that it makes sense not to document it.

3) Viruses and Trojan horses are a recent phenomenon.

Trojan horses have been around since the first days of the computer. Hackers toyed with viruses in the early 1960s as a form of amusement. Many different Trojan horse techniques were developed over the years to embezzle money, destroy data, etc. The general public wasn’t aware of this problem until the IBM PC revolution brought it into the spotlight. Just five years ago, banks were still covering up computerized embezzlements because they believed they’d lose too many customers.

4) Computer viruses are reaching epidemic proportions.

Wrong again. Viruses may be spread all over the planet but they aren’t taking over the world. There are only about fifty or so known virus “strains” at this time and a few of them have been completely eliminated. Your chances of being infected are slim if you take proper precautions. (Yes, it’s still safe to turn on your computer!)

5) Viruses could destroy all the files on my disks.

Yes and a spilled cup of coffee will do the same thing. If you have adequate backup copies of your data, you will be able to recover from a virus/coffee attack. Backups mean the difference between a nuisance and a disaster.

6) Viruses can be hidden inside a data file.

Data files can't wreak havoc on your computer — only an executable program can do that. If a virus were to infect a data file, it would be a wasted effort.

7) My files are damaged, so it must have been a virus attack.

A power flux, or static electricity, or a fingerprint on a floppy disk, or a bug in your software, or perhaps a simple error on your part could also have caused it. Power failures and spilled cups of coffee have destroyed more data than all the viruses combined.

8) Viruses can spread to all sorts of computers.

All Trojan horses are limited to a family of computers, and this is especially true for viruses. A virus designed to spread on IBM PCs cannot infect an IBM 4300-series mainframe, nor can it infect a Commodore C64, nor can it infect an Apple Macintosh because the structure of the systems are different.

9) My backup disks will be destroyed if I back up a virus.

No, they won't. Let's suppose a virus does get backed up with your other files. Backups are just a form of data, and data can't harm your system. You can recover the important files from your backups without triggering the virus.

10) Anti-virus software will protect me from viruses.

Anti-virus packages offer some good front-line protection, but they can be tricky to use at times. You could make a crucial mistake in deciding whether to let a "flagged" event take place. Also, Trojan horses can be designed to take advantage of holes in your defence.

11) Copy-protected software is safe from an attack.

This is totally wrong. Copy-protected software is the most vulnerable software in a Trojan horse attack. You may have big problems trying to use or re-install such software, especially if the master disk was attacked. It should also be noted that copy-protection schemes rely on extremely tricky techniques which have occasionally "blown up" on users. Some people mistakenly believe that they were attacked by a clever virus.

12) Viruses are written by hackers.

Yes, hackers have written viruses — just to see how they operate. But they DON'T unleash them to an unsuspecting public. Wormers are the ones who do that. (You can think of a wormer as a hacker who was seduced by the Dark Side of the Force.) Hackers got a bum rap when the press corrupted the name.

Types of Computer Viruses

Memory Resident Viruses: Most common virus. Loads like a TSR (Terminate and Stay Resident) staying in memory where it can easily replicate itself into programs of boot sectors.

Non-Resident Viruses: A rare type of virus. Does not stay in memory after the host program is closed, thus can only infect while the program is open.

Macro Viruses: Consists of instructions in Word Basic or other macro language, and resides in documents. While the documents cannot be infected, any application which supports macros (E.g. Microsoft Winword and Excel) that automatically execute is a potential victim for macro viruses.

Common Viruses: Viruses that you are most likely to encounter.

Program Viruses: Viruses that can infect program files that you run. (Executable programs such as those with the extension of Com, Exe, Ovl, Drv, Sys and Bin)

Boot Viruses: Viruses that can infect Boot Records (BR), Master Boot records (MBR), File Allocation Table (FAT) and Partition Table on disks.

Multipartite Viruses: Viruses that infect both program files and boot records.

Stealth Viruses: Viruses that try to conceal themselves from attempts to detect or remove them.

1. Full Stealth - Virus redirects disk reads to avoid detection.
2. Size Stealth - Disk directory data is altered to hide the additional bytes of the virus.

Polymorphic Viruses: Viruses with the ability to mutate by changing code segments to look different from one infection to another, making detection more difficult.

Encrypting Viruses: Technique of hiding by means of transformation. Virus code converts itself into cryptic symbols. However, in order to execute and spread, the virus must first decrypt itself.

Armored Viruses: An armored virus is one that uses special tricks to make tracing, disassembling and understanding of its code more difficult.

Cavity Viruses: A cavity virus is one which overwrites a part of the host file that is filled with a constant, without increasing the length of the file, but preserving its functionality.

Fast Infectors: Fast infector is a virus that, when it is active in memory, infects not only programs which are executed, but even those that are merely opened. The result is that if such a virus is in memory, running a scanner or integrity checker can result in all programs becoming infected.

Slow Infectors: The term “slow infector” is sometimes used to refer to a virus that only infect files as they are modified or as they are created. The purpose
is to fool people who use integrity checkers into thinking that modifications reported by their integrity checker are due solely to legitimate reasons.

Sparse Infectors: The term “sparse infector” is sometimes used to describe a virus that infects only occasionally, or only files whose lengths fall within a narrow range, etc. By infecting less often, such viruses try to minimize the probability of being discovered.

Windows Viruses: Viruses that infect Windows programs.

Agent Viruses: Viruses that infect agent programs (such as those that download software from the Internet).

Tunnelling Virus: A tunnelling virus is one that finds the original interrupt handlers in DOS and the BIOS and calls them directly, thus bypassing any activity monitoring program which may be loaded and have intercepted the respective interrupt vectors in its attempt to detect viral activity. Some antivirus software also uses tunnelling techniques in an attempt to bypass any unknown or undetected virus that may be active when it runs.

Dropper: A dropper is a program that has been designed or modified to “install” a virus onto the target system. The virus code is usually contained in a dropper in such a way that it won’t be detected by virus scanners that normally detect that virus. While quite uncommon, a few droppers have been discovered. A dropper is effectively a Trojan Horse whose payload is installing a virus infection. A dropper which installs a virus only in memory is sometimes called an “injector”.

Triggered Event Virus: An action built into a virus that is set off by the date, a particular keyboard action or DOS function. It could be as simple as a message printed to the screen or serious as in reformatting the hard drive or deleting files.

In the Wild: A virus is referred to as “in the wild” if is has been verified by groups that track virus infections to have caused an infection outside a laboratory situation. A virus that has never been seen in a real world situation is not in the wild, and sometimes referred to as “in the zoo”.

However, there are actually only 3 classifications of viruses,

1. **Boot Sector Virus**
2. **Program Virus**
3. **Application Virus**.

The different type of viruses mentioned above falls into these 3 classification although some of them are of a hybrid model and some other have special features.

1. Boot Sector Virus

A **Boot Sector Virus** (BSV) infects boot sectors on diskettes and/or hard disks. On diskettes, the boot sector normally contains code to load the operating system files. The BSV replaces the original boot sector with itself and stores the original boot sector somewhere else on the diskette or simply replaces it totally. When a computer is then later booted from this diskette, the virus takes control and hides in RAM. It will then load and execute the original boot sector, and from then on everything will be as usual.

Except, of course, that every diskette inserted in the computer will be infected with the virus, unless it is write-protected. A BSV will usually hide at the top of memory, reducing the amount of memory that the DOS sees. For example, a computer with 640K might appear to have only 639K.

Most BSVs are also able to infect hard disks, where the process is similar to that described above, although they usually infect the master boot record instead of the DOS boot record.

2. Program Virus Program Viruses

The second type of computer viruses, infect executable programs; usually .COM and .EXE files, but they sometimes also infect overlay files, device drivers or even object files.

An infected program will contain a copy of the virus, usually at the end, in some cases at the beginning of the original program, and in a few cases the virus is inserted in the middle of the original program.

When an infected program is run, the virus may stay resident in memory and infect every program run. Viruses using this method to spread the infection are called “Resident Viruses”.

Other viruses may search for a new file to infect, when an infected program is executed. The virus then transfers control to the original program. Viruses using this method to spread the infection are called “Direct Action Viruses”. It is possible for a virus to use both methods of infection.

Most viruses try to recognize existing infections, so they do not infect what has already been infected. This makes it possible to inoculate against specific viruses, by making the “victim” appear to be infected. However, this method is useless as a general defence, as it is not possible to inoculate the same program against multiple viruses.

3. Application Virus

The third type of viruses are **Application Viruses**, which do not infect normal programs, but instead spread as “macros” in various types of files, typically word-processor documents or spreadsheets. Once again, as I’d said earlier, viruses are just programs - rather unusual programs perhaps, but written just like any other program. It does not take a genius to write one - any average assembly language programmer can easily do it.

Detailed information of individual / Specific Viruses

I would not provide detailed information of individual virus because any good anti-virus software should contain a detailed library of Viruses information, besides, if I would to include them, the size of this tutorial would be enormous.

How to extract a Virus

To extract a virus form memory, one must be able to understand how a virus works, this includes knowing the general structure of a virus and the boot process of an IBM compatible PC.

Anatomy of a Virus

The 1st condition needed by the typical virus is that it MUST be loaded in memory to be able to infect. This is because a virus is just another program. Yes, it is executed just like an application program or utility program! The 2nd condition is that it must have a host/target to infect. (Think of the target as a helpless victim). In an infection, the virus will duplicate itself and copy it somewhere inside the target program, (usually the first few bytes) after which the target program will become a virus host (you can classified that as a virus too). This "infected" program will in turn infect your system whenever it is execute/run because when you execute/run the "infected" program, the virus code inside the program will also be execute/run.

Boot-up Process

Bear in mind that if the virus attacks before the anti-virus is loaded, there is a high possibility that your anti-virus program will be infected also.

Therefore it is only necessary to know and understand the boot-up process of an IBM compatible PC. When the switch is on, the power supply will start and the following will be loaded in order;

- BIOS
- POST (Power-On-Self-Test)
- Search for OS (Operating System)
- Io.Sys
- Msdos.Sys
- Config.Sys
- Command.Com
- Autoexec.Bat

The Extraction

Now that you have understood the general structure and concept of a virus, lets go down to extracting a virus from memory. The extracted virus can be used for a lot of purposes but please DO NOT use the virus to infect other people's machine!! It is totally unethical and is against the Law.

First you write a program that has a start and a end (or a head and a tail, beginning and end…) but does nothing other than that. I have included an example in Turbo Pascal.

```
Program Virus_carrier;
Begin
End.
```

This program acts as a dummy program which will be infected by the virus resident on the system when executed/run on an infected machine. It's advantages are that it's size is minimum and it's serves no other purposes, therefore, when the virus is captured onto this program, this program will become the virus executable itself.

(*Note: Turbo Pascal is used to illustrate the example because it is usually used in schools for teaching purposes, you can use other languages like Assembly, C, C++, JAVA or any other 3rd GL programming language.)*

Safe Computing

Rest assured that neither you nor anyone you know will suffer a major data loss from a viral attack if safe-computing measures are implemented regularly. When and if a viral infection is discovered, turn your computer off and contact a good viral diagnostician for eradication advice. Do not use your computer or any floppy disks associated with your computer until your system has been thoroughly cleansed. Take comfort in the knowledge that safe-computing techniques, employed properly, will serve to protect your data from harm.

There is no single set of solutions for preventing virus attack. Each installation must assemble its own procedures for containing the problem. However this 5 step process is suggested.

- **Education**
  All users of computers should be told about the existence of Trojan Horses and Computer Viruses, what they are and how to tell whether their system has been infected. Be frank when discussing the threat of computer viruses. (This is what this document is about!!!)
- **Backup and recovery procedures.**
  Develop easy procedures for routine backup of important computer files. Make backup hardware (i.e. tape units) readily available to all users. Users connected to LANs should use automatic backup features. Suggest file organization structures that facilitate backup and recovery of disks that have been ruined by computer viruses.
- **Isolate Software Libraries**
  On larger computer systems, consolidate libraries into 'Read Only' directories. In general system or shared software should have limited update and write attribute privileges.
- **Implement Software Library Management Procedures**
  Enforce program testing, version control, and quality assurance checking for all software libraries. Use software library management tools to control and audit programs. Assign responsibility for testing public domain software and providing "approved" copies of that kind of software. Known source of software, inspect distribution media and documentation for tapering, and develop a "master copy" system.

- **Develop an Virus Alert Procedure**
  Getting the word out about potential or known viruses can contain or minimize the eventual spread and harmful effects of a computer virus. Notices, telephone trees to, phone or electronic mail are all good vehicles. Procedures for containment and eradication should be thought out before hand. These procedures usually require shutting system down, reformatting disk or tape storage media and re-building software libraries with known uninfected copies

====The End====

Cracker and Hacker Definition

On USENET, calling someone a "**cracker**" is an unambiguous statement that some person persistently gets his/her kicks from breaking from into other peoples computer systems, for a variety of reasons. She or he may pose some weak justification for doing this, usually along the lines of "because it's possible", but most probably does it for the "buzz" of doing something which is illicit/illegal, and to gain status amongst a peer group. Particularly antisocial crackers have a vandalistic streak, and delete filestores, crash machines, and trash running processes in pursuit of their "kicks".

The term is also widely used to describe a person who breaks copy protection software in microcomputer applications software in order to keep or distribute free copies.

On USENET, calling someone a "**hacker**" is usually a statement that said person holds a great deal of knowledge and expertise in the field of computing, and is someone who is capable of exercising this expertise with great finesse.

In the "real world", various media people have taken the word "hacker" and coerced it into meaning the same as "cracker" - this usage occasionally appears on USENET, with disastrous and confusing results.

Posters to the security newsgroups should note that they currently risk a great deal of flamage if they use the word "hacker" in place of "cracker" in their articles.

(Article taken from Monica Khandpur's Concept Page)

The article has clearly shown the difference between Hackers and Crackers, Hackers has a set of Ethics, Crackers don't.

The Hacker's Code of Ethics

- Access to computers-and anything which might teach one something about the way the world works-should be unlimited and total.
- All information should be free.
- Mistrust authority-promote decentralization.
- Hackers should be judged by their hacking, not by other criteria.
- One can create art and beauty on a computer.

- Computers can change one's life for the better

Contact

Media and all other Queries: media@binaryhealthcare.com

About BinaryHealthcare.com

BinaryHealthcare.com is a vendor-neutral knowledge management repository pertaining to selected IT topics, Healthcare Informatics and its relevant industries (Biomedical Engineering, Radiology, Health Informatics, Telemedicine etc.) for working Professionals, students and anyone who is interested in this unique profession.

For more information, visit www.binaryhealthcare.com