

PROTECTION AGAINST VIRUSES

Only 10-15 years ago there was no such problem as computer viruses and only selected computer specialists knew about the rare cases of virus appearance. However, due to tremendous increase of personal computer use in recent years, the virus problem has spread on a mass scale. Therefore, it is useful to get general information about viruses, consider them a potential source of danger to stored data, and to know methods of protection against viruses.

Generally speaking, in this context, a virus is a computer program that is capable of self-multiplication and transmission from one computer to another through a diskette (most common cause) or through a network (for example, through Internet). This program usually camouflages its presence in the system and is designed to cause damage to a PC user one way or another. Fortunately, viruses that can physically damage or, in other words, destroy a computer do not currently exist. However, the possibility losing all of one's programs and data forces us to address the problem of protection against virus quite seriously.

Why Create Viruses?

Creation of a virus requires that its creator have a good knowledge of computers and operating systems. It may be a manifestation of personal abilities or expression of vanity. However, intention to cause damage to a large group of innocent people does not honor virus authors. Besides, in many countries creation and distribution of such programs is considered a felony when the damage is made. For understandable reasons, authors of many viruses are students of universities and computer specialists who have not found better use for their skills. Sometimes users transmit a virus themselves as a "gift" or prank to somebody.

Types of Viruses

As described above, it is clear that a virus is a computer program. However, virus is not present in a computer in the form of a program file (such as *.EXE, *.COM, *.DLL etc., for example VIRUS.EXE), because it would allow us simply to eliminate it on the operating system level.

Instead, some viruses reside in the hidden system areas of a hard drive, which are read during the boot process. This ensures automatic activation and camouflages the virus. Frequently the Master Boot Record or Boot Record on a hard drive or diskette is where the virus stores its own activation program. Viruses that infect the disk or diskette system areas are called "Boot" viruses.

A virus may also add itself to an existing executive file (program), which leads to its activation during each run of the infected program-carrier. Most frequently, executable file with extensions EXE and COM are subject to such virus infection. In this case, activation of the virus takes place during the first start of the infected program. These types of viruses are called "file viruses". However, there are different types of these viruses that infect DOS, Windows, and other device driver files.

Recently, a new type of virus has appeared that infects computers through MS Word and Excel documents by using the executable macro/command language of the word processor. In this case, virus activation takes place during opening of the infected document in the word processor. This type of virus is called a "macro-virus".

Note. It is noteworthy that installation of an “infected” diskette in the floppy drive does not lead to automatic infection of a computer. Virus activation from an infected diskette can take place in the following cases:

- If an infected diskette is in a floppy drive during the boot process and the computer is reading from it to boot the system (for boot viruses).
- When running an infected program (for file viruses)
- During opening of an infected document in a word processor (for macro-viruses).

Virus behavior after activation depends on its author intentions and can consist of one or several manifestations:

- Infection of other executable programs
- Infection of the boot area of inserted diskettes
- Imitation of malfunctioning of physical components: floppy disk drive, hard drive, display, keyboard
- Slow computer performance, showing strange messages, making awkward sounds, etc.
- Modification or deletion of the information on a disk

Viruses that destroy or modify information are the most dangerous for the user. It is hard and sometimes impossible to restore information after such viruses have done their damage.

How to Fight Them

The appearance of viruses has led to the development of anti-virus programs. The goal of an anti-virus program is to detect the presence of a virus, inform the user about it and, ideally, eliminate the virus itself, as well as all consequences of its “work” without any harm to the data.

Anti-virus programs can be divided into two large groups by their performance:

- Detector Programs
- Security Programs

Detector programs can be activated manually when suspicious changes take place or each time when computer is booted. Programs of this type contain large databases regarding all possible viruses and use it for scanning viruses in the Random Access Memory, disk system areas, and files that may be subject to infection. Additionally, detector programs can include algorithms for heuristic search for unknown viruses. Wide spread *Dr. Web* and *AIDS Test* are examples of detector programs. One of the shortcomings of detector programs is that they fight a virus after it has already infected the system.

Security Programs begin to work during the operating system startup and stop when a computer is turned off. They also contain the database with virus descriptions, but in contrast to detector programs, they check each started program and each new file “on the fly”. Programs of this type check diskettes before they are read, i.e. before a virus can get into the computer. Some degradation of the computer performance and mishandling of some applications have been the shortcomings of this program class for a long time. However, the most recent versions of these programs for Windows 95 work faster and more reliable. One of these programs is Norton AntiVirus, which AIHA installs on the training center computers.

In any case, it is worthwhile to have several different anti-virus programs. Also, it is important to have the most recent version of the programs to ensure successful protection against new viruses. For instance, the well-known macro virus *Word.CAP* is not included in

the database of the early versions of the Norton Antivirus program; therefore, to ensure protection against this virus, the program must be updated (see below).

Additional information about viruses and anti-virus programs is available at the following Internet sites:

<http://www.symantec.com/avcenter>

<http://www.dials.ccas.ru/home.htm>

<http://virus.komi.ru/>

Norton AntiVirus Program

After installation on a computer, Norton AntiVirus (NAV) works without the user's participation. It automatically checks diskettes, new files, and started programs for the presence of viruses. Visually, the program is located on the Task Bar (see the drawing):

When NAV finds a virus, it makes a sound (pretty loud) and displays a dialog box on the monitor screen, asking to choose one of the following actions:

- interrupt the process, which has triggered this message (Stop)
- continue work without any actions (Continue)
- clean the virus from the infected file and restore the original file (Repair)
- exclude this type of phenomena from the database and do not react to such manifestations in future (Exclude)

When such message appears, it is recommended to try at first to clean the virus (select Repair). This works in most cases. If NAV tells you that the virus cannot be eliminated, try to delete the entire file (Delete) to avoid the infection of the computer. You may continue your work without any actions (Continue) or without excluding suspicious manifestations (Exclude) from the database, only if you are absolutely sure the suspicious file contains no virus.

Also, to perform a manual check of files and disks, as well as to configure working parameters, one can, at any time, start NAV from the Start menu (Start/Programs/Norton AntiVirus/Norton Antivirus).

You can check the selected disk for viruses by pressing the key - ScanNow (see the Drawing).

Presently there are several versions of the Norton AntiVirus Program (hereinafter called NAV), one of which can be installed on your computer:

- NAV for Windows 95, version 1.0 or 95.0b
- NAV for Windows 95, version 2.0
- NAV for Windows 95, version 4.0

To verify your program version, start NAV from the Start menu (Start/Programs/Norton AntiVirus/Norton AntiVirus) and look in "About NAV" in the Help menu.

New versions of NAV provide more reliable protection, work faster, and are more efficient. Also, the virus description database for NAV is updated every month, and only new database versions contain information to provide protection against new viruses.

Therefore, it is necessary to update the database (virus definitions) and NAV itself (product update). For this purpose, you may visit Norton Antivirus webpage at:

<http://www.symantec.com/avcenter/download.html>

Where you can find programs for possible updates of your program version (Product updates):

- for NAV for Windows 95 v1.0, 95.0b
Large Volume Update
File name: NAC95OB.EXE
- for NAV 2.0 for Windows 95, 2.01 Network Support Update
File name: NAV95201.EXE
As well as new additions to the virus database (Virus Definitions Updates).

After the update program is loaded on your computer, it is necessary to run it and reboot the computer.

The last versions of Norton AntiVirus include a feature called LiveUpdate, which starts from Control Panel and can automatically communicate with Symantec. It checks for the availability of new update programs on the server and, if available, downloads and installs them on your computer.

BACKUPS

A computer is a sophisticated combination of hardware and software and, as any other system, is not guaranteed from malfunctioning. Hardware failures can be a result of a breakdown of one of the devices, and software failures may result from errors in the operating system configuration or from viruses. In addition to failures, there is also the danger of accidental or deliberate removal or alteration of information by the user himself.

To avoid information losses, while you are working with a computer, it is necessary to make backups, i.e. periodically copy information to external stores (diskettes or magnetic tape). Since most of the Training Centers do not have Tape Backup, we will review backup onto diskettes. The items to backup are:

- User files
- Windows 95 configuration

User's files

Diskette capacity is limited to 1.4 MB. Therefore, simple copying of multiple files to a diskette is not effective. To ensure compact storage of information, the documents must be compressed with the help of archival programs (PKZIP, ARJ, WinZip), which significantly reduce the size of the files, preserve structure of the directories, and can split large archives into parts suitable for storage on diskettes (except WinZip).

It may be helpful to keep important user files in one directory on a hard drive (primary data directory) and then divide the information into sub-directories from this primary data directory. For example, it is possible to store important information related to the Learning Resource Center in the directory *LRC* on disk C: (C:\LRC). This directory will play role of a primary data directory. Then, the subdirectory *Reports* (C:\LRC\Reports) can be created to store reports in the directory *LRC*. For correspondence, the subdirectory *Letters* (C:\LRC\Letters), etc.

This allows one to select, using a data archival program, the primary data directory for archival, and all its subdirectories will be included in the archive automatically.

Windows 95 configuration

The Windows 95 Configuration, or *Registry*, is a database, which contains parameters and settings for programs and devices installed on the computer. The *Registry* consists of two files – USER.DAT and SYSTEM.DAT. Windows actively uses the *Registry* when the operating system is loaded and in subsequent work. Therefore, damage to the *Registry* may stop normal computer work. It makes sense to periodically copy the *Registry* either manually by copying these files into separate directory or with the help of a program called *Configuration Backup*, which can be found on the Windows 95 CD-ROM in the subdirectory Other/Misc/Cfgback. This program does not require installation – it can be copied directly to any directory and in then run from the hard drive. It is rather simple to work with the program (see Drawing).

To make a new copy of the configuration, you should name it in the Selected Backup Name field and click on “Backup”. To restore the configuration, you should select the needed copy from the list of previous Backups and click on “Restore” and then re-boot the computer. If one of the copies becomes outdated, it can be removed by hitting “Delete” key.

Each copy consists of a zipped file in Windows directory with the extension *.rbk. When necessary, copies of configuration files can be transferred to a diskette, but the copy must be in the Windows directory in order to restore it.

For future identification, diskettes should be marked with labels indicating the type of the stored information and date of the copy. Obviously, diskettes with important information should be stored in a secure place, for example, in a safe.

If you have any questions or comments in regards to problems with protection against viruses or regarding backup copying of information, contact author of this article at: aihaca@online.ru.