The American Journal of Engineering and Technology
(ISSN – 2689-0984)
Published: January 31, 2021 | **Pages:** 48-51
Doi: https://doi.org/10.37547/tajet/Volume03Issue01-09

IMPACT FACTOR
2021: 5. 705
OCLC - 1121105677

Computer Viruses And Diagnostics

Korotkova Larisa Alexandrovna
Senior Lecturer, Department Of "Radio Engineering Devices And Systems", Faculty Of "Electronics And Automation", Tashkent State Technical University, Tashkent, Uzbekistan

Aripova Mapusa Kasimovna
Senior Lecturer, Department Of "Radio Engineering Devices And Systems", Faculty Of "Electronics And Automation", Tashkent State Technical University, Tashkent, Uzbekistan

Baimatova Nargiza Tukhtabayevna
Senior Lecturer, Department Of "Radio Engineering Devices And Systems", Faculty Of "Electronics And Automation", Tashkent State Technical University, Tashkent, Uzbekistan

Ibragimova Barno Bahramova
Senior Lecturer, Department Of Radio Engineering Devices And Systems, Faculty Of Electronics And Automation, Tashkent State Technical University, Tashkent, Uzbekistan

ABSTRACT

Computer viruses are specially written small programs that can embed themselves in the source code of other programs (i.e. infect them) or in documents of a special format containing macros, such as Word, Excel, as well as perform various unwanted actions on the computer.

KEYWORDS

Computer viruses, virus program, destructive capabilities, worm viruses, Trojan program, companion viruses, stealth virus.

INTRODUCTION

A virus program can create its own copies (not necessarily the same as the original), which are distributed in various resources of computer systems, networks, etc. Many viruses harm the data on infected computers, although sometimes their only purpose is to infect as many computers as possible.

Also, viruses can perform various undesirable actions not always, but only when certain conditions are met. [1]

The American Journal of Engineering and Technology
(ISSN – 2689-0984)
Published: January 31, 2021 | **Pages:** 48-51
Doi: https://doi.org/10.37547/tajet/Volume03Issue01-09

IMPACT FACTOR
2021: 5. 705
OCLC - 1121105677

MATERIALS AND METHODS

Conventionally, viruses can be classified according to the following characteristics:

The habitat of the virus

According to the method of infecting the habitat,

According to the destructive capabilities,

According to the features of the virus algorithm.

1. In the environment of the virus:

Network – spread over a computer network local or global-network worms.

File-embedded in executable files.

Boot-embedded in the boot sector of the disk (Boot-sector)

There are combinations-file-boot viruses

2. By the method of infecting the habitat:

Resident-when the computer is infected, it leaves its part in the operational part. When accessing RAM to other programs, they also infect them. Resident viruses are stored in RAM and are active until the computer is turned off.

Non-resident – do not infect the computer's memory and are active for a limited time.

3. According to the destructive capabilities

Harmless – does not affect the operation of the computer, except for the reduction of free memory on the disk as a result of its distribution.

Non-dangerous-reduce the amount of free disk space and are limited to graphics, sound, and other effects.

Threat – lead to serious malfunction of the computer

Very dangerous – they can lead to the loss of programs, destroy data, erase the information necessary for the operation of the computer, recorded in the system memory areas.

4. According to the features of the virus algorithm.

Student-primitive, contain a large number of errors.

Companion-viruses – viruses that do not modify files. The algorithm is that they create satellite files for EXE files that have the same name, but with the COM extension . Thus, when the application starts, it will first launch a file with the COM extension, i.e. a virus, which will then launch the EXE file. This method of self-launching is also used by Trojan programs. [2]

RESULTS

A Trojan program, Trojan, Trojan is a type of computer program that "pretends" to perform a certain function, but in reality it works completely differently. Some Trojans are initially designed to mislead the user: for example, the program simulates another application (a game, a text editor, an installation program), but in fact performs some unauthorized actions by the user: deleting, modifying information, collecting and forwarding information to third parties, transferring control of the computerto a remote user. Or a standard program can be used as a Trojan: a certain person places a disk formatting program and a command file for downloading under the guise of a "useful" program or updates, which runs it with the necessary parameters.

Viruses – worms-get into the computer's memory from the computer network, calculate the network addresses of other computers and send their copies to these addresses.

Parasitic-all viruses (except worms and companions), which, when distributing their

The American Journal of Engineering and Technology
(ISSN – 2689-0984)
Published: January 31, 2021 | **Pages:** 48-51
Doi: https://doi.org/10.37547/tajet/Volume03Issue01-09

IMPACT FACTOR
2021: 5. 705
OCLC - 1121105677

copies, necessarily change the contents of disk sectors or files. [2]

Stealth virus — a virus that completely or partially hides its presence in the system by intercepting the operating system's access to the affected files, "substituting" for itself the uninfected areas. These viruses have original algorithms that allow them to deceive resident antivirus programs.

Polymorphic viruses - do not have a single permanent code section, difficult to detect,

Macro Viruses-are written not in machine code, but in WordBasic, live in Word documents, and rewrite themselves in Normal . dot .

DISCUSSIONS

There are a number of signs that indicate an infection of the computer: an

Increase in the size of files (especially executable files).)

The appearance of strange, previously non-existing files

Slows down the work of some programs.

Some programs stop working or work incorrectly

Friends or acquaintances tell you about messages from you that you did not send or attachment ;

Frequent freezes and computer crashes;

Slow computer operation when running programs;

Unable to boot the operating system;

The disappearance of files and directories or distortion of their content;

Frequent access to the hard disk (the light on the system unit flashes frequently);

Anti-virus program (antivirus) — a program for detecting and possibly treating programs infected with a computer virus, as well as possibly preventing a file from being infected with a virus. [3]

The first, most simple antivirus programs appeared almost immediately after the appearance of viruses. Now large companies are engaged in the development of antiviruses. Like the creators of viruses, this area has also developed original techniques — but this time for finding and fighting viruses. Modern antivirus programs can detect tens of thousands of viruses.

Antivirus software consists of computer programs that attempt to detect, prevent the propagation of, and remove computer viruses and other malicious programs.

There are the following types of antivirus programs:

Detectors scan the files to search for known viruses that meet the definition in the dictionary of the virus.

Doctors-not only find virus-infected files, but also remove the body of the virus program from the file.

Auditors are the most reliable method of protection. Auditors remember the initial state of programs, directories, and system areas, and then periodically compare the current state with the original one.

The doctor and the auditors. Filters are small resident programs designed to detect suspicious behavior of any of the programs, similar to the behavior of an infected program. Unlike the method of matching the definition of a virus in the dictionary, the method of suspicious behavior provides protection against completely new viruses that are not yet in any virus dictionary. However, it should be borne in mind that programs built on this method also produce a large number of erroneous warnings, which makes the user less susceptible to all warnings.

The American Journal of Engineering and Technology
(ISSN – 2689-0984)
Published: January 31, 2021 | **Pages:** 48-51
Doi: https://doi.org/10.37547/tajet/Volume03Issue01-09

IMPACT FACTOR
2021: 5. 705
OCLC - 1121105677

Suspicious actions are:

Attempts to correct files with COM and EXE extensions;

Change file attributes;

Direct write to disk at an absolute address;

Write to the boot sectors of the disk;

Load the resident program. [4]

An example of a filter program is the Vsafe program, which is part of the MS DOS operating system utilities package.

CONCLUSIONS

Unfortunately, the competition between antivirus companies has led to the fact that the development is going in the direction of increasing the number of detected viruses (primarily for advertising), and not in the direction of improving their detection (ideal-100% detection) and algorithms for treating infected files.

Confession. Vaccines. They are used to process files and boot sectors in order to prevent infection with known viruses (recently, this method is used less and less often - you can only vaccinate against a specific virus, and some antiviruses may well confuse such vaccination with the disease itself, since the difference between the virus and the vaccine is actually vanishingly small). As you know, none of these types of antivirus software provides one hundred percent protection of the computer, and it is desirable to use them in conjunction with other packages. In general, the choice of only one" best " antivirus is extremely wrong.

RECOMMENDATIONS

Methods of fighting computer viruses - do not download or run unknown programs from the Internet) .

Computer users do not have to work with administrator rights all the time. If they used the normal user access mode, some types of viruses would not be able to spread (or, at least, the damage from the viruses would be less). This is one of the reasons why viruses are relatively rare in Unix-like systems.[4]

REFERENCES

1. Voronin P. A. Antivirus programs. , characteristics, application. Moscow: Dodeka, 2001, 384 p.
2. Diakonov V. P. et al. Encyclopedia of anti-virus software devices.. - Moscow: SOLON-Press, 2002. - 512 p.
3. Diakonov V. P. et al. Methods of fighting computer viruses . // Izvestiyavuzov. Instrumentation. - 1980. - No. 4. - p. 6.
4. Diakonov V. P. et al. High-current non-saturable keys on composite transistors / / Electronic industry. - 1981. - No. 2. - p. 56.