DOI: https://doi.org/10.36910/6775-2524-0560-2022-48-04
UDC 004.05(075.8)
Andrushchak Igor Yevhenovich, Ph.D., Professor,
https://orcid.org/0000-0002-8751-4420
Matviiv Yurii Yaroslavovich, Ph.D., Professor,
https://orcid.org/0000-0003-4872-7949
Koshelyuk Viktor Andriyovych, candidate of technical sciences, associate professor,
https://orcid.org/0000-0002-4136-5087
Lutsk National Technical University, Lutsk, Ukraine

COMPONENTS OF VIRUSES AND ANTIVIRUS SOFTWARE IN MODERN INFORMATION SECURITY

Andrushchak I., Matviiv Yu., Koshelyuk V. Components of viruses and antivirus software in modern information security. In fact, in today's conditions of continuous innovative development of technologies, in the field of programming, computer networks and the Internet, the dark side of progress continues to grow at great rates: virus software. As a result, in this article we will try to focus on all aspects of the fight against viruses: prevention of infection, methods of detecting malicious programs, their destruction, as well as elimination of consequences. To do this, we conducted research and study of the main scientific sources on this topic and statistical data. As a result, this article focuses on different types of viruses and analyzes the methods of their classification, detection and destruction.
Keywords: information security, software, cyber security, viruses, antivirus, software product, global networks.

Андрущак І.Є., Матвіїв Ю.Я., Кошелюк В.А. Компоненти вірусів та антивірусного програмного забезпечення в сучасній інформаційній безпеці. Власне, у сучасних умовах безперервного інноваційного розвитку технологій, у галузі програмування, комп'ютерних мереж та мережі Інтернет великими темпами не перестає зростати і темна сторона прогресу: вірусне програмне забезпечення. Як наслідок, у данній статті спробуємо акцентувати увагу на всі аспекти боротьби з вірусами: запобігання зараженню, методам виявлення шкідливих програм, їх знищення, а також ліквідації наслідків. Для цього ми провели дослідження та вивчення основних наукових джерел з цієї тематики та статистичних даних. Як результат, у цій статті, акцентується увага на різних видах вірусів та проводиться аналіз методів їх класифікації, виявлення та знищення.
Ключові слова: інформаційна безпека, програмне забезпечення, кібербезпека, віруси, антивіруси, програмний продукт, глобальні мережі.

Formulation of the problem. From the time of the appearance of the first computers to today, many types of viruses are undoubtedly one of the main reasons for the appearance of certain negative problems in the work of modern computers, leaks of information, including confidential, financial and state information. At the same time, during this time, computer viruses managed to evolve and acquire numerous new types and forms. Now, it costs nothing for any software developer to create a certain virus program according to a developed template, so new malware appears almost every second.

However, there is no doubt that the evolution of antivirus software products is constantly improving. Methods for detecting and preventing malicious activity also continue to evolve significantly. In most cases, there are paid versions of most programs that provide wider functionality in addition to working with viruses: for example, a firewall, VPN. Despite all the advantages, modern security software is far from perfect and has many of its shortcomings. As a result, the actual issue of combating virus programs remains open.

Analysis of research. The concept and basic idea of a mechanical structure capable of self-reproduction, activation, capture and mutation was derived long ago by the American scientist L. Penrose. Certainly the problem of computer viruses may not have arisen, since computers themselves were originally only owned by large and powerful corporations, state government organizations, and similar entities, since the complexity of computers made them an extremely expensive pleasure for ordinary citizens, until Apple released the first available an Apple II personal computer. After many users got a personal computer at their disposal, a virus as a type of program appeared that which in itself enables its existence: a potential habitat and distribution [1].

Since then, many programs have been written to spread and combat various types of viruses. Many of them became a kind of legends. As mentioned earlier, the evolution in the world of information technologies does not stand still and various types of malicious programs have become much more, as a result of which there was a need for a systematic classification of these programs.

Classifying the entire range of programs is quite difficult and not an easy task in connection with various aspects, but it is possible to give a certain basic classification according to key features and

concepts. Specifics such as the affected operating system and features (such as user tracking, data destruction, data theft) can also be added.

Presentation of the main material and the justification of the results. First of all, in the fight against the virus and subsequently the restoration of computer information, there is, of course, the detection of this harmful proprietary product or tool. In certain cases, this is a simple task: the user can independently understand that his computer or laptop has been infected. For example, the Internet browser cannot access certain websites as usual, the home page changes regularly, or the browser itself usually runs slower than usual. Also, users often notice the following signs:

- slow operation or freezing of the computer.
- constantly pop-up notifications on the work browser or desktop.
- unexpected reboots of the computer system.
- error message that system files are damaged.
- lack of access to the command line of the task manager and other system programs.

But there are usually cases when errors in the operation of the operating system or browser are not so obvious and the user calmly performs certain necessary work, but there are viruses on the computer. That is why you should periodically scan all content with antivirus programs that use their own methods of detecting virus software. They can be divided into two main groups:

- *detection of viruses by "dictionary"* - then the antivirus simply scans all files and programs and compares them with the dictionary where existing viruses are entered. If there is a match, the antivirus will delete or quarantine the malware. Of course, in order for this method to cope with its task, it is necessary to update the dictionary and introduce new malicious programs into it. Since there are quite a lot of them these days, most likely, the antivirus dictionary will not contain all the necessary viruses. But most often this is almost enough, because most antiviruses use the dictionary method for detection.

- *detection of viruses on the behavior of programs* - certain antiviruses that work according to this principle monitor how programs behave and what actions they perform. Basically, all the suspicious activity of the programs was reduced to writing new data to the executable file, but now ordinary programs often do the same. As a result, the user receives many false warnings when the antivirus again mistakes an innocent file for a malicious one. It is not surprising that this method is used less and less [2].

Of course, the method of detection based on the behavior of the program can also include the principle of operation of antiviruses that imitate a small part of the code of the program that is launched or imitate the operating system, and only then execute the program on it. It is not difficult to guess that such a check can take a significant part of time, which is why it is used by professionals, and not by ordinary computer users. Instead, it is really effective and can detect all the viruses occupying the laptop. Speaking about certain methods of detecting viruses, we have already mentioned that, of course, the main means of combating pests is antivirus programs. They combine everything the user needs: they find the virus, eliminate it and its consequences, if damage was caused to these or other programs [3].

Analyzing the listed methods of detecting certain types of viruses, we have already mentioned that, usually, the main means of pest control are antivirus programs. They clearly combine everything necessary and necessary for the user: they find the virus itself, eliminate it and its negative consequences, if damage was caused to information or other software products [4].

At the same time, modern antivirus software can be divided into several types, in which the functionality itself is somewhat different:

- *detectors* are the same as the antiviruses described above. They find an existing problem and "cure" it using the dictionary method. They include the banal and well-known antivirus of Kaspersky, Doctor Web.

- *filters* - monitor the disk. When any program tries to register on the filter, the user will be notified about this and will be asked for permission to perform the operation. You can also fight against new unknown viruses, if they interact with the disk and not with the BIOS.

- *vaccinators* - is used only to fight against specific known malware, because the vaccinator needs to take the signs of the virus. It then writes them to the user's secure program, and the virus thinks it is already infected.

- *auditors* - store information about the status of programs and files, and during repeated scanning use them to compare and analyze changes. Many factors are checked: from the size of the files and the time of their creation to the state of the BOOT sector. However, the antivirus itself does not determine whether the file is harmful to it or not. It transmits all data about the changes to the user, who must decide

for himself what caused them. If it is, according to the person, a virus, then the auditor deletes the dangerous data or quarantines it.

Despite the fact that there are many types of antiviruses with different functionalities and principles of operation, as well as a large register of developers of this software product or tool, there are unfortunately also many disadvantages of antiviruses [5].

But no specific antivirus program can unequivocally guarantee one hundred percent protection against any virus. It can be a new unknown virus that is not yet listed in dictionaries, or a strongly encrypted virus. Then you will need a powerful packer, which, of course, is not available in many antiviruses. Moreover, antiviruses like to find threats in safe files. Therefore, ordinary users themselves miss certain warnings about viruses and malicious files, which makes this protection less reliable.

Table. 1 Classification of different types of viruses

Harmfulness	- harmless - programs that can spread in the network, moving from one computer to another, but at the same time do not perform any destructive functions in relation to the system. - safe - malicious programs capable of overloading the memory, generating sound signals, computer images. - dangerous - programs capable of harming the system. - extremely dangerous - viruses capable of destroying data located in various segments and sectors of memory, leading to the breakdown of mechanical parts of the computer.
Habitat	- file - damage to executable files, the habitat of which is respectively COM and EXE files. - bootable - damage to boot sectors (Boot sectors) of hard drives or system boot sectors. - network - damage to computer networks and systems. - macro - damage to Microsoft Office files.
Method of infection	- resident viruses - remain in RAM after the execution of a certain infected program. - non-resident viruses - do not occupy the RAM of the device and are executed only once during the execution of a certain virus program
Features of the work algorithm	- companion viruses - damage to EXE files, in which a duplicate of the COM file is created, after which the file with the virus is first executed, then the file of the program itself. - worms-viruses - spread in the network by calculating the addresses of other devices connected to this network and sending their own copies to these devices. - viruses-parasites - change the contents of files and memory segments of infected devices. - stealth viruses - intercept the access of the disk operating system (DOS) to the affected areas of the disk and substitute uninfected memory segments. - polymorph viruses - do not have parts of the code, therefore such viruses are very difficult to detect. - macro viruses - infect macros in file editors such as Microsoft Word and Microsoft Excel. - viruses capable of self-encryption - change their program code. - viruses with a non-standard algorithm - have their own signatures and structural algorithms, which greatly complicate the detection of the virus

Network interception is a specific process that is carried out using a "man-in-the-middle attack". Special software redirects the user's encrypted connection to any requested site and succeeds. The interceptor then opens a new connection to the source web resource and passes data through itself between the two connections. Because an interceptor has access to most of the data within the connection, they can assume, modify, and block any content transmitted or received by the client. This can be used for both good (blocking malicious sites) and bad purposes (fraud, hacking devices). Programmers of Google, Mozilla, Cloudflare and several companies sharply criticized the processes of interception of HTTPS traffic by antiviruses and network filters [6].

Thanks to the work performed, it was found that the network interception of HTTPS traffic by antivirus programs can threaten the safety of users and their connection to the World Wide Web. Therefore, this software cannot gain specific access to HTTPS packets, but antivirus companies have found a way to analyze the data that goes over encrypted connections: they have started to install their own root certificates on the device, which significantly reduces the security of the connection.

Moreover, the analysis shows that the traffic scanners presented in some antiviruses have even greater vulnerability due to their shortcomings. Intercepted connections use weak cryptographic algorithms and cracked ciphers that can allow attacks on the device and decryption of the connection. Thus, at least about 10% of traffic is intercepted not only by antiviruses, but also by third-party software that uses it, easily deciphers and analyzes it for its own purposes. That is why antivirus companies should think about a new way of collecting information.

However, the actual interception of HTTPS packets significantly reduces the security of the user and his data on the network. Another existing problem is how common network interception is [7].

Measuring the number of existing interceptions is clearly not an easy task, so an improved version of the TLS fingerprinting technology is used to detect the interception. This will determine who is making the connection: the interceptor or the browser. The technology actually evaluates the construction of the client's TLS package (mainly cipher suites and TLS options) and compares it to an existing database that was already known.

Actually, the work processes of the online store, the Cloudflare site and the Firefox update servers were evaluated. However, we looked at exactly how much browser traffic they intercept. And the results, in turn, showed that from 4 to 10% of traffic is intercepted, while 4% are Firefox servers, and 10% are Cloudfare. This is quite a lot, but it should be remembered that some of the interceptions are not carried out by criminals [8].

If you break down the existing intercepted HTTPS packets by operating systems, it turns out that Windows is definitely intercepted much more often than Linux and MacOS. And the traffic itself from mobile devices (IOS or Android) is intercepted less often than from the OS for a personal computer, but not in the case of existing Firefox servers. Oddly enough, however, most of the interception is done by mobile providers. This may be due to the fact that the desktop version of Firefox uses its own separate store for root SSL certificates, thereby reducing the chance of data being intercepted. At the moment, this is one of the main maneuvers that can be a temporary solution to the existing problem of HTTPS traffic interception. But the main disadvantage of the maneuver is that it is provided by the owner of the server and the requested Internet resource, and not the antivirus, which is undoubtedly the initiator of the interception [9].

Thus, we can only determine for sure the main extent of damage caused to the user by network interceptors and only slightly eliminate it, because everything depends on a significant number of factors: the software used and the connection, the requested specific site, the user's device and the operating system itself system on it. But at the same time, it is absolutely impossible to avoid this, until the antivirus manufacturers themselves evolve to a less vulnerable way of controlling HTTPS traffic [10].

Conclusion and prospects for further research

It's impossible not to respect how large a number of different types of viruses exist and are created in the modern world, and also how badly stench it's right to set up coristuvachi computers and Internet. Prote, use a lot of anti-virus programs, even though they don't have a general agreement, but they can save bad or eliminate negative consequences. It is unambiguously necessary for those koristuvachs themselves to learn how to correctly hack as modern antiviruses, so even if they don't know the files that are sent - to that, be it mitigated stench, they can appear shkidlivimi.

Moreover, the distributors of anti-virus software products and services can also do something about it. The methodology for detecting and reducing viruses on a computer is far from ideal, which can change both on the butts of the state, and on a special certificate. Those creators of shkidlivih programs zasobiv do not sit on the job, gradually improving their code and encryption. Itself in such stages of the efficiency of viruses and anti-viruses of the modern coristuvach is unequivocally learned for the help of various software tools and security, various operating systems to secure their own security and the security of their personal laptops.

References

1. Bay H., Ess A., and Tuytelaars T. SURF: Speeded Up Robust Features // Computer Vision and Image Understanding (CVIU). 2008. V. 110. No. 3. P. 346-359.

2. Dukhan E.I., Sinadsky N.I., Khorkov D.A. Software and hardware protection of computer information. Ekaterinburg: USU; 2008. 240 p.
3. Ivanov V.Yu., Zhigalov K.Yu. A technique for detecting traces of malicious software in RAM dumps. cloud science. 2018:5(2):2–5.
4. Kiyaev V.I. Security of information systems. M.: Open University "INTUIT"; 2016. 192 p. Ginodman V.A., Obelets N.V., Pavlov A.A. From the first viruses to targeted attacks. M.: MEPhI; 2014. 96 p.
5. Martseniuk V. Features of multifunctional Backdoor technology. Scientific journal "Computer-integrated technologies: Education, science, production" / V. Martseniuk, A. Sverstiuk, I. Andrushchak, O. Sivakovska, M. Poteichuk // Issue №40, Lutsk. - 2020 - p. 123-127.
6. Martsenyuk V.P. On Application of Latticed Differential Equations with a Delay for Immunosensor Modeling / V.P. Martsenyuk, I.Ye. Andrushchak, P.N. Zinko, A.S. Sverstiuk // Journal of Automation and Information Sciences (Begell House / New York) – 2018. – Volume 50 issue 1. – pp. 55-65.
7. Panov S.S. The five best antiviruses to protect your smartphone. Science and education today. 2018;(3):18–21.
8. Rudnichenko A.K., Shakhanova M.V. Actual ways of introducing computer viruses into information systems. Young scientist. 2016;(11):221–223.
9. Spitsyn V.G. Information security of computer technology. Tomsk: El Content; 2011.148 p.
10. Vlasov D.V., Minaev A.S. Methods for counteracting the analysis of executable files in information systems. Information and security. 2014;17(2):308–311.