Львівський державний університет безпеки життєдіяльності

Національний університет Львівська політехніка

Департамент кіберполіції Національна поліція України

Львівська міська рада

LVIV IT CLUSTER

softserve

UnderDefense

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет "Львівська політехніка"

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

Львів
Растр-7
2022

УДК 351.746:007:004
І 74

Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – Львів: Растр-7, 2022. – 380 с.

ISBN 978-617-8134-79-2

У збірнику опубліковано матеріали IV Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології". На основі теоретичних та експериментальних досліджень представлено інноваційні підходи у сфері кібербезпеки та інформаційних технологій. Обговорено та запропоновано сучасні шляхи щодо захисту інформації як на особистому, так і на державному рівнях.

УДК 351.746:007:004

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

ISBN 978-617-8134-79-2

Zbigniew KOKOSIŃSKI – dr hab. Inż., prof. PK kierownik Katedry Politechnika Krakowska im. Tadeusza Kościuszki;

Volodymyr SAMOTYY – prof. dr hab. inż., professor, Katedra Automatyki i Informatyki Politechnika Krakowska im. Tadeusza Kościuszki;

Sergii TELENYK – prof. dr hab. inż., professor, Department of automatic control and computer engineering Cracow University of Technology;

Володимир РОМАКА – д.т.н., професор, професор кафедри захисту інформації Національного університету "Львівська політехніка";

Іван ОПІРСЬКИЙ – д.т.н., професор, професор кафедри захисту інформації Національного університету "Львівська політехніка";

Любомир СІКОРА – д.т.н., професор, професор кафедри автоматизованих систем управління Національного університету "Львівська політехніка";

Наталя ЛИСА – д.т.н., доцент, доцент кафедри кафедри автоматизованих систем управління Національного університету "Львівська політехніка";

Тетяна ГОВОРУЩЕНКО – д.т.н., професор, завідувач кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету;

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

Андрій Івануса – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Орест ПОЛОТАЙ – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Секція 1

КІБЕРБЕЗПЕКА

UDC 004.491.22

COMPUTER VIRUS: WHAT ARE COMPUTER VIRUSES?

Oleksii Polishevskyi[1], Lyudmila Pet'ko[2]

[1]Student at the Department of Software engineering Faculty of Mathematics, Informatics and Physics Dragomanov National Pedagogical University, sity Kyiv, Ukraine

[2]PhD professor, docent at the Department of Foreign languages Dragomanov National Pedagogical University, sity Kyiv, Ukraine

Abstract. *Described the origins of computer viruses and presented their types according to the degree of influence. Given the notion of computer viruses. Analyzed the names of computer viruses, what can be clearly divided into several groups: names of computer viruses by place of origin, by date of activation, by action, by number of bytes, by characteristic text, visual effect, by author, etc.*

Keywords: *computer viruses, Worms, Stoned virus, Marijuana virus, Israeli virus, Dinamo virus, Pakistani virus, Lehigh virus.*

Анотація. *Описано походження комп'ютерних вірусів та наведено їх види за ступенем впливу. Розкрито поняття* "*комп'ютерний вірус*"*. Проаналізувано назви комп'ютерних вірусів, які можна чітко розділити на кілька груп: назви комп'ютерних вірусів за місцем походження, за датою активації, за дією, за кількістю байтів, за характерним текстом, візуальним ефектом, за автором тощо.*

Ключові слова: *комп'ютерні віруси, вірус Worms, завантажувальний вірус Stoned, вірус Marijuana, Ізраїльський вірус, вірус Dinamo, Пакистанський вірус, вірус Lehigh.*

The user of a modern personal computer has free access to all resources of the machine. This opened up the possibility of a danger called a computer virus. I set myself the following goal: to determine what computer viruses are, how to fight them, which programs work better and more effectively, how to protect a device from viruses.

Computer viruses cause damage in billions of dollars each year, causing system critical errors, shutting down large sites and web applications, destroying or modifying files, and increasing response time.

Viruses pose a threat even to users protected by antivirus software, because they can bypass the system of blocking and protecting the program itself. Viruses are also used by hackers to infiltrate the security systems of some web systems to obtain or destroy certain information.

Viruses act only by software. They usually attach to the file or penetrate inside the file. In this case, the file is said to be infected with a virus. The virus enters the computer only together with the infected file. To activate the virus, you need to download the infected file, and only then the virus begins to act

independently. Some viruses become resident (permanently in your computer's RAM) when you run an infected file and can infect other downloaded files and programs. Other types of viruses can cause serious damage immediately after activation, such as formatting the hard disk.

Computer virus – a type of malicious software that can be embedded in the code of other programs, areas of system memory, boot sectors, and distribute their copies through various communication channels (Fig. 1, 2, see the video [13]).

Depending on the location the viruses can be divided into network, file, boot and file- boot. Network viruses are spread on various computer networks. File viruses are implemented mainly in executable modules, i.e. in files with COM or EXE extensions. Boot viruses are introduced into the boot sector of the disk (Boot sector) or into the sector that contains the boot program of the system disk (Master Boot Record). File boot viruses affect both files and boot sectors of disks [6, 11].

According to the degree of influence the viruses can be divided into the following types:

1. Safe, do not disturb the computer's operation, but reduce the amount of free RAM and memory on disks, the actions of such viruses are manifested in any graphic or sound effects.

2. Dangerous viruses that can cause various computer malfunctions.

3. Very dangerous, the impact of which can lead to the loss of programs, data destruction, erasure of information in the system areas of the disk [2].

In more than 80% of computer crimes investigated by the FBI, hackers enter the attacked system via the global Internet. This process can be automated by a virus called a network worm.

Worms are viruses that spread on global networks, infecting entire systems, not individual programs. This is the most dangerous type of virus, as the objects of attack in this case are the information systems of the state scale. With the advent of the global Internet, this type of security breach poses the greatest threat, as it can affect any of the 40 million computers connected to this network at any time (Fig. 3, 4, see the video [3]).

Fig. 1. Computer Virus

Fig. 2. Computer Virus

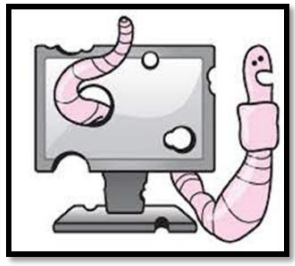

Fig. 3. Virus Worm

Names of computer viruses (Fig. 5). Conditionally, they can be classified as follows according to the following common features:

1) Place of residence:

1. Bootable.
2. File.
3. Boot-file.
4. Network.

2) Level of effects:

1. Relatively safe.
2. Dangerous.
3. Very dangerous.

3) Algorithm features.

1. Invisible viruses
2. Retroviruses
3. Worm-viruses

*4. Trojans Method of infec*tion.

1. Residents
2. Non-residents [10].

Fig. 4. Virus Worm

Mostly the names of computer viruses in modern Ukrainian are borrowed from English, as they have English names, and in Ukrainian they exist as literally translated words or phrases.

Specialists and ordinary PC users make a literal translation of such names into Ukrainian, very rarely giving malware adapted Ukrainian names. Exceptions are viruses created by Ukrainian-speaking or Russian-speaking users, which retain in their names the concepts familiar to such users.

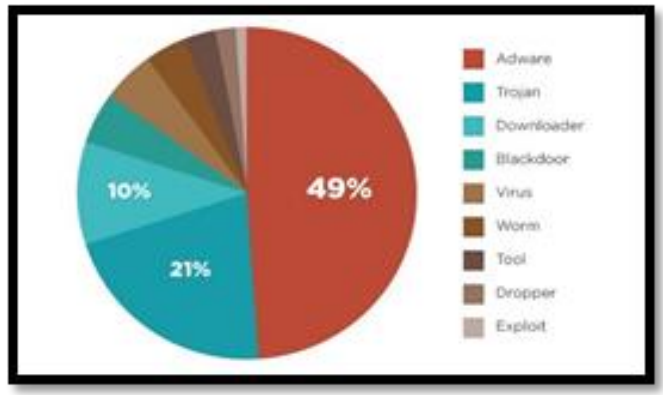

Fig. 5. Rating of the most common computer viruses

Analyzing the names of computer viruses, they can be clearly divided into several groups: names of computer viruses by place of origin, by date of activation, by action, by number of bytes, by characteristic text, visual effect, by author, etc.

Names of computer viruses by date of activation. A separate group of virus names consists of programs that are named after the date when they are activated. For example, the name of the virus ***Black Friday*** is motivated by the fact that if the time of work with infected software falls on Friday the 13th, then infected files are destroyed. Another name for this virus is ***Friday the Thirteenth*** [11], Fig. 6.

The ***Stoned virus*** is so called because when you boot the system, the text '*Your PC is now Stoned'* is simply displayed, after which the work continues (Fig. 7, see the video [1]).

Fig. 6. Friday. The Thirteenth logo

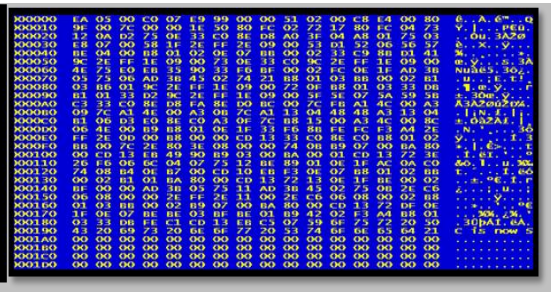

Fig. 7. Stoned virus

The name of the ***Marijuana virus*** is motivated by the phrase *Legalize Marijuana!* which pops up when booting the infected system [11] (Fig. 8).

Fig. 8. Marijuana virus

Fig. 9. Dinamo virus

The Israeli virus (also known as Jerusalem) was first detected at the University of Jerusalem (Israel) in 1987. It is well known in the history of

computer virology for the fact that at one time its spread for the first time became a pandemic among computer systems [10, 5], Fig. 9.

The Jerusalem virus is one of the oldest computer viruses. It infected files in the MS-DOS operating systems that were standard at the time. After DOS operating systems were succeeded by newer types of operating systems, the Jerusalem virus became largely obsolete. The virus also infected executable programs repeatedly until they became too large to run on a computer. Other variants of the Jerusalem virus included additional marginal effects, such as cryptic slogans that would populate the command line interface. Some versions of the virus would apparently restrict the operation of programs during certain days of the week, such as Saturday and Sunday [12].

Dinamo virus displays the phrase: Dinamo (Kiev) – champion !!! – hence the name. Bye! virus name also motivated by the text that follows when booting the system (Fig. 10). The most well-known of these viruses is the Viennese virus. It is one of the first primitive viruses to be discovered in Vienna. When downloaded to computer memory, this virus infects all com programs.

The Pakistani virus (Fig. 11), developed by brothers Amjat and Basit Alvi in 1986, was discovered in the summer of 1987. The malware was supposed to punish local pirates who steal software from their company. The program listed the names, addresses and telephone numbers of the brothers, and this is the first stealth virus (virus-invisible) – when trying to read the infected sector, it substituted its uninfected original [6, 11].

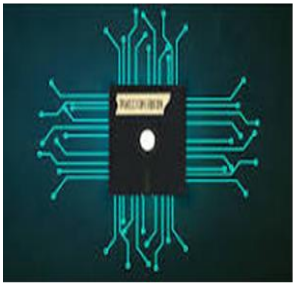

Fig. 10. The Pakistani virus

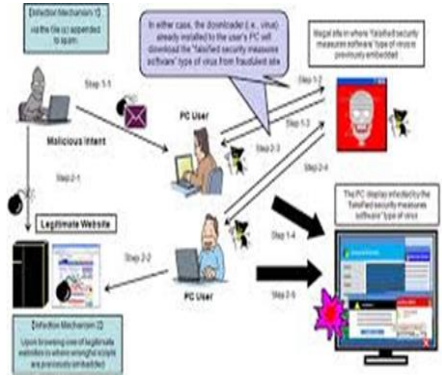

Fig. 11. Types of viruses

The Lehigh virus. Its name is associated with the name Lehigh University (USA), and it was launched in November 1987. Before Thanksgiving 1987, a microcomputcr virus infected several hundred floppy disks at Lehigh University in Bethlehem, PA. The virus was a particularly destructive one; it copied itself

from disk to disk at least four times and then destroyed the contents of the original disk. Each of the copies that were made then went on to do the same thing. This, and the fact that Lehigh University has hundreds of Zenith microcomputers spread all around its campus, on which students shared programs in the form of floppy diskette libraries,proved to bc a rather volatile combination, particularly with Thanksgiving break rapidly approaching. At the time of the viral infection, Lehigh operated approximately 10 microcomputer labs, each one containing an average of between 10 and 15 PCs [4, p. 107].

Within a few days, the virus destroyed the contents of hundreds of floppy disks from the library of the university's computer center and students' personal floppy disks. About four thousand computers were infected during the epidemic [10].

References

1. 500th Video: Virus. Boot Stoned. URL: https://**youtu.be**/kfk4g0iPv74.

2. Cracking: Reversing and Malware Analysis Training Articles. 2012. 60 p. URL: http://index-of.es/Cracking/Malware%20Analysis%20Training_2011_12_Articles.pdf.

3. Malware: Difference Between Computer Viruses, Worms and Trojans. URL: https://youtu.be/n8mbzU0X2nQ.

4. Kenneth R. van Wyk. The Lehigh virus. *Computers & Security*. Vol. 8. Issue 2, April 1989, pp. 107–110. doi: https://doi.org/10.1016/0167-4048(89)90064-3

5. Malwarebytes. URL: https://www.malwarebytes.com/computer-virus.

6. Norton. URL: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

7. Pet'ko Lyudmila. Developing students' creativity in conditions of university // Research: tendencies and prospects: Collection of scientific articles. – Editorial Arane, S.A. de C.V., Mexico City, Mexico, 2017. P. 272−276.

8. Pet'ko L. Multicultural upbringing of students and the formation of professionally oriented foreign language teaching environment // Perspectives of research and development: Collection of scientific articles. – SAUL Publishing Ltd, Dublin, Ireland, 2017. P. 164−170.

9. Pet'ko L. V. Teaching of students' professionally oriented foreign language writing in the formation of professionally oriented foreign language learning environment // Economics, management, law: innovation strategy: Collection of scientific articles. Henan Science and Technology Press, Zhengzhou, China, 2016. P. 356−359.

10. WEBROOT. URL: https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-computer-viruses#:~:text=A%20computer% 20virus%20is% 20a,kind%20that%20makes%20you%20sick.

11. What Are The Different Types Of Computer Viruses? Uniserve. URL: https://uniserveit.com/blog/what-are-the-different-types-of-computer-viruses.

12. What Does Jerusalem Virus Mean? Technopedia Dictionary. URL: https://www.techopedia.com/definition/27875/jerusalem-virus

13. What is a Computer Virus | Tech. URL: https://youtu.be/Ip-u5NZJiwY.

14. What is computer virus? What are various types of viruses? URL: https://www.wired.com/2009/11/1110fred-cohen-first-computer-virus/.

З М І С Т

СЕКЦІЯ 1

КІБЕРБЕЗПЕКА

НАПРЯМ 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

Відповідальні за випуск **Ростислав ТКАЧУК**
Олександр ПРИДАТКО

Оригінал-макет **Ростислав ТКАЧУК,**
Андрій ІВАНУСА

Видано в авторській редакції

Підписано до друку 30.11.2022 р.
Формат 60×84/16. Папір офсетний. Друк цифровий.
Умовн. друк. арк. 22,09. Обл.-вид. арк. 20,55.
Наклад 100 прим.

Видавець і виготовлювач: ТОВ "Растр-7"
79005, м. Львів, вул. Кн. Романа, 9/1.
Тел./факс: (032) 235 72 13. E-mail: rastr.sim@gmail.com
www.rastr-7.com.ua
Свідоцтво суб'єкта видавничої справи
ЛВ № 22 від 19.11.2002 р.

IV International Scientific and Practical Conference
CYBERSECURITY AND INFORMATION TECHNOLOGY
CIT 2022

November 30 - 2022 Lviv - Ukraine

РАСТР·7

ISBN 978-617-8134-79-2