COMPUTER VIRUSES AND VIRUS PROTECTION PROBLEMS

Omonov Fayziddin Komil o'g'li
Telefon: +998(94) 111 14 02
fayziddinomonov7@gmail.com
2nd year student of Oriental University, Pedagogy and Psychology
Abduraxmonova Dilnoza Alisher qizi
Student of the Faculty of Telecommunication Technologies of Tashkent University of Information Technologies

Annotation: *This article is about computer viruses and viruses security problems , computer virus definitions , injecting itself or a modified copy into other programs , downloading Viruses provide information about the program that takes control of the system boot.*

Key words: *Computer virus , twin , companion viruses , MicrosoftWord, MicrosoftExcel .*

Annotatsiya: *Mazkur maqolada kompyuter viruslari va virusdan himoyalanish muammolari, Kompyuter virusining ta’riflari, boshqa dasturlarga o‘zini yoki o‘zgartirilgan nusxasini kiritish, yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur haqida ma’lumotlar berilgan.*

Kalit so’zlar: *Kompyuter virusi, egizak, kompanon viruslar, MicrosoftWord, MicrosoftExcel.*

Аннотация: *В этой статье представлена информация о компьютерных вирусах и проблемах защиты от вирусов, определения компьютерного вируса, внедрения себя или модифицированной копии в другие программы, загружаемых вирусов, программы, которая берет на себя управление загрузкой системы.*

Ключевые Слова: *компьютерный вирус, близнецы, вирусы-компаньоны, MicrosoftWord, MicrosoftExcel.*

INTRODUCTION

There are many definitions of a computer virus. The first definition

In 1984, Fred Cohen said: “A computer virus is a program that infects other programs by modifying them by inserting itself or a modified copy of itself into them. In this case, the introduced program maintains the ability to reproduce further. "

The ability of the virus to reproduce itself and modify the computational process are the basic concepts in this definition. These features of the computer virus are similar to the parasitism of biological viruses in living natural organisms .

Currently, a computer virus is a software code that has the following characteristics:

– the ability to create copies that do not necessarily come asligamos, but have the properties of the original (self-recovery);

- the presence of mechanisms that ensure the inclusion of created copies in the executable objects of the computer system .

It should be noted that these characteristics are necessary, but not sufficient. The specified features should be supplemented with destructiveness and non-disclosure features of the impact of harmful programs in the computing environment.

REFERENCES AND METHODOLOGY

Viruses can be classified according to the following main symptoms: - habitat;

- operating system;
- performance algorithm feature; -destructive capabilities.

It is common to categorize computer viruses according to their habitat, in other words, the types of computer system objects into which viruses enter.

File viruses insert themselves into executable files in a variety of ways (the most common types of viruses), either by creating file-twins (companion viruses) or by exploiting the ability to organize file systems (link viruses).

Bootable viruses write themselves to the boot sector of the disk (boot sector) or to the sector that is the system bootloader (MasterBootRecord) of the Winchester. Download viruses act as program code that takes control of the system boot.

Macroviruses infect macro programs and files of modern information processing systems, in particular Microsoft Word, Microsoft Excel, etc. poisons the files and spreadsheets of mass editors such as

Network viruses use computer networks and email protocols and commands to spread themselves. Network viruses are sometimes referred to as worm-like programs. Network viruses are divided into Internet worms (spread over the Internet), IRC worms (chats, InternetRelayChat).

RESULTS

There are also many combinations of computer viruses, for example, a web macro virus infects editable documents and distributes its copies via e-mail. Another example is file-loading viruses, which infect files and the boot sector of disks.

Life cycle of viruses. As with any program, computer viruses can be divided into two main stages of life cycle - storage and execution stages.

The storage phase corresponds to the period of storage of the virus on the disk together with the object into which it was inserted. At this stage, the virus is vulnerable to anti-virus software because it is inactive and cannot monitor the operating system for protection.

The execution cycle of computer viruses usually includes five stages:

1. Loading the virus into memory. 2. Search for the victim.
3. Poisoning the found victim.
4. Performing destructive functions.
5. Transferring control to the virus program carrier.

Loading the virus into memory. Virus memory access is performed by the operating system simultaneously with the executable object into which the virus is

inserted . For example, if a user runs a program file that contains a virus, the virus code will obviously be loaded into memory as part of that file. Normally, the process of loading a virus is copying from disk to RAM, and then control is transferred to the virus body code. These actions are performed by the operating system, the virus itself is in a passive state. In more complex tasks, the virus may perform additional actions after taking control. There are two aspects to this.

The first is related to the maximum complexity of the virus detection procedure. During the storage phase, some viruses use a fairly complex algorithm to ensure protection. Such complexity can include encryption of the main part of the virus. But using only encryption is a short-term solution, because the part of the virus that provides the decryption must be kept in plain sight during the loading phase. To avoid this situation, virus developers use the decryption code "mutation" mechanism. The essence of this method is that when a copy of the virus is introduced into the object, its decryption part is modified in such a way that textual differences with the original appear, but the result of the work does not change.

CONCLUSION

the code mutation mechanism User viruses are called polymorphic viruses . Polymorphic viruses (polymorphic) are viruses that are difficult to identify and do not have signatures, that is, they do not contain any constant part of their code. Polymorphism occurs in file, download and macro viruses.

REFERENCES:

1. Марков А. С., Барабанов А. В., Дорофеев А. В., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С.Маркова. –М.: ДМК Пресс, -2017. – 224с.
2. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtoyeva. Kriptografiyaning matematik asoslari. O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 192 bet.
3. Akbarov D.Y. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi // Toshkent, 2008, 394 bet.
4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.
5. Raef Meeuwisse. Cybersecurity for Beginners (2nd. ed.). Cyber Simplicity Ltd, London, England, 2017, - 224 p.