KEYLOGGER PROGRAM FOR EDUCATIONAL PURPOSES

A.A. Golovan, E.S. Pankratova, A.V. Agureeva

Samara National Research University, Samara, Russia

Background. Ensuring information security is a topical area today. There are more and more types of computer viruses. However, many ordinary users are not even aware of the risks. The main problem is the ignorance of users, the lack of ideas about the vulnerabilities of operating systems.

Aim. To determine how aware of the risks associated with information security the students-programmers of our university are, to identify the vulnerability of the Windows operating system and then create a program.

Method. To identify the scale of the problem, we decided to survey the students-programmers of our university. A keylogger was chosen as a program demonstrating the capabilities of virus software. We created a demo version of the program, disguised as legal software. Technologies such as Windows Forms, C# and Java programming languages were used.

Results. We have presented the results of the survey (Fig.); As you can see, only 13 % of students use software from trusted publishers. Another 56 % admitted that they are ready to download software from any unverified publisher if they like the product. Unfortunately, hackers take advantage of this. So, the question was, how to force the user to download virus software? Offer them a unique, free, legal product. Each user has already downloaded such programs (at least once).

In order to demonstrate the vulnerabilities of the Windows operating system, we have created a keylogger program. Keylogger is a program that can receive data about keystrokes on your keyboard [1]. This type of virus is not detected by most antivirus programs [2]. Keyloggers can intercept information from the clipboard. You will need a simple program that users may want to download. It could be a game or a music player. The files of this program will contain a keylogger running in the background. Special software will send data to a remote server, process it and extract useful information. Our program is an organizer for a computer.

The keylogger was written in the C# programming language, which allows you to receive data on keystrokes for a certain period. Every 100 ms we get information about the pressed keys. This allows us to get a log file that stores all the information sent by the victim.

The keylogger is wrapped in “friendly” software and hidden in the files of an organizer we have written. The organizer was written using Windows Forms technology.

The server was written in Java. The main task was to send responses to user queries, and to save data collected by the keylogger to the database.

Conclusions. No matter how secure the operating system is, there will be vulnerabilities that hackers can exploit. Most users are still unaware of how easy it is to download virus software, as the survey showed. We were able to find a vulnerability in the Windows operating system and create a demonstration keylogger program based on it.

Keywords: Computer viruses; Operating system vulnerabilities; Virus software; Information Security; Keylogger.

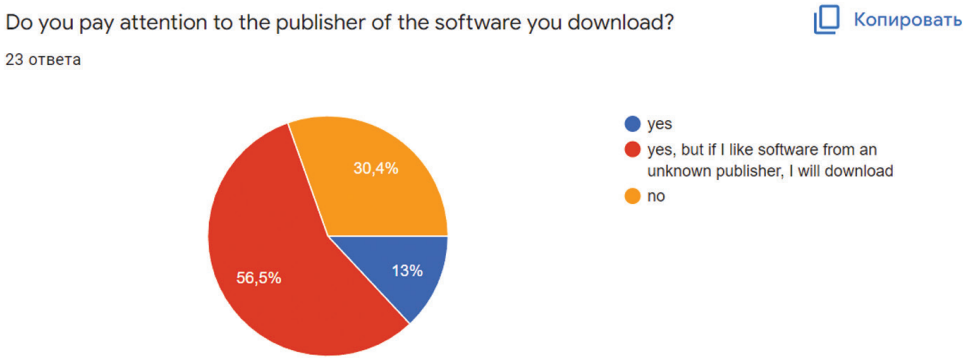

Fig. The results of the survey

References

1. Zaitsev O. Skeleton keys. The purpose and applications of keyloggers // Network Security. 2010. Vol. 2010. No. 10. P. 1–20. DOI: https://doi.org/10.1016/S1353-4858(10)70126-4
2. Vybornykh V.V., Sergeeva I.I. Output spies and methods of protection against them (дата обращения: 30.07.2022). Доступ по ссылке: https://elibrary.ru/item.asp?id=17933904&ysclid=l7g2m1pqg7897910640

Information about authors:

Anna A. Golovan — student, group 6207, Faculty of Information Technologies; Samara National Research University, Samara, Russia. E-mail: golovanshalom@gmail.com

Ekaterina S. Pankratova — student, group 6207, Faculty of Information Technologies; Samara National Research University, Samara, Russia. E-mail: ccoo00@yandex.ru

Alina V. Agureeva — PhD (Pedagogical Sciences), Associate Professor of Department of Foreign Languages and Russian as a Foreign Language; Samara National Research University, Samara, Russia. E-mail: midalina@mail.ru