Internasional Journal of Integrative Sciences (IJIS)
Vol.2, No.6, 2023: 855-860

Keylogger Threats in Computer Security Aspects

Samsoni[1], Ditonius Zebua[2], Basir[3], Bayu Aji Pamungkas[4], Hafidsyah Eka Prayogi[5], Rifaldie Muhammad[6], Supri Wahyudi[7], Wira Samudra[8*]
Pamulang University
Corresponding Author: Wira Samudra uwiera@gmail.com

ARTICLEINFO

Keywords: KeyLogger Threat, Computer Security

Received : 5 April
Revised : 17 May
Accepted: 20 June

ABSTRACT

Along with the development of increasingly advanced technology, the level of need for information security is very important. With the development of information, new problems arise regarding computer security, an example of computer security that often occurs is data theft. Data security in accessing a computer is a form that must be considered both physically and non-physically. One form of data theft crime is recording traces of a computer keyboard with the help of hardware or software. Keylogger is a data theft technique by recording typing on a computer keyboard, by recording when the computer is entered, intruders can enter and steal it. The purpose of this paper is to understand how keyloggers work so that prevention can be carried out by carrying out various kinds of solutions and also to maintain data security systems and know supporting and anti-keylogger software

DOI: https://doi.org/10.55927/ijis.v2i6.4520
ISSN-E: 2985-9050
https://journal.formosapublisher.org/index.php/ijis

INTRODUCTION

A. Background

In today's technological era, the shadow of cyber attacks always overshadows data security. Not only personal information, all data in the system can be infiltrated and misused by irresponsible parties. Keyloggers are a very dangerous form of hacking.

Keyloggers have been in use since the 1970s and continue to grow. Nowadays, keylogger hacking methods are implemented via more sophisticated software. The purpose varies, but the most common is to access important data or information in a database system.

Advances in information systems have provided many conveniences for human life. Even so, there are still many negative aspects, such as computer crime or attacks by irresponsible groups in the form of wiretapping of computer network data. This is due to lack of proper security and ignorance of the public. Even the victim of this wiretapping did not know that someone was eavesdropping on him. Not only that, eavesdroppers also record and monitor the activities carried out by users. In fact, there are still few solutions that are suitable for detecting or preventing these wiretapping activities. Current network intruder detection systems are often able to detect various types of attacks but fail to take further action.

B. Research Objectives

The purpose of this article is to understand how the computer security threat known as KeyLogger works and how to prevent it in order to maintain system security in protected information systems and to find KeyLogger supporting software.

According to Hamzah (2004) in his book entitled Aspects of crime in the computer domain, he considers the concept of computer crime to refer to unauthorized activities using computers, not criminal acts. Even any influence or influence resulting from unauthorized or illegal use of a computer is a crime. In a narrow sense, computer crime is an act against the law that is carried out using the latest computer technology.

LITERATURE REVIEW

A. Definition of Keylogger

Keylogger is a hacking method that is carried out by secretly recording computer keyboard activity. This attack is in the form of spyware or malicious software that is usually attached to emails. If spyware is installed on the computer, the hacker can record every keystroke on the computer device's keyboard.

Keylogger is a dangerous hacking activity that must be watched out for. The data that has been gathered from the keyboard recordings allows attackers to obtain important and sensitive information.

Keyloggers have the ability to sit between the keyboard and the operating system stealing all communications without the user's knowledge.

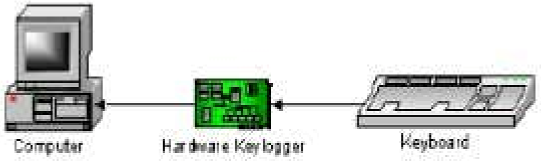

Figure 1. Hardware Keylogger

1. **Computer security**

Selon Howard (1997) and son livre "An Analysis of Security Incidents on The Internet" state that information security is a preventive action related to office user attacks or irresponsible access to the network.

Selon l'assistant dans son live "Securing Computers from Spywere : 2007" Sécurité des données et des medias ainsi que des communication (Sécurité de la communication). There are several types of security of this type that are part of the failover logic, on top of the application logic and application logic used to acquire the database.

The security attack model according to Stallings (1995), consists of:

1. Crashes: System devices become corrupted or unavailable. The attack is directed towards system availability. An example of an attack is a "denial of service attack".
2. Interception: An unauthorized party manages to access assets or information. An example of this attack is wiretapping
3. Modification: An unauthorized party not only manages to access, but is also capable of alteration (damage) of assets. Examples of this attack include modifying website content with messages that are detrimental to the website owner.
4. Fabrication: Unauthorized parties enter counterfeits into the system. An example of this type of attack is to enter a fake message such as a fake e-mail into a computer network.

B. **Types of KeyLogger**

Based on the attack method launched, keyloggers have different types. The following are several types of keyloggers that must be known:

1. Packet analyzers

   Packet analyzers are the easiest and most frequently used spyware. As a type of keylogger, packet analyzers are able to record all keyboard activity and capture network traffic related to HTTP POST. Furthermore, this spyware will steal important information as well as unencrypted passwords.

1. Hypervisor

   Just like other types of keyloggers in general, hypervisor is malicious software whose function is to record all keystrokes on a computer keyboard. The most popular examples of hypervisors are Blue Pill or AMD-V.

2. Spyware kernel-based

   Spyware is a very powerful type of keylogger. This spyware is often used by reliable and experienced hackers. Kernel-based spyware is difficult to fight because the existence of the kernel itself is quite difficult to detect on computer devices.

3. Keylogger API keyboard
   The keyboard API keylogger is spyware that attaches to and works with the operating system. Just like other keyloggers, the way this spyware works is to record and record all the typing on the victim's keyboard keys automatically. Examples of well-known keyboard API spyware are GeaAsyncKeyState and GetForeground- windows.
4. Spyware forms
   In contrast to other types of keyloggers, form spyware only records data through forms submitted by attackers. This attack method is carried out by recording the delivery function on the website. Therefore, the resulting data or information is in the form of HTTPS language encryption.
   To detect the presence of a hardware keylogger, we can only rely on our own eyes to see directly the existence of a "suspicious object" installed between the computer and the keyboard.
   1. Hook Method
      To understand the working principle of keylogger software, we must first understand the working principle of the Windows operating system in handling input from the keyboard. Whenever a user presses a key on the keyboard, Windows captures the input the user entered, then forwards that keyboard input to the intended application using system messages.
   2. Anti Keylogger
      Anti Keylogger method as far as is known, there is no definite method that can be used to detect keyloggers. The most frequently suggested methods are observing the applications running on the system, installing antivirus, anti spyware and firewall etc. but neither of those methods is a specific solution for keyloggers. The methods that have been mentioned can still be overcome easily by using certain techniques that are not discussed here.

2. How to Avoid KeyLogger

After knowing the dangers of keyloggers, you have to be more vigilant so that you don't get attacked by them. Here are some ways to avoid keyloggers:

1. Implement two-factor authentication
   Two-factor authentication security method is a double protection measure to protect account security. To log in to the system, you must enter a unique code sent by the system itself as additional authentication. This will minimize the occurrence of hacking because the code used generally can only be used once.
2. Make an Update
   The latest version of the software certainly has a security patch that is stronger than the previous version. The security system continues to be developed so that the software is not easily exposed to cyber attacks. For this reason, it's a good idea to update your operating system, browser, and apps that you use frequently.

3. Strengthen password
   You can strengthen your password by combining uppercase, lowercase, symbols and numbers. Use long characters to make it less predictable for hackers. Besides, you are not advised to use the same password on multiple accounts.
4. Use anti-spyware and keylogger software
   Anti-spyware programs or software will help detect and clean the device from hacking keyloggers. As long as the keylogger is in the form of software, the use of anti-spyware is very effective in protecting computer devices. There are tons of free software that you can choose from, for example Avast Free, AVG Free, SpywareBlaster, SUPERAntiSpyware, and so on.

METHODS

How does this keylogger work on our computer. Usually the keylogger is implanted by hackers on the victim's computer using viruses and trojans as intermediaries. The viruses and trojans they send will install a keylogger on the victim's computer. So that after the key logger is installed on the victim's computer, hackers will easily gain control of the victim's computer, including stealing confidential data from the victim's computer. The keylogger runs in the background (hidden) without the knowledge of the computer owner.

In order to install a keylogger, physical access to our computer is required. One of them has been mentioned above by Dewaweb, namely through an email attachment. In addition, attackers can also directly install it on the target computer.

Spyware that has been installed will continue to operate without the knowledge of the victim. The keylogger will record and record all keyboard activity in the form of a log file. Then the log files are usually sent directly to the owner of the spyware automatically.

So, the log file in question contains a collection of important data including the username and password that the victim has typed. Furthermore, the attacker uses the data to break into certain accounts, for example hacking the victim's e-banking account.

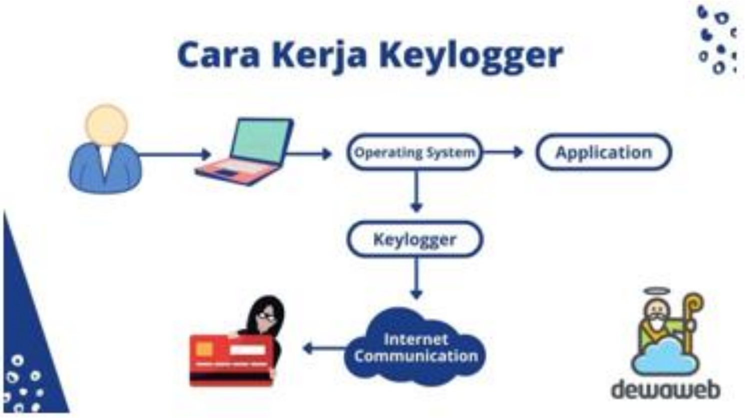

Figure 2.Keylogger Working Model

RESULTS

1. The essence of computer security is to protect computers and their networks with the aim of securing the information contained therein. Prevent system attacks.
2. Because of that we need to pay attention to things that can be detrimental in the data security process.
3. The process of recording keystrokes is something that can happen anywhere without us knowing it, the most important thing for data security is to always monitor the use of data storage media, network and always use the latest anti-virus

CONCLUSION

There are many techniques for securing data and information stored on storage media on computers. Among them is Always keep an eye on the software installed on the computer.

Looking at the structure of the computer hardware there is nothing suspicious. This technique must be applied if we do not want the risk of losing important data. However, the selection of this technique needs to be done carefully.

REFERENCES

Hasibuan, M. S. (2018). Keylogger pada Aspek Keamanan Komputer. Jurnal Teknovasi: Jurnal Teknik dan Inovasi Mesin Otomotif, Komputer, Industri dan Elektronika, 3(1), 8-15.

Hidayat, W., Syahputra, M. A., Amrullah, M. F., Susanto, L., & Putri, A. S. (2023). Analisis Upaya Meningkatkan Keamanan Komputer Terhadap Ancaman di Lingkup Mahasiswa. Indonesian Technology and Education Journal, 1(1), 29-36

Sutarti, S., Pancaro, A. P., & Saputra, F. I. (2018). IMPLEMENTASI IDS (INTRUSION DETECTION SYSTEM) PADA SISTEM KEAMANAN JARINGAN SMAN 1 CIKEUSAL. PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 5(1).

Sinaga, A. S. R. (2020). Keamanan Komputer. CV INSAN CENDEKIA MANDIRI.

https://kumparan.com/how-to-tekno/keylogger-cara-kerja-sejarah-dan-cara-menghindarinya-1vrVWHW7bNb

https://www.dewaweb.com/blog/pengertian-keylogger/ John D. Horwart, Analisis Insiden Keamanan Di Internet 1989-1995, tesis PhD,

Teknik dan Kebijakan Publik, Universitas Carnegie Mellon.

W. Stallings, 1995, “Jaringan dan Keamanan Internet,” Prentice Hall

Wicak, hidayat, 2007, Mengamankan Komputer Dari Spyware. (Jakarta: Media Kita).