International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Survey on Keyloggers: A Monitoring Tool

Ajay Babu N V[1], Feon Jaison[2]

[1]Master of Computer Application, [2]Assistant Professor,
[1,2]Jain Deemed-to-be University, Bangalore, Karnataka, India

ABSTRACT

A Keylogger is a tool that is used to capture keystrokes and other sensitive details from a target computer such as Pin codes, Passwords and System Information and send the collected details to the attacker without the knowledge of the victim. Keyloggers poses a big threat to business transactions such as E-commerce, email chats, online banking or the system database. There are legitimate uses for keylogger including parents monitoring their children and employers keeping an eye on the employees to make sure that they are working at the office time. This paper gives description about keyloggers, its types, the method they use and also how can we prevent the attack of a keylogger.

KEYWORDS: *Keylogger, Software keylogger, Monitoring, Capturing*

How to cite this paper: Ajay Babu N V | Feon Jaison "Survey on Keyloggers: A Monitoring Tool" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1542-1544, URL: www.ijtsrd.com/papers/ijtsrd35704.pdf

IJTSRD35704

I. INTRODUCTION

Security threats and attacks are increasing day by day and the need for cyber security is increasing everyday. Many antivirus and other security tools are being introduced by many vendors in order to keep our computer from being infected by attacks like viruses, malwares, phishing, keyloggers and others.

Keylogger is an advanced type of threat to a computer system because its difficult to detect. Keylogger's once entered in a computer works without the knowledge of the user and records all the keystrokes and other sensitive information from the computer. Details of Email account, Facebook account or any other social media accounts can be captured using a keylogger without letting the user's knowledge. String matching is a technology used in keyloggers to make it faster and comfortable. String matching is a character matching technique which checks every incoming character.

II. Types of keyloggers:

Keylogger is a tool that is used to capture keystrokes and other sensitive details from a target computer such as Pin codes, Passwords and System Information and send the collected details to the attacker without the knowledge of the victim. Keyloggers are mainly of four types based on the way it logs the keystrokes: hardware, acoustic, wireless intercept and software. Although all these types of keyloggers have different methods of capturing the information, they have one thing in common; they save the captured information in a log file.

A. Hardware Keylogger:

Hardware keylogger is a physical device connected between the computer and the keyboard. They capture all the keystrokes made by the user and stores it in the physical memory. A hardware keylogger can be used in either two ways; keylogger can be connected between the computer and the keyboard. Example for this type of keylogger is PS/2 and the USP keylogger.

Second method is to install the keylogger circuit into keyboard standard. This method does not require any physical connection with the computer. This method is dangerous than the first method because it's much more difficult to identify this type of keylogger.

B. Acoustic Keylogger:

This is a complex and rarely used keylogger. Acoustic keylogger uses the principles of acoustic cryptanalysis to record the keystrokes. Each key on a keyboard has a different acoustic signal irrespective of the keyboard used. This method is very time consuming and the data that is captured may not be as accurate as the data captured by the other keyloggers. Sound capturing microphones are used in this type and are kept in the workspace area or in a remote location to listen to the keystrokes.

C. Wireless Keylogger:

Wireless keylogger uses Bluetooth interface to send the captured data to the log file which is located within the distance of 100M. The primary goal of the wireless keylogger is to capture the packet transmitted from the wireless keyboard which uses 27 MHz of RF connection of RF

encrypted transported keystroke character. The main thing about the wireless keyboard is that it needs an antenna/receiver near the target work area.

D. Software Keylogger:

Software keylogger collects the keystrokes between the keyboard and operating system. Their monitoring is mainly based on the operating system. They log's and monitors all the keystrokes made by the user, store it in a remote location and send it to the attacker who installed the keylogger in the computer. A software keylogger is mainly installed in a system by downloading attachments from an untrusted email or a website.

III. Software Keylogger Categories:

Software keylogger has four main types; interrogation cycle, root kits keylogger, traps keylogger and kernel mode keylogger. These categories are made based on the operation of keylogger.

1. Interrogation Cycle Software Keylogger:

Interrogation Cycle Software Keylogger uses different API functions that return information to int variables and custom functions to return char during function call. This is a simple type of keylogger and which can be easily detected. Get A sync Key State function is used ensure whether a key is up or down at the time of the function call. The Get Keyboard State copies the status of all the keys in the keyboard and returns the state of each key. To avoid data missing it is used with high speed interrogations 10-20 polls each second.

2. Traps Software Keylogger:

Generating of keyboard spyware that supported trap of hook mechanism is considered to be classical method. This mechanism works just for GUI applications to trap not only the keystrokes themselves but, message that are processed in window of other GUI application as well. For purpose of installation hook mechanism, the hook handling code has got to be put in a DLL, with the help of API functions. The Set WindowHookExfunction performs installation of an application defined hook procedure into a hook chain, and unhooks WindowHookEx function helps for removal of the hook. When SetWindowHookEx function is called, the keylogger determines which sort of message called the hook handler.

3. Rootkits Software Keylogger:

The rootkits software keylogger is more dangerous than any other keyloggers and are rarely used. They capture's the functions responsible for the processing of the transmitted messages. It has functions like Get Message, Translate Message library, and PeekMessage user32.dll to capture the message and monitior the messages received by GUI applications. Rootkits software keylogger interprets the messages easily using these set functions and methods.

4. KernelMode Software Keylogger:

As the name tells, keylogger resides inside the OS kernel of the computer and records all the key stroke that pass through the kernel. Since the kernel based keylogger is difficult to write, it is rarer than other software keyloggers. As the keylogger is located in the kernel of the system it is very difficult to find out. It is transferred via rootkits and malicious software can evade the kernel and target the hardware.

IV. How does a keylogger works?

The working of a keylogger happens between two steps, when a key is pressed and when the keystroke is displayed in the monitor. When the victim enters any key in the keyboard the keylogger software installed in the system captures all the keystroke that are made by the user. Every keystrokes from the keyboard gets recorded in the keylogger which stores it in a remote location and later sends it to the attacker's email id. The attacker would have already mentioned the time interval for the keylogger to capture the information being typed in the keylogger and send to the attacker. The data that is being send can be sensitive information that can result in attack over the system. As the keylogger is hidden and is not easy to detect the victim is unaware that they are being monitored and the details are being transferred.

V. How does keylogger gets in your computer?

Keylogger can be installed in a computer through many methods.

- A keylogger can be installed in your computer by opening attachments from an untrusted email or any other messages.
- It can be installed through an infected site.
- It can be installed by any malicious programs that are already present in the system.
- It can be installed by a file launched from an open-access directory of P2P network.

VI. Detection and prevention of keyloggers:

Some of the keyloggers can be easily identified by an antivirus software, while others are a bit difficult to identify because a keylogger is designed like a legitimate software that can bypass the antivirus or anti-malware software. If you suspect that a keylogger is installed in your system, even if the antivirus software is not able to detect the keylogger, you can use windows task manager to identify one. Launch the task manager and watch out for any unidentifiable process running. You can also use the windows firewall for incoming and outgoing data.

Prevention of keylogger can include some of the following steps;

- Turn of the computer when not in use.
- Update the security patches as early as possible.
- Use an update antivirus and anti-malware software.
- Enable safe surfing by enabling web filtering to block access to malicious sites.
- Use a keylogger detection software.
- Enable access controls in the system and enable only necessary protocols on end point devices.
- Use virtual keyboards whenever possible.
- Check for hardware keyloggers and remove it.
- Perform continuous scans.

VII. What should be done if you are infected by keylogger?

If one of your system or more than one system is infected by a keylogger, the following steps is to be followed.

- Disconnect the system that is infected from all the network and isolate that system.

- Scan the computer for the keylogger and get the log file to find out the data that has been send to the attacker.
- If it's a hardware keylogger, remove it from the system.
- Change all the passwords of the affected system including the network password.
- Notify the management.

VIII. Conclusion:

Keylogger is a monitoring tool that is used to capture keystrokes and other sensitive details from a target computer such as Pin codes, Passwords and System Information and send the collected details to the attacker without letting the victim know. Keyloggers poses a big threat to business transactions such as E-commerce, email chats, online banking or the system database. Some of the keyloggers can be easily identified by an antivirus software, while others are a bit difficult to identify because a keylogger is designed like a legitimate software that can bypass the antivirus or anti-malware software. A keylogger attack can be prevented if we enable the preventive measures in our system and do a regular checkup.

IX. References:

[1] Hemita Pathak, A. P. (2015). A Survey on Keylogger: A malicious Attack. IJARCET, 2,3,4.

[2] Malwarebytes. (n.d.). Retrieved from https://www.malwarebytes.com/keylogger/

[3] Olzak, T. (2008, May). Keystroke Logging. Retrieved from Research Gate: https://www.researchgate.net/publication/228797653

[4] Rahim, R. (2018). Keylogger Application to Monitoring Users Activity. Journal of Physics: Conf. Series 954 , 2,3.

[5] SoftwareLab.org. (n.d.). Retrieved from https://softwarelab.org/what-is-a-keylogger/

[6] Veracode. (n.d.). Retrieved from https://www.veracode.com/security/keylogger

[7] Yahye Abukar Ahmed, M. A. (2014). Survey of Keylogger Technologies. International Journal of Computer Science and Telecommunications, 2,3,4.