Cyber Security – KEYLOGGERS Comparison of Detection Techniques & Its Legitimate Use

Aaradhya Gorecha

Information Technology Department SVKM NMIMS MPSTME, Shirpur, Maharashtra, India.

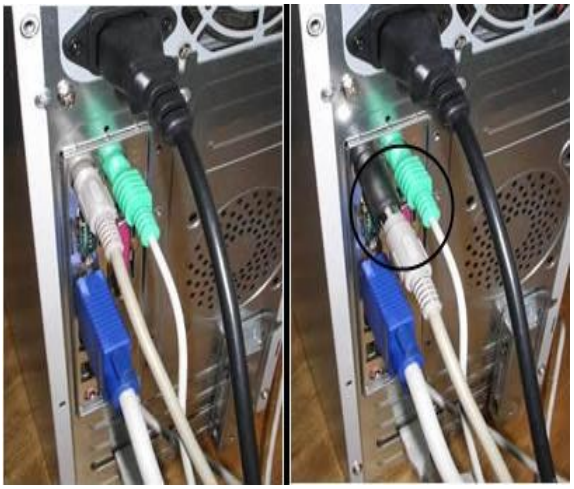
ABSTRACT

This paper presents an introduction of key loggers with explaining the different types and comparison of different detection techniques overview. Also how one of these technique which could be used for keeping to keep a watch on the children web activites to guarentee their protection from online predators and dangers. And also organizations can also use this technique to monitor their employee's activity on internet.

Index Terms:- Keyloggers, hooking, KLIMAX, OS.

1. INTRODUCTION

Keyloggers are software or hardware tools which capture the computer user's keystrokes and then send this information back to attackers. Keylogger has some bad reputation in the world of technology because it is often linked with illegal use of the someone personal data. But it can also be used for some of the legal functions. An example can be taken as of the company security purpose, which states that web activities of workers can be checked and keylogger can be used to monitor any employee, which is suspected of being a insider threat. An inexpensive tool like keylogger can be used to save a large amount of damage of any company .Also parents can use these to keep a check on the web activity of their children to guarentee their protection from internet as their could be misuse of that by childrens.



Mainly keyloggers are divided into two types Hardware keylogger and Software keylogger. Hardware key loggers are the electronic devices used for keystroke logging or capturing the information between the keyboard device and input/output port. These type of devices have a inbuilt storage where they capture the keystrokes so a person who had installed it on the system can get the information of all the activities done on that system.

Software keylogger programs are made to work on the target operating systems.Itcolletcts the data travelling along the keyboard and the OS.

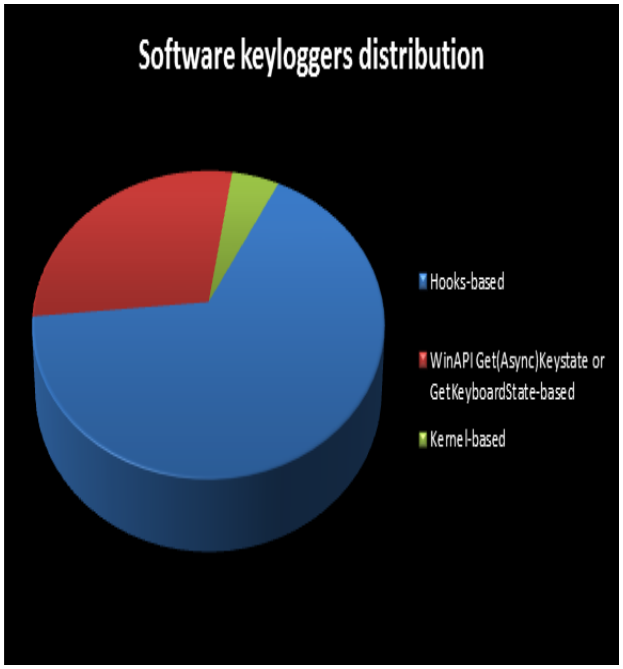
Software keylogger intercepts the keystroke events, stores them in a remote location, and then sent to the attacker who is already having a keylogger software installed.

Research about the removal of spyware founded a total of 540 keyloggers and they were found to be mostly software based keyloggers.

Window operating system has many event mechanisms which provide the information to the keyloggers, for example when a character is pressed on the keyboard or mouse is clicked, the keyboard driver on the operating system translates this event into a window message called as WM_KEYDOAWN.

Characteristics of keylogger Software key loggers have characteristics that captures the user information without depending on a keyboard keystrokes as the sole input. Some of these characteristics include:

- Clipboard logging.
- Screen logging
- Chatting Monitoring
- Program / Tracking Application
- Site Monitoring
- E-mail Reporting
- Password Protection
- The recording of all the search engine queries, downloads and other Internet-based activities.

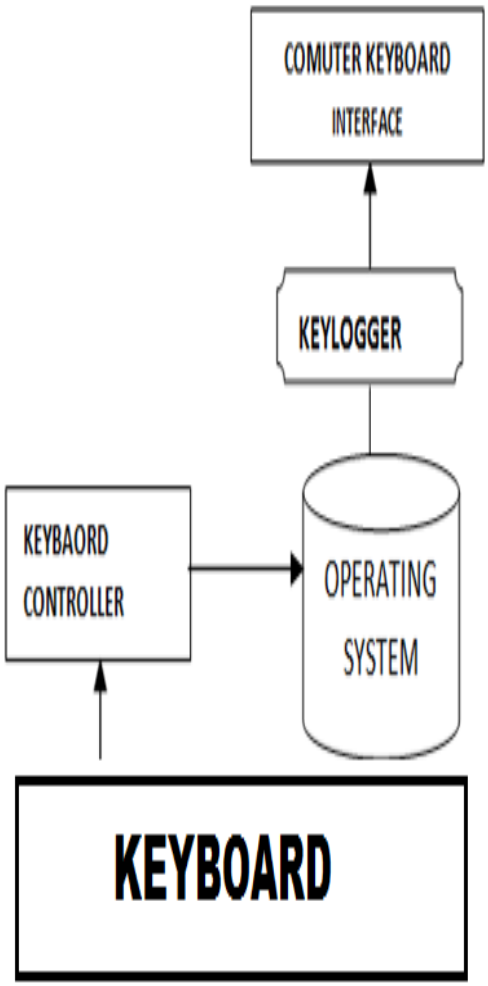


Since Keyboard is the primary target of most common keyloggers so how the keyboard works?

It consists of the matrix of circuit with keys known as key matrix, there are many different types of key matrix available depending on the keyboard manufactures.

The circuit closes key matrix when the user presses a key, then the keyboard processor and ROM detect this event.[3] The processor then translates the circuit location to a character or a control code and sends it to the keyboard buffer. The computer's keyboardcontroller receives the keyboard data which is coming and forwards it to the windows operating system. Data travelling between the operating system and a computer keyboard interface is intercepted by a keylogger. The flow the message is not forwarded

to the upcoming hook procedure .



2. COMPARING THE DETECTION METHODS

Comparison of Detection Techniques

No	Paper Name and Author	Keylogger Detection Technique	Results	Future scope
1	Aslam at el. (2004) AntiHook Shield against the Software Key Loggers.	This paper describes the anti-hook technique to scan all the processes and static executables and DLLs of the system.	Since hook technique is the core of the detection of keylogger. So it can easily find all the suspicious files and processes which are present on any level.	This technique requires much more calculation to be doe and also the false positive rate is very high.
2	Stefano at el. (2011). KLIMAX Profiling Memory Written Patterns to Detect the Keystroke-Harvesting Malware	Behavior based detection technique using KLIMAX (Kernel- Level Infrastructure for Memory and execution profiling)	They proposed using KLIMAX to diagnose and detect malware with normal keylogging behavior. Also, Almost every malware sample was classified incorrectly by many antivirus programs with keylogging behavior.Therefore a proposed model in this paper can potentially be reused to identify other sections of malware.	Malware theft techniques that delaythe information leakage are not concern for this detection technique.Also this detection technique can be proposed for broader range of malicious activities.
3	Le at el. (2008). Detecting Kernel Level Keyloggers Through Dynamic Taint Analysis	host-based IDS dynamic taint analysis to detect kernel level key loggers.	Framework can accurately detect kernel keylogging activities and identify their main causes.	Integration with VMscope and Panorama techniques can improve their efficiency.

Profiling Memory Written Patterns to Detect the Keystroke-Harvesting Malware can be used for the domestic purpose such as for the use of parents and organizations to keep a watch on their children/employee web activity which can help to the safety from online risks.As discussed in the paper of Stefano at el. (2011), the new behavior-based detection model has been introduced based on memory writing method framework, which is especially important for privacy-infringement malware, which demonstrates kelogging behavior.

KLIMAX Design and Implementation: Based on their new model, the kernel-level infrastructure and memory and execution frameworks are to be deployed transparently on the ongoing Windows platform.[1] The source code used is available for allto download. So these software could be made available at different stores and these software would not be much expensive .We can explain the working and benefits related to keylogger and focus on especially on customers who are buying computer/laptop for their childrens as it would be helpful to keep a watch on their children web activity and also for the organizations who want to keep a check on their

employees.These behavior based detection technique using KLIMAX can be installed at the store by taking the permission of the customers.

3. CONCLUSION

In this paper, we discussed about the keylogger and the common types of keylogger. Since keylogger have a bad reputation as the users confidential data such as user name, password, and pin can be recorded by the use of keylogger. But at company level, key loggers can be used to check the employees web activity and also for domestic purpose parents can keep a check on their children web activities. Also we have done the comparison between different detection techniques and selected one technique which can be used for the domestic purpose.

REFERENCES

[1] https://www.researchgate.net/publication/221427552_KLIMAX_Profiling_Memory_Write_Patterns_to_Detect_Keystroke-Harvesting_Malware

[2] http://web.eng.fiu.edu/~aperezpo/DHS/Std_Research/Keylogging.

[3] Survey of Keylogger Technologies, Yahye Abukar Ahmed, Mohd Aizaini Maarof, Fuad Mire Hassan and Mohamed Muse Abshir, International Journal of Computer Science and Telecommunications, Volume 5, Issue 2, February 2014, page 25-31

