A Survey on Keylogger: A malicious Attack

NameHemita Pathak, Apurva Pawar, Balaji Patil

***Abstract*—Now a days, internet has become part of basic needs for modern society. People are using internet for online banking and confidensial information sharing through email and chats on social networking sites. Intruters are using malwares to damage systems. Keylogger is one of the harmful malwares. Keylogger tries to obtain private information through monitoring keystroke and communicating this data to intruter with malicious intentions. And thus, keylogger is said to be a main threat for business and personal activities. To prevent from huge economical/personal loss, system needs to protect valuable information from Intruters. But before planning for prevention it is necessary to be aware of few things like key logger working. This paper gives a brief description of keylogger, it's working, prevention detection of key logger and various applications of key logger.**

***Index Terms*—Malware, password attack, intruder, keylogger, prevention, detection, application.**

I. Introduction

Malware is used to disturb system process, collect sensitive data and gain access to systems [1]. Detecting and preventing malware attack is very important area under discussion in cyber world as malwares can badly affect computer operation. Once an intruder got access to private user data, he/she can easily make money transfer from user account to untrusted account. Unluckily, hold of private data can have many times consequences which can prove to be more hazards than particular individual's financial loss. WE can summarized malware as program intentionally developed for damaging computer specifically those have internet connection [2]. Malware reinstall themselves again though they are removed from system , this make them more harmful and are almost difficult to remove as they hide themselves deep inside operating system [3]. Adware, Spyware, Hijackers, Toolbars, Dialers, Keylogger etc. are some types of malware. Malware can also be any combination of these with keylogger attached to each.

The keylogger spyware is exceptionally risky for those systems which are involved in transaction processes daily. The keystrokes of keyboard got recorded by keylogger and are then sent to intruder through email. It is very important to valuable information like account numbers, ATM's PIN code, passwords etc.[4].

In our paper we are focusing on keylogger, its working, prevention detection of key logger and various applications of key logger. This paper is organized in seven sections. Section II describes different password attacks. Section III gives introduction to keylogger and its types. In section IV we are depicting working of keylogger. Section V suggests various prevention and detection methods. We enlist different applications of keylogger in section VI. Finally, we conclude our paper in section VII.

II. Different Password Attacks

For authentication of any system password is first and foremost step so, passwords play an important role in daily life in various computing applications like ATM machines, internet services, windows login, authentication in mobiles etc. Intruders/hackers can make system vulnerable, can get access of it and can also get valuable information of ours. In this section we enlisted some of possible password attacks.

A. *Brute Force Attacks:*

For password cracking this technique is very fast. It will check all short passwords but for longer passwords it not so useful. It is like trial and error method used to retrieve information like password and PIN, also known as brute force cracking.

B. *Dictionary Attack*:

It works on the assumption that most passwords consist of whole words, dates or number taken from dictionary. It is a technique of breaking into a password protected computer or server by sequentially and logically inserting each word in a dictionary. It is also used to achieve key required to decrypt an encrypted document or message.

C. *Shoulder Surfing:*

Shoulder surfing refers to direct observation method. As you can spy to someone's shoulder to get information. This will efficiently work in mob or crowded place where a person is uses personal computer, ATM or access through smart phone.

D. *Hash guessing:*

Some password cracking method can both extract and crack password hashes, but most password crackers need to have the LM password hash before they can begin the cracking process.

E. *Rainbow table attack:*

It is list of pre-computed hashes, the numerical values of an encrypted password. It also frequently used hackers in now days. As in rainbow has table the hashes of all possible password combination for any given hashing algorithm. The required time to for cracking password is reduced to the time it takes to look it up in the list.

F. *Key Loggers:*

A keylogger or screen scraper can be installed by malware which will capture everything you type, or it will capture screen shots during typing of password or by doing login to specific system. After that it will forward this valuable

***Manuscript received April, 2015*.**

Hemita Pathak, *Computer Engineering, MAEERS MIT Pune, India*
Apurva Pawar, *Computer Engineering, MAEERS MIT, Pune, India*
Balaji Patil, *Computer Engineering, MAEERS MIT, Pune, India*

information to the hacker or to intruders.

G. *Spidering*:

Hackers and intruders have realized that many corporate passwords that are connected to the business and project. By looking or doing ground work for corporate research, website sales materials and even the websites of rivals and enlisted clients can provide the ammunition to construct a custom word list to use in brute force cracking.

H. *Password Sniffing:*

Some password crackers can sniff authentication traffic between server and client and retrieve password hashes or information related to the authentication.

III. Keylogger and Its Types

A keylogger, sometimes called a keystroke logger, key logger, or system monitor, is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard. A keylogger program does not require physical access to the user's computer. It can be downloaded on purpose by someone who wants to monitor activity on a particular computer or it can be downloaded unwittingly a spyware and executed as part of a rootkit or remote administration (RAT) Trojan horse. A keylogger program typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file (which does all the recording) and an executable file (.EXE) that installs the DLL file and triggers it to work [5]. The keylogger program records each keystroke the user types and uploads the information over the Internet periodically to whoever installed the program. The attackers are exploring different techniques of keylogging using hardware keyloggers, software keyloggers and screen capturing software to steal the user sensitive data [6].

Although keylogger programs are promoted for benign purposes like allowing parents to monitor their children's whereabouts on the Internet, most privacy advocates agree that the potential for abuse is so great that legislation should be enacted to clearly make the unauthorized use of keyloggers a criminal offense.

Keyloggers are mainly classified into two categories: Hardware Keyloggers and Software Keyloggers.

A. *Hardware Keyloggers:*

Hardware keyloggers are used for key stroke logging. It is a method of recording victim's keystrokes which will include ATM PIN, login password, etc.

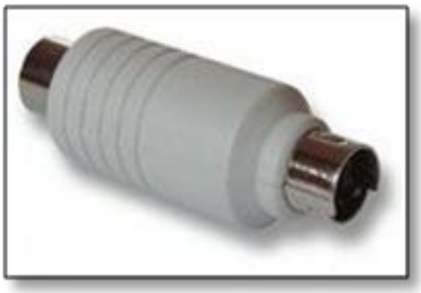

Fig 1: A hardware-based keylogger.

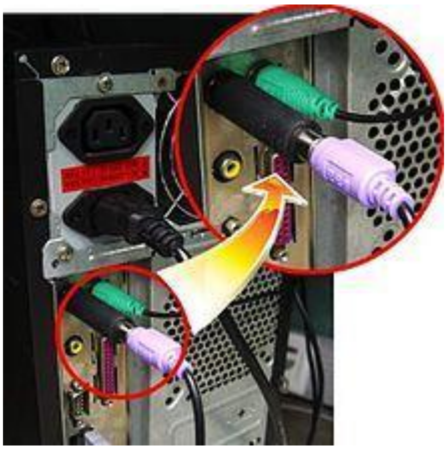

Fig 2: A connected hardware-based keylogger

They can be implemented by BIOS-level firmware or may be used through a device plugged in line between a computer keyboards and a computer. It will retrieve all activities held on victim's computer and will record log to their internal memory [7]. Types of hardware loggers include wireless keylogger sniffers, firmware, regular hardware keylogger, keyboards overlays.

B. *Software Keyloggers:*

Software keyloggers logs and monitors the keystrokes and data within the target operating system, store them on hard disk or in remote locations, and send them to the attacker. Software keylogger [8], [9] monitoring is mainly based on the operating-system.

The Major Problem of Data Theft due to use of the key loggers were minimized by the use of various anti-key logging mechanisms. Virtual keyboard is one very popular among them. Since virtual keyboard only operates through mouse clicks so the key strokes are not captured [10]. The virtual keyboard uses the concept of random shuffling of keys; hence it is not having a definite structure. Therefore the key presses if captured cannot be used because of the random changing of the key locations. There is a bigger threat residing that is the screen recording software which is present and undetected.

IV. Working Of Keylogger

In order to prevent system from keylogger attacks and to use particular buyed keylogger for security purpose, it is very necessary to know how keylogger works. This section gives brief idea behind keylogger functionality.

The keyloggers are active between two steps of events, those are when a key is pressed and when information about that keystroke is displayed on the monitor. This is achived through video surveillance, intercepting input/output, a hardware bug in the keyboard, the filter driver in the keyboard stack, substituting the keyboard driver, intercepting kernel functions by any means possible for example, substituting addresses in system tables and splicing function code, intercepting DLL functions in user mode, and at last, requesting information from the keyboard using standard documented methods.

How keylogger spyware attacks user's system is shown in Fig 3. There are three users accessing different internet services like email and online banking. An intruder is present within network which has keylogger spyware, this intruder make sure that keylogger enters into users system as easily as any other normal application software installation or when user performs steps performed mentioned in next section. It acts as legitimate software to fool user, so, the user downloads it on system and installs it. The every keystrokes of keyboard got recorded by keylogger in log file and key log are then sent to intruder through email. The entry of keylogger to the system is represented using red arrows in figure 3. As soon as keylogger enters the system, the spyware starts an automatic email process as given in figure 4 through blue arrows [11].

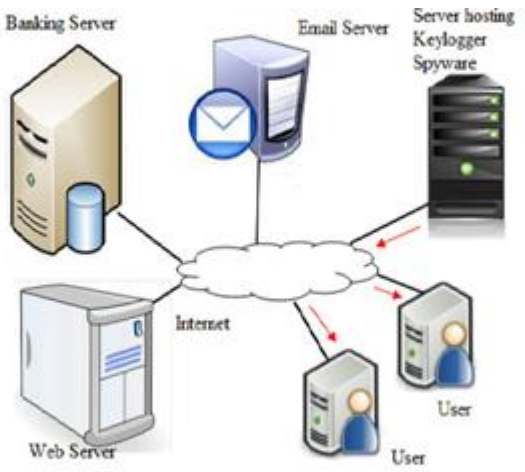

Fig 3: Keylogger Spyware attack on User' s system

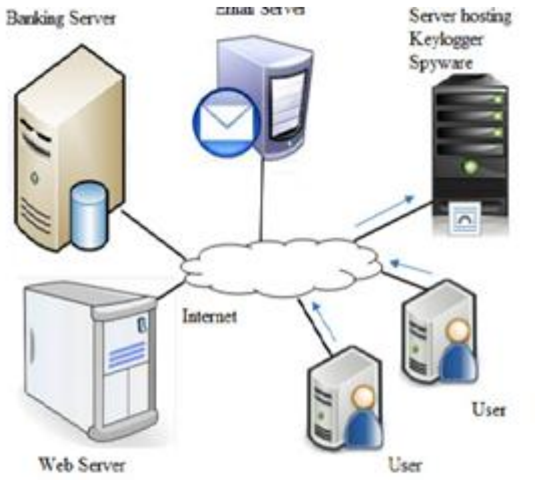

Fig 4: Transfer of email containing confidential Information from users system.

At the time of online transaction, if keylogger is present in system, then keylogger could record password which is sent to intruder after every 2 minutes or can be said periodically. This could result in huge financial loss as entire bank account can be hacked.

V. Detection And Prevention

Intruters are using malwares to damage systems. Keylogger is one of the harmful malwares. Keylogger tries to obtain private information through monitoring keystroke and communicating this data to intruder with malicious intentions. And thus, keylogger is said to be a main threat for business and personal activities. Hence it is important to protect form these attacks. This section mentions some of detection and prevention techniques.

Keylogger spreads in a same way as other malicious algorithms spreads, leaving the case when keylogger are purchased for positive/security purpose. The mainly observed methods are:

- A keylogger can possibly get installed after opening a file attached to email.
- When a file is launched from an open-access directory on a P2P network, a keylogger can get installed.
- A keylogger can be installed through an infected site;
- A keylogger can be installed by some other malicious program present in victim machine, if the program is able of download and install other malware on the system

Way for detection and prevention is given by various industries and researchers. Industries has launched softwares like antivirus with malware prevention and anti-keyloggers. Many antivirus had added kelogger to their database to provide protection against malicious attack by keylogger. Users just need to keep their antivirus database up to date. While on other hand anti-keylogger or anti–keystroke logger is special software designed to detect keylogger program. Anti-keylogger can also detect hidden unassembled keylogger software inside system. But when compared with anti-virus or anti-spyware software, anti-keylogger can't make difference between a legitimate keystroke-logging program and an illegitimate keystroke-logging program like malwares. All the keylogger are marked and removed regardless they appear to be legitimate or not.

In earlier days, keylogger were very simple. The keystrokes of keyboard got recorded by keylogger and are then sent to intruder through email or FTP(File Transfer Protocol)[12]. In order to deal with these, virtual keyboard was introduced for electronic payment pages[13]. Every time user log in to financial website or portal keyboard button changes to virtual keyboard making key being pressed unrecognized to intruder. Thus, now due to use of virtual keyboard attacker fail to read passwords. Additionally, security software installed on operating systems used to carefully examine startups in order to prevent system from running keylogger concurrently with other softwares. By analyzing keylogger files and verifying the structure of executable, these applications were capable to recognize new keylogger.

As time gone, many advanced keylogger come, requiring special treatment. And many researchers had given solution to detect and prevent from them. For instance, consider paper[14]. It had provided a novel framework to detect and prevent a keylogger attack. This method makes use of Honeypot in order to monitor the user system. A detection and prevention system is used to detect keylogger and remove. This technique can be defenseless if the intruder uses database of email addresses to send email of system key log to intruder.

Authentication which uses images is a challenge for keylogger given in [15] In order to keep passwords safe, it uses cryptographic hash function, which is greatly resistant to brute force attacks while prone to Dictionary attack, allows users to obtain passwords from any of the locations.

Another approach[11] make use of monitoring system for detection and prevention. Monitoring system captures the traffic on the SMTP port of all the connected users in the network and records it to a log file of each user. with the help of a program which runs in background on server for detection and prevention . Now, log file contains details of each mail send from any system.. By analyzing these files keylogger affected system and intruder are identified. And other system on network are secured by blocking affected ststems and removing keylogger from them.

VI. Keylogger Applications

As explain in earlier section most of the times keyloggers are used for the malicious purpose but apart from it there do affirmative and positive uses of keyloggers also exist. In IT organizations for troubleshooting technical problems with computers and business networks keyloggers are used. Other legal uses include family or business people using them to monitor the network usage without their users' direct knowledge. However, malicious individuals may use keyloggers on public computers to steal passwords or credit card information.

From a technical perspective there are several categories given next.

- **Hypervisor-based**: for effective virtual machine keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which remains untouched. Blue Pill is a conceptual example.
- **Kernel-based**: A program on the machine obtains root access to hide itself in the OS and starts intercepting keystrokes that pass through the kernel. This method is difficult both to write and to combat. Such keyloggers reside at the kernel level and are thus difficult to detect, especially for user-mode applications that don't have root access. They are frequently implemented as root kits that subvert the operating system kernel and gain unauthorized access to the hardware, making them very powerful. A keylogger using this method can act as a keyboard device driver for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.
- **API-based**: These keyloggers hook keyboard APIs inside a running application. The keylogger registers for keystroke events, as if it was a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it. Windows APIs such as GetAsyncKeyState(), GetForegroundWindow(), etc. are used to poll the state of the keyboard or to subscribe to keyboard events. A more recent example simply polls the BIOS for pre-boot authentication PINs that have not been cleared from memory.
- **Form grabbing based**: Form grabbing-based keyloggers log web form submissions by recording the web browsing on submit events. These happen when the user finishes filling in a form and submits it usually by clicking a button or hitting enter. This records form data before it is passed over the Internet.
- **Memory injection based**: Memory Injection based keyloggers alter memory tables associated with the browser and other system functions to perform their logging functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors who are looking to bypass Windows UAC (User Account Control). The Zeus and Spyeye Trojans use this method exclusively. Non-Windows systems have analogous protection mechanisms that need to be thwarted somehow by the keylogger.
- **Packet analyzers**: This involves capturing network traffic associated with HTTP POST events to retrieve unencrypted passwords. This is made more difficult when connecting via HTTPS, which is one of the reasons HTTPS was invented.
- **Remote access Software keyloggers:** With an added feature that allows access to the locally recorded data from a remote location. Remote communication may be achieved using one of these methods:

○ Data is uploaded to a website, database or an FTP server.

○ Data is periodically emailed to a pre-defined email address.

○ Data is wirelessly transmitted by means of an attached hardware system.

○ The software enables a remote login to the local machine from the Internet or the local network, for data logs stored on the target machine to be accessed.

○ Most of these aren't stopped by HTTPS encryption because that only protects data in transit between computers to the keyboard.

VII. Conclusion

In this paper we have shown different password attacks, as keylogger is also one kind of password attack. Also we described what is keylogger and different types of keylogger. Through keylogger one can get access to our valuable information and to our personal system so, detection and prevention of keylogger is highly desirable. In this paper we have enlist some of the prevention and detection methods for keylogger. As every coin has two sides keylogger also has advantages and disadvantages. It can affirmatively use in IT organizations to troubleshoot technical problems with computers and business networks. To provide prevention mechanism on its malicious use or to make positive use of keylogger in IT organization, it is necessary to understand-how keylogger works. Thus, paper has also given keyloggers working.

References

[1] Malware Definition Available at http://en.wikipedia.org/wiki/Malware.

[2] Malware Definition Available at <http://www.wisegeek.com/what-is-malwa re.htm>.

[3] Types of Malwares Available at http://arstechnica.com/security/2004/111rnalware/.

[4] Working of Keyloggers available at http://securelist.com/analysis/publications/36138/keyloggers-how-theywork-and-how-to-detect-them-part-1/.

[5] Fujita, K. and Y. Hirakawa, 2008. A study of password authentication method against observing attacks. 6th International Symposium on Intelligent Systems and Informatics, SISY 2008.

[6] Arvind Narayanan and Vitaly Shmatikov, 0000. Fast dictionary attacks on passwords using time-space tradeoff, Conference on Computer and Communications Security, Proceedings of the 12th ACM Conference on Computer and Communications Security, pp: 364-372.

[7] Huanyu Zhao Xiaolin Li, 2007. A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme, Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21 International Conference, 2(s): 467-472.

[8] G. Canbek, “Analysis, design and implementation of keyloggers and anti-keyloggers” Gazi University, Institute Of Science And Technology, M.Sc. thesis (in Turkish), Sept. 2005, pp. 103

[9] F.S. Lane, “The naked employee: How technology is Compromising workplace privacy” AMACOM Div American Mgmt. Assn.,2003, pp.128-130.

[10] S. Gong “Design and Implementation of Anti-Screenshot Virtual Keyboard Applied in Online Banking “E-Business and E-Government (ICEE), 2010 International Conf., 7-9 May 2010,pp-1320-1322

[11] Akhil S, Neeraja M Nair, Asst Prof. Arun R, “Detection And Prevention Of Keylogger Spyware Attacks,” IJCET,2014, pp. 167-172.

[12] Christopher A. Wood and Rajendra K. Raj,” Keyloggers in Cybersecurity Education”, New York, USA (2010).

[13] Afolayan A. Obiniyi and Mohammed Aminu Umar,” Random Number Based Dynamic Anti-Screenshot Virtual Keyboard for Securer Web Login”, The International Journal of Engineering And Science, 2: (2013).

[14] Mohammad Wazid, Avita Katal, R.H. Goudar, D.P. Singh, Asit Tyagi, Robin Sharma, and Priyanka Bhakuni ,” A Framework for Detection and Prevention of Novel Keylogger Spyware Attacks”,7th International Conference on Intelligent Systems and Control (ISCO 2013).

[15] M.N. Doja, Naveen Kumar, "Image Authentication Schemes against Key-Logger Spyware", 9th ACM ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2008 (SNPD '08).

Hemita Pathak pursuing Masters of Engineering from Maharashtra Institute of Technology, Pune. Studied Bachelors of Engineering from VNSGU, Surat. Currently working on Machine Learning and Bioinformatics domain.

Apurva P. Pawar received degree of Bachelor of Engineering in Computer Science and engineering from Santa Gadage baba Amravati University, Amravati, Maharashtra, India. She is currently pursuing Master of Engineering from Maharashtra Institute of Technology, Pune in Computer Engineering affiliated to the University of Pune, India. Her research interests include networking, cloud computing and mobile cloud computing.

Balaji Patil is working as Associate Professor at MAEER’s Maharashtra Institute of Technology, Pune with 16 years of work experience. He has completed Masters of Engineering and currently pursuing PhD. His publication includes three National and one international paper and his area of interest includes networking.