ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Unprivileged Detection of User Space Keyloggers

Mugdha Kolte[1], Rutuja Wadekar[2], Rachana Late[3], Palak lodha[4]Saranga Bhutada[5]

B.E. Student, Department of Information Technology, MITCOE, Kothrud, Pune, India[1]

B.E. Student, Department of Information Technology, MITCOE, Kothrud, Pune, India[2]

B.E. Student, Department of Information Technology, MITCOE, Kothrud, Pune, India[3]

B.E. Student, Department of Information Technology, MITCOE, Kothrud, Pune, India[4]

Assistant Professor, Department of Information Technology, MITCOE, Kothrud, Pune, India[5]

ABSTRACT: This application allows maximum flexibility to the user to work on the internet. There is software which install on thesystem, continuously monitoring to find the existing key-logger which is present in the systems and give alert to prevent them. It is most efficient way to get secured from hacking. Key loggers are implanted on a machine to intentionally monitor the user activity by logging keystroke sand eventually delivering them to a third party. We propose a new approach to detect keyloggers running as unprivileged user-space processes. To match the same deployment model, our technique will be entirely implemented in an unprivileged process. As a result, our solution will be portable, easy to install, and yet very effective. In addition, the proposed detection technique will be completely black-box, i.e., based on behavioural characteristics common to all keyloggers. In other words, our technique will not rely on the internal structure of the keylogger or the particular set of APIs used for this reason; our solution is of general applicability. The modules which will be present in this system are that we detect key loggers running as unprivileged user-space processes.

KEYWORDS*:* Keyloggers, Unprivileged, Keystrokes, Detection, user-space, memory diagnostics.

I. INTRODUCTION

To evaluate the ability to detect real-world keyloggers, During the era of 21st century most of the people uses internet to complete their work so to prevent from hacking our accounts we are creating such software which detects the keylogger present in the system and kill them manually. This application Allow maximum flexibility to the user to work on internet. There is software which install on the system, continuously monitoring to find the existing key-logger which is present in the systems and give alert to prevent them. It is most efficient way to get secured from hacking.

The main function of the system is to Prevention, Detection with IP trace back system where we can trace back the IP address of the person who is launching attacks on our web server or database. Anti-key loggers are used both by large organizations as well as individuals in order to scan for and remove keystroke logging software on your computer. It is generally advised the software developers that anti-key logging scans be run on a regular basis in order to reduce the amount of time during which a keylogger may record your keystrokes; for example, if you scan your system once every three days, there is a maximum of only three days during which a keylogger could be hidden on your computer and recording your keystrokes.

A software acting as a keylogger can be implemented by means of two different techniques: as a kernel module or as a user-space process. It is important to notice that, while a kernel keylogger requires a privileged access to the system, a user-space keylogger can easily rely on documented sets of un-privileged API commonly available on modern operating systems.A fully unprivileged keylogger can be implemented by a simple user-space process. This is not the case for a keylogger implemented as a kernel module. In kernel space, the programmer must rely on kernel-level

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

facilities to intercept all the messages dispatched by the keyboard driver, undoubtedly requiring a considerable effort and knowledge for an effective and bug-free implementation. Despite the rapid growth of keylogger-based frauds (i.e., identity theft, password leakage, etc.), not many effective and efficient solutions have been proposed to address this problem. Traditional defense mechanisms use fingerprinting strategies similar to those used to detect viruses and worms. Unfortunately, this strategy is hardly effective against the vast number of new keylogger variants surfacing every day in the wild. In this project, we are presenting an unprivileged user space key logger approach for accurate detection of the most common user-space
key loggers. We are going to model the behavior of a key logger by surgically correlating the input (i.e., the keystrokes) with the output (i.e., the I/O patterns produced by the key logger).

II. RELATED WORK

several approaches have been recently proposed to detect privacy-breaching malware, including keyloggers. Behavior-based spyware detection has been first introduced by Kirda et al. in [16]. Their approach is tailored to malicious Internet Explorer loadable modules. In particular, modules monitoring the user's activity and disclosing private data to third parties are flagged as malware. Their analysis models malicious behavior in terms of API calls invoked in response to browser events. Those used by keyloggers, however, are also commonly used by legitimate programs. Their approach is therefore prone to false positives, which can only be mitigated with continuously updated white lists.

Other keylogger-specific approaches have suggested detecting the use of well-known keystroke interception APIs. Aslam et al. [17] propose binary static analysis to locate the intended API calls. Unfortunately, all these calls are also used by legitimate applications (e.g., shortcut managers) and this approach is again prone to false positives. Xu et al. [18] push this technique further, specifically targeting Windows-based operating systems.
Our approach uses Memory diagnostics concept which helps us to detect an application which is holding our sent Strings.

III. PROBLEM STATEMENT

Keyloggers are implanted on a machine to intentionally monitor the user activity by logging keystroke sand eventually delivering them to a third party. We proposed a new approach to detect key loggers running as unprivileged user-space processes. To match the same deployment model, our technique is entirely implemented in an unprivileged process. As a result, our solution is portable, easy to install, and yet very effective. In addition, the proposed detection technique is completely black-box, i.e., based on behavioural characteristics common to all keyloggers. In other words, our technique does not rely on the internal structure of the keylogger or the particular set of APIs used for this reason; our solution is of general applicability. We have prototyped our approach and evaluated it against the most common free keyloggers. Our approach has proven effective in all the cases. Key loggers are increasing rapidly and are the number one threat on the internet. Users and businesses are unknowingly losing their data though these hacks.

IV. PROJECT REQUIREMENTS

Minimum System requirements
Hardware Requirements:
Processor: Pentium IV

RAM: 2GB
Hard Disk: 80GB
Software requirements:
Operating System: Windows XP
Front End: Java, dot net,.dll files

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

V. ARCHITECTURE

We first send keys to all the applications which we think are affected due to some software and check the process use through task manager. After monitoring the processes, we separate the processes into two parts i.e. Malicious and reliable processes.

In the database we have stored the known keylogger patterns which help us to identify the malicious processes affected by the keyloggers. Memory diagnostics is a module wherein we check the changes that occur in the processes memory size after sending keys at fixed interval of time and check which processes change according to the keys sent. This diagram shows the basic structure of our system of how it will detect the keyloggers.

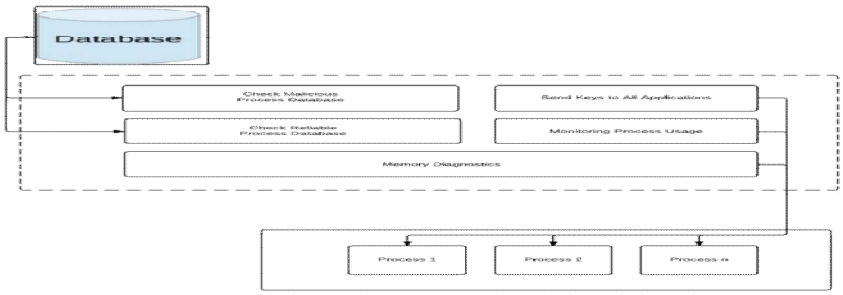


Fig.1. Architecture Diagram

VI. METHODOLOGY

A number of techniques can be used to defeat keyloggers, but no one technique is effective against all types of keyloggers.

A keylogger can be housed in a hardware device that plugs into the keyboard port on your computer. Some hardware keyloggers are hidden inside of keyboards themselves. Hardware keyloggers cannot be detected by software, but they have the drawback of requiring physical access to a computer. If you suspect a hardware keylogger is present on your system, inspecting the keyboard's connection to the computer, or replacing the keyboard will solve the problem. Form-filling software such as Rob form stores passwords, credit card info, and other information in a database, then enters it into Web forms as needed. This eliminates the user's need to type such data on the keyboard, and can prevent keyloggers from recording it. However, there are other forms of spyware which can intercept data posted to forms by form-fillers. Speech-to-text software or virtual keyboards can eliminate the keyboard connection, too. However, the text has to get to its destination somehow, and that path may be vulnerable to clever keystroke loggers.

An anti-keylogger program attempts to detect and/or disable keylogging programs.Anti-keyloggers scan your hard drive for the digital signatures of known keyloggers, and look for low-level software "hooks" that indicate the presence of a keystroke grabber. Anti-keyloggers and keylogger detectors are more effective against keyloggers than general antivirus programs because the latter often don't identify keyloggers as malware.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

VII. METHODS USED FOR DETECTION

Keylogger detection, as for viruses and other malwares, can basically be achieved through two methods:

A. Signature based detection

This type of software has a signature base, which has the list of all the known keyloggers, each time you run 'System Scan' this software looks for the items from its list on your hard disk drive. This type of software is a rather widespread one, but it has its own drawbacks, the biggest drawback of signature-based anti-keyloggers is that, while using them you can only be sure that you are protected only from keyloggers from your signature-base list, thus staying absolutely vulnerable to other keyloggers. Thus a criminal can download one of many famous keyloggers, change it and your anti-keylogger won't recognize it.

B. Heuristic based detection

This software doesn't use signature bases; it analyzes the methods of work of all the modules in your PC, thus blocking the work of all the keyloggers. Though this method gives better keylogging protection than signature-based anti-keyloggers, it has its own drawbacks. One of them is that this type of software blocks non-keyloggers also. The thing is that many 'non-harmful' software modules include processes which are peculiar to keyloggers. They do not send received information and are absolutely safe for the user. Usually all the non-signature-based keyloggers have the option to unblock all the modules, but they can cause difficulties among inexperienced users.

An unknown keylogger will not get caught by signature-based detection products, and you will have to rely on heuristics or behavioral detection, which usually generate a more false-positive results.

Fortunately, the keylogger developers usually rely on well-known methods to develop their malicious code, and that allows researcher to quickly find and detect them. Such methods are for example:

A. Send Keys

Hidden deep within the Windows Script Host's object model is a small but powerful method called sends Keys that allows you to send keystrokes to the active window just as if you had manually typed them on the keyboard.

B. Monitoring Process Usage

Running keyloggers temporary store all its received keys in its process memory. Due to this its process memory keeps changing. So our application will keep track of all the process and there used memories.

C. Reliable and Malicious Database

Our Anti-keylogger application will maintain its own Databases for All Malicious Process and Reliable Process. After executing our Application, it checks databases against all users running processes. If some entries are found than the result is displayed otherwise further steps are executed.

D. Memory Diagnostics

Memory Diagnostics are used to check installed keylogger. Initially our application sends the random strings to all applications and checks which application is grabbing the strings. Normal applications neglect strings but keylogger application starts grabbing those keys and store it in its own memory space. Memory Diagnostics helps us to detect an application which is holding our sent Strings.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

VIII. USE OF KEYLOGGERS

A. Parental control: parents can track what their children do on the Internet, and can opt to be notified if there are any attempts to access websites containing adult or otherwise inappropriate content;
B. Jealous spouses or partners can use a keylogger to track the actions of their better half on the Internet if they suspect them of virtual cheating‖;
C. Company security: tracking the use of computers for non-work-related purposes, or the use of workstations after hours;
D. Company security: using keyloggers to track the input of key words and phrases associated with commercial information which could damage the company (materially or otherwise) if disclosed;
E. Other security (e.g. law enforcement): using keylogger records to analyze and track incidents linked to the use of personal computers;

IX. HOW TO PROTECT FROM KEYLOGGERS

Most antivirus companies have already added known keyloggers to their databases, making protecting against keyloggers no differentfrom protecting against other types of malicious program: install an antivirus product and keep its database up to date. However, since most antivirus products classify keyloggers as potentially malicious or potentially undesirable programs, users should ensure that their antivirus product will, with default settings, detect this type of malware. If not, then the product should be configured accordingly, to ensure protection against most common keyloggers.

Methods that can be used to protect against unknown keyloggers or a keylogger designed to target a specific system. The most logical ways to protect against unknown keyloggers are as follows:

A. Using one-time passwords or two-step authentication.
B. Using a system with proactive protection designed to detect keylogging software (Anti-keylogger).
C. Using a virtual keyboard.

X. APPLICATIONS OF ANTI-KEYLOGGERS

A. Public computers

Public computers are extremely susceptible to the installation of keystroke logging software and hardware, and there are documented instances of this occurring. Public computers are particularly susceptible to keyloggers because any number of people can gain access to the machine and install both a hardware keylogger and a software keylogger, either or both of which can be secretly installed in a matter of minutes. Anti-keyloggers are often used on a daily basis to ensure that public computers are not infected with keyloggers, and are safe for public use.

B. Gaming usage

Keyloggers have been prevalent in the online gaming industry, being used to log steal which are then used to hack a user's gaming account online. Anti-keyloggers are used by gaming community members in order to keep their gaming accounts secure.

C. Financial institutions

Financial institutions have become the target of keyloggers, particularly those institutions which do not use advanced security features such as PIN pads or screen keyboards. Anti-keyloggers are used to run regular scans of any computer on which banking or client information is accessed, protecting passwords, banking information, and credit card numbers from identity thieves.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

D. Personal use

The most common use of an anti-keylogger is by individuals wishing to protect their privacy while using their computer; uses range from protecting financial information used in online banking, any passwords, personal communication, and virtually any other information which may be typed into your computer. Keyloggers are often installed by people you know, and many times have been installed by an ex-partner hoping to spy on their ex-partner's activities (particularly chat).

E. Banks

Security experts consider keylogging as the most dangerous threat because it allows cyber criminals to capture everything you type on your keyboard. This includes passwords so that they can gain access to your online accounts such as your email, banking, forums, websites and etc to steal valuable information. To overcome this problem anti-keyloggers are used.

F. IT Organizations

Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks.

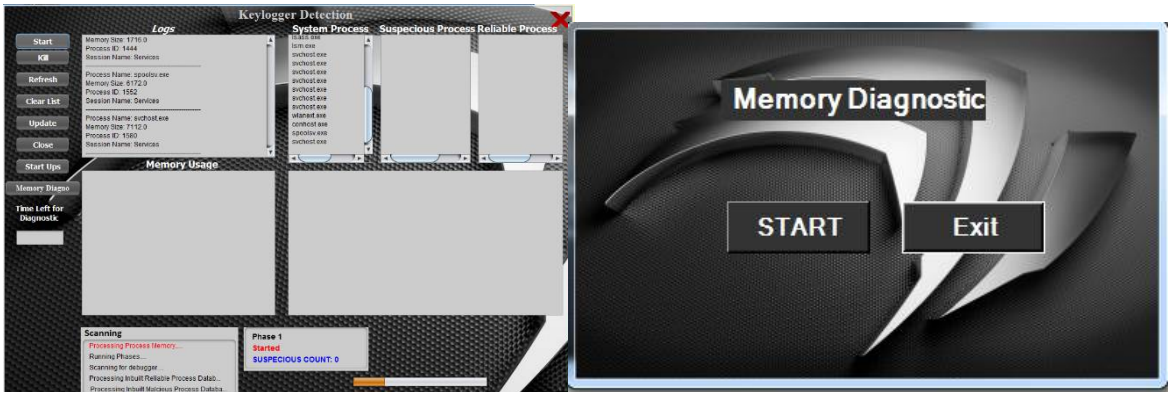
G. Optical Surveillance

Optical surveillance, while not a keylogger in the classical sense, is nonetheless an approach that can be used to capture passwords or PINs. A strategically placed camera, such as a hidden surveillance camera at an ATM, can allow a criminal to watch a PIN or password being entered.

H. Smartphone Sensors

Researchers have demonstrated that it is possible to capture the keystrokes of nearby computer keyboards using only the commodity accelerometer found in smartphones. The attack is made possible by placing a smartphone nearby a keyboard on the same desk. The smartphone's accelerometer can then detect the vibrations created by typing on the keyboard, and then translate this raw accelerometer signal into readable sentences with as much as 80 percent accuracy.

XI. RESULTS AND SIMULATION



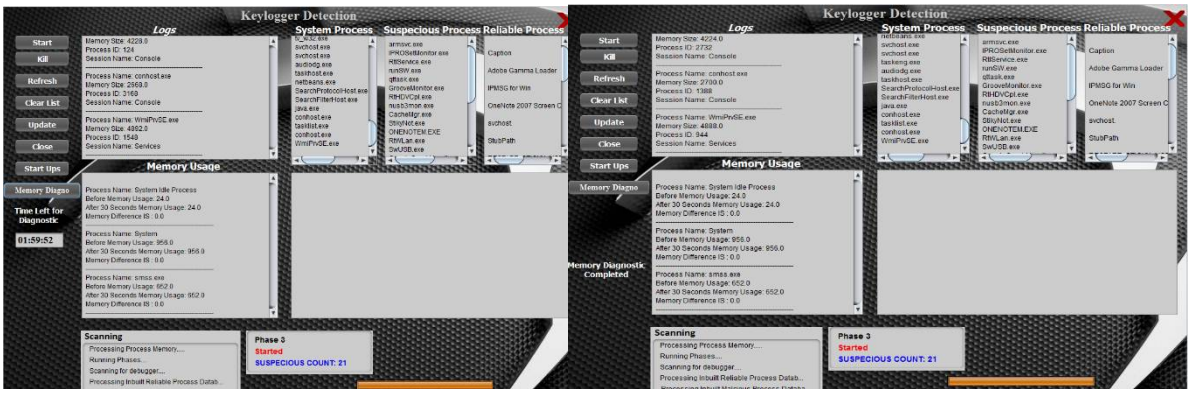
(a) (b)

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016



(c) (d)

Fig.2. Keylogger Detection GUI (a) Scanning background processes phase 1 to phase 3 (b) Memory Diagnostics GUI (c) Memory Diagnostics started timer (d) Memory Diagnostics Completed.

XII. ACKNOWLEDGMENT

We wish to express our heartfelt gratitude to all those who have helped us in making this project success. We wish to express our deep sense of gratitude to our Project Guide, Prof. Saranga Bhutada and Stackmint Project Team Head Mr. Shivprasad Dhumal and Manager Mr. Rahul Jaiswal, for their able guidance and useful suggestions, which helped us in completing the project work, in time. Without their co-operation, it would have been extremely difficult for us to complete the project.
Our sincere Thanks to Prof. (Dr.) A. S. Hiwale, Head of Department for having permitted us to carry out this project work and who has been a source of inspiration and for his timely guidance in the conduct of our project work.

Thanks to all who helped us directly or indirectly to complete this project.

XIII. CONCLUSION

In this project, we are presenting an unprivileged user space key logger approach for accurate detection of the most common user-space key loggers. We are going to model the behaviour of a key logger by surgically correlating the input (i.e., the keystrokes) with the output (i.e., the I/O patterns produced by the key logger). In addition, we are augmenting our model with the ability to artificially inject carefully crafted keystroke patterns. We are then discussing the problem of choosing the best input pattern to improve our detection rate. Subsequently, we are going to present an implementation of our detection technique on Windows, arguably the most vulnerable OS to the threat of key loggers. To establish an OS independent architecture, we are also going to give implementation details for other operating systems. We are successfully going to evaluate our prototype system against the most common free key loggers

REFERENCES

[1]. . N. Grebennikov, *"Keyloggers: How They Work and HowtoDetectThem,"* http://www.viruslist.com/en/analysis?pubid=204791931, 2012.
[2]. Security Technology Ltd., *"Testing and Reviews of Keyloggers, Monitoring Products and Spyware,"* http://www.keylogger. org, 2012.
[3]. Kirda, C. Kruegel, G. Banks, G. Vigna, and R. Kemmerer, *"Behavior-Based Spyware Detection,"* Proc. 15th USENIX Security Symp., pp. 273-288, 2006.
[4]. M. Aslam, R. Idrees, M. Baig, and M. Arshad, *"Anti-Hook Shield against the Software Key Loggers,"* Proc. Nat'l Conf. Emerging Technologies, pp. 189-191, 2004
[5]. Y. Al-Hammadi and U. Aickelin, *"Detecting Bots Based on Keylogging Activities,"* Proc. Third Int'l Conf. Availability, Reliability and Security, pp. 896-902, 2008.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

[6]. . Author: Gauraw B. Chahande1; Dixit M. Kolhatkar2; Mayur L. Paradkar3 ; Punam S. Budhe4 ; Nilam V. Pawade5 ; Mrs. Chandrayani N. Rokde.*"Detection of User-Space Key loggers For Legitimate Users"* pp.2347-4890, 2012.
[7]. . Stefano Ortolani, Cristiano Giuffrida, and Bruno Crispo, Senior Member, IEEE,*"Unprivileged Black-box Detection of User-spaceKeyloggers"*, pp.1545–5971, 2013.
[8]. Theron, kristen "*What is Anti Keylogger*"(19 February 2016).
[9]. Cormac Herley ,Dinei Florencio *"How To Login From an Internet Cafe Without Worrying About Keyloggers"*. MicrosoftResearch. Retrieved 2008-09-23.
[10]. *"What is a Keylogger?"*.PC Tools.
[11]. *"The Evolution of Malicious IRC Bots" . Symantec. 2005-11-26: 23–24. Retrieved 2011-03-25.*
[12]. J. Aldrich, *"Correlations genuine and spurious in pearson and yule,"* Statistical Science, vol. 10, no. 4, pp. 364–376, 1995.
[13]. W. Hsu and A. Smith, *"Characteristics of I/O traffic in personal computer and server workloads,"* IBM System Journal, vol. 42,no. 2, pp. 347–372, 2003.
[14]. H. W. Kuhn, *"The hungarian method for the assignment problem,"* Naval Research Logistics Quarterly, vol. 2, pp. 83–97, 1955.
[15]. Kochenberger, F. Glover, and B. Alidaee, *"An effective approach for solving the binary assignment problem with sideconstraints,"* Information Technology and Decision Making, vol. 1, pp. 121–129, May 2002.
[16]. Kirda, C. Kruegel, G. Banks, G. Vigna, and R. Kemmerer, *"Behavior-based spyware detection,"* Proc. of the 15th USENIX Security Symposium, pp. 273–288, 2006.
[17]. M. Aslam, R. Idrees, M. Baig, and M. Arshad, *"Anti-Hook Shield against the Software Key Loggers,"* Proc. of the National Conference on Emerging Technologies, p. 189, 2004.
[18]. M. Xu, B. Salami, and C. Obimbo, *"How to protect personal information against keyloggers,"* Proc. of the 9th Intl. Conf. on Internet and Multimedia Systems and Applications, 2005.