Cyber Crime Combating Using KeyLog Detector tool

Mahak Arora[1], Kamal Kumar Sharma[2], Sharad Chauhan[3]

[1]Student, M. Tech, ESEAR, Ambala
[2]Professor, Dept. of ECE, E-Max group of Institutions, Ambala
[3]Assistant Professor, Dept. of CSE, E-Max group of Institutions, Ambala

Abstract— **Cyber Crime has become a major threat to integrity of data owned and maintained by any organization or individual. One of the easiest ways to collect information from a system is by using a keylogger which tracks down the keyboard strokes, either using a Software-based keylogger or using a hardware-based keylogger. Though hardware-based keyloggers can be easily identified most of the times, the software-based keyloggers can pose a great threat if not detected timely. For this, a software called an anti-keylogger can be installed on the system which would track the use of any keylogger. The paper presents one such anti-keylogger named 'KeyLog Detector' which will not only display the list of suspected processes, but will also allow the user to modify, add to or delete from the names of existing suspected processes list apart from generating a system command to terminate the same.**

Keywords— **keylogger, suspected processes, anti-keylogger, KeyLog Detector, terminated processes**

I. INTRODUCTION

Cyber Crime or Computer-related crime has seen a tremendous rise in the last two decades. The Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and communication technologies are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings, Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs. The influence of technology on society goes far beyond establishing basic information infrastructure.

In such circumstances, the entire connected system becomes vulnerable to threats of stealing of information, identity thefts, etc. for which one of the easiest ways out is by tracking 'key' movements. Yes, these vital movements can be very easily tracked using something called a keylogger. Though many private sector organizations find it a boon to be able to track down their employees' work, there are yet many others which are at the risk of information theft because of their movements being noted and used by a malicious hacker. For this, anti-keloggers are of great help and the paper presents one such anti-keylogger called KeyLog Detector and explains how it is better than most of the anti-keyloggrs in use.

II. KEYLOGGING

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Through keylogging process, a person can get complete account of another's person's activities on a system as the former can receives a record of the user's keystrokes. Keylogging can also be used to study human–computer interaction.

A. Various areas where Keylogging pose a threat:

1) 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 like KeyLog Detector can be often used on a daily basis to ensure that public computers are not infected with keyloggers, and are safe for public use.

2) 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; of particular importance has been World of Warcraft, which has been the target of numerous keylogging viruses. KeyLog Detector can beused by many World of Warcraft and other gaming community members in order to keep their gaming accounts secure.

3) 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. KeyLog Detector can be 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.

4) Personal use

© 2016 IJRRA All Rights Reserved

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).

B. Basic terms related to cryptography

1) Keylogger:

A program or software which enables a person (mostly malicious hacker) to initiate the process of recording keyboard or key strokes of a user is a keylogger. It generally is installed on a system without the knowledge of the user. For example, REFOG, DanuSoft keyloggers are easily available for free online and are very commonly used.

2) Suspected Processes:

The processes which run in the background or the foreground and are detected by an Anti-Keylogger to be of potential threat to a system are referred to as suspected process. They may or may not be actually harmful but are recognized by the anti-malware softwares as dangerous. For example, any keylogger which runs in the background without the knowledge of the user would be able to extract all confidential information and thus, is bound to be listed in the category of suspected process.

3) Anti-keylogger:

A program or software which efficiently handles and manages all suspected processes, particularly a keylogger; it detects such processes and may also be capable of terminating them. There are many examples of anti-keyloggers, including the application currently in hand, that is, the KeyLog Detector.

4) KeyLog Detector:

An anti-keylogger which is a combination of signature-based and heuristic-based and provides mixed benefits of both. It is built to ensure that the suspected processes are not just detected but terminated as well. It automatically detects the potentially harmful process and adds them to its 'suspected processes' list. Moreover, it gives the user an added advantage of being able to modify, add or delete from the list of suspected processes.

5) Terminated Processes

A terminated process is the one which was detected to be harmful and was ended manually or automatically by an anti-keylogger program.

III. KEYLOGGER

A program or software which enables a person (mostly malicious hacker) to initiate the process of recording keyboard or key strokes of a user is a keylogger. It generally is installed on a system without the knowledge of the user. For example, REFOG, DanuSoft keyloggers are easily available for free online and are very commonly used.

On the basis of their mode of operation, keyloggers may be classified as:

A. Hardware-Based:

Hardware-based keyloggers do not depend upon any software being installed as they exist at a hardware level in a computer system.

Firmware-based: BIOS-level firmware that handles keyboard events can be modified to record these events as they are processed. Physical and/or root-level access is required to the machine, and the software loaded into the BIOS needs to be created for the specific hardware that it will be running on.

Keyboard hardware: Hardware keyloggers are used for keystroke logging by means of a hardware circuit that is attached somewhere in between the computer keyboard and the computer, typically inline with the keyboard's cable connector. There are also USB connectors based Hardware keyloggers as well as ones for Laptop computers (the Mini-PCI card plugs into the expansion slot of a laptop). More stealthy implementations can be installed or built into standard keyboards, so that no device is visible on the external cable. Both types log all keyboard activity to their internal memory, which can be subsequently accessed, for example, by typing in a secret key sequence.

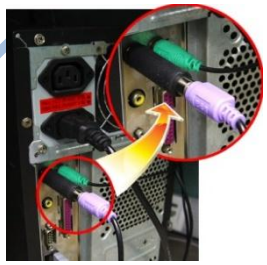

Figure 1. A hardware-based Keylogger

A hardware keylogger has an advantage over a software solution: it is not dependent on being installed on the target computer's operating system and therefore will not interfere with any program running on the target machine or be detected by any software. However its physical presence may be detected if, for example, it is installed outside the case as an inline device between the computer and the keyboard.

Some of these implementations have the ability to be controlled and monitored remotely by means of a wireless communication standard.

B. Software-based:

These are computer programs designed to work on the target computer's software. Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Families and business people use keyloggers legally to monitor network usage without their users' direct knowledge. However, malicious individuals can use keyloggers on public computers to steal passwords or credit card information.

© 2016 IJRRA All Rights Reserved

From a technical perspective there are several categories:
Hypervisor-based: The keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which thus remains untouched. It effectively becomes a virtual machine. Blue Pill is a conceptual example.
Kernel-based: A program on the machine obtains root access to hide itself in the OS and intercepts keystrokes that pass through the kernel. This method is difficult both to write and to combat. Such keyloggers reside at the kernel level, which makes them difficult to detect, especially for user-mode applications that don't have root access. They are frequently implemented as rootkits that subvert the operating system kernel to gain unauthorized access to the hardware. This makes 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 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. This happens when the user completes a form and submits it, usually by clicking a button or hitting enter. This type of keylogger records form data before it is passed over the Internet.
Memory injection based: Memory Injection (MitB)-based keyloggers perform their logging function by altering the memory tables associated with the browser and other system functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors to bypass Windows UAC (User Account Control). The Zeus and Spyeye Trojans use this method exclusively. Non-Windows systems have analogous protection mechanisms that the keylogger must thwart.
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: These are local software keyloggers with an added feature that allows access to locally recorded data from a remote location.
Related features:
Software keyloggers may be augmented with features that capture user information without relying on keyboard key presses as the sole input. Some of these features include:
Clipboard logging: Anything that has been copied to the clipboard can be captured by the program.
Screen logging: Screenshots are taken to capture graphics-based information. Applications with screen logging abilities may take screenshots of the whole screen, of just one application, or even just around the mouse cursor. They may take these screenshots periodically or in response to user behaviours (for example, when a user clicks the mouse). A practical application that is used by some keyloggers with this screen logging ability, is to take small screenshots around where a mouse has just clicked; thus defeating web-based keyboards (for example, the web-based screen keyboards that are often used by banks), and any web-based on-screen keyboard without screenshot protection.
Programmatically capturing the text in a control: The Microsoft Windows API allows programs to request the text 'value' in some controls. This means that some passwords may be captured, even if they are hidden behind password masks (usually asterisks).
The recording of every program/folder/window opened including a screenshot of each and every website visited: The recording of search engines queries, instant messenger conversations, FTP downloads and other Internet-based activities (including the bandwidth used).

IV. ANTI-KEYLOGGER

An anti-keylogger (or anti–keystroke logger) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on your computer. In comparison to most anti-virus or anti-spyware software, the primary difference is that an anti-keylogger does not make a distinction between a legitimate keystroke-logging program and an illegitimate keystroke-logging program (such as malware); all keystroke-logging programs are flagged and optionally removed, whether they appear to be legitimate keystroke-logging software or not.

A. Types Of Anti-Keyloggers:

1) Signature-based:

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.

2) Heuristic analysis:

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

© 2016 IJRRA All Rights Reserved

option to unblock all the modules, but they can cause difficulties among inexperienced users.

B. KeyLog Detector:

In our proposed work we create an application to detect if a potential KeyLogger software or other malicious software may be running on the system which could be hidden and unknown to the user. The application will run in the background and warn the user whenever any malicious software is suspected. Anti-viruses do not generally categorize many of these applications like the KeyLogger as a virus and allows it to run on the system without further looking into it. Our work, 'KeyLog Detector' application detects the suspected malicious potential threat to the system which might have further led to identity thefts or thefts of crucial personal information or data. Anti-vius may be used to detect a certain virus and prevent the computer from its attack but it may not work against other critical applications or processes which may amount to cyber crime.

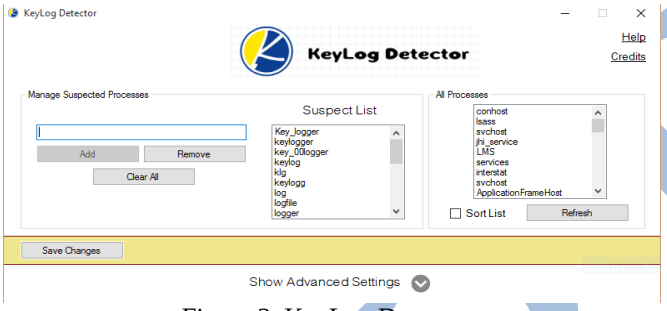

Figure 2. KeyLog Detector

By default, the KeyLog Detector runs in the background on startup and whenever a process suspected by the user or by the program initiates, it curbs it there and then. The user can change the frequency of this process scan to a more desirable number. The more the scan delay is, the less memory will be consumed. Though, quite a high scan delay will mean that scan is not occurring quite frequently. It is possible that the suspected process may trigger through an ajax program or through network trafficking, which will allow the process to generate only when a specific web browser or a specific website is triggered, respectively or both. Soon after the job is done on the particular website, the process may be ended. So, the scan delay is recommended to be set at 5 seconds so that it can detect such programs within time.

V. LITERATURE SURVEY

Siddharth Ghansela Network security is main issue of this generation of computing because many types of attacks are increasing day by day. Establishing a network is not a big issue for network administrators but protecting the entire network is a big issue. There are various methods and tools are available today for destroying the existing network. In this paper we mainly emphasize on the network security also we present some major issues that can affect our network [1].

S. Vinothkumar Keylogger, a highly specialized tool designed to record every keystroke made on the machine to giving the attacker the ability to steal large amounts of sensitive information silently. The primary objective of this project is to detect keylogger applications and prevent data loss and sensitive information leakage. In This project aims to identify the set of permissions and storage level owned by each of the applications and hence differentiate applications with proper permissions and keylogger applications that can abuse permissions .This technique of detecting keyloggers is completely Black-box. It is based on behavioral characteristics common to all keyloggers and it does not rely on the internal structure of the keylogger. The paper intends to develop a machine learning-based keylogger detection system on mobile phones to detect malware applications.[2]

Preeti Tuli It is likely that about one out of many large companies systematically monitors the computer, internet, or email use of its users employees. There are over hundred's different products available today that will let organizations see what their users do at work on their "personal" computers, in their email, and on the internet. But what do such numbers really mean? What does company monitoring of user/employee email, internet, and computer usage actually look like? What sorts of things can an organization/company see users do at their computers, and what sorts of computer activities are currently invisible to workplace monitoring? This admittedly document attempts to propose, as concretely as possible what "Informational Flow" on internet and computer usage looks like: its extent, the key concepts involved, and the forces driving its adoption. The keylogging program logs all keystrokes (aka Keystroke Logging) along with the name of the application in which the keystrokes were entered. Using keylogger we prevent the miscellaneous use of system. Using this we capture all information in text and image form.[3]

William Lopez et. Al., When the Keylogger has been implemented it can focus on its execution. Keylogger implement each technique differently, most use a common execution technique known as hooking. Hooking reroutes the information to its location and returns the information back to the system routine. Hooks can be executed in any operating systems for utmost functions. Keyloggers that are well-made can be executed in the user-mode of operating systems which uses a variation of hooks. Every keystroke are flagged through a message mechanism that gets transferred from the keyboard device to the windows procedures, during the process the hook can grab the information before the information reaches windows procedures. Keyloggers can be developed into implementing a global hook or a local depending on which information the person wants to retrieve from the keystrokes.[4]

Terrye N. Schaetzel et. al., Updating security plans is a continuous process. Internal and external data sources provide a wealth of information for the enterprise to remain predictive and aware of new sophisticated technique employed by cyber criminals. An ever-changing security plan incorporates innovative techniques and tools to reduce exploitation opportunities. Security professionals must stay current, updating certifications and skills sets, to effectively maintain this pace of change. Cyber security is the responsibility of the enterprise rather than a single team. As such, building a culture that supports security standards compliance, teaches its members how to recognize abnormal behavior (e.g., phishing attacks) is vital. Furthermore,

© 2016 IJRRA All Rights Reserved

organizations must reward participation in security programs. People are the eyes and ears of the daily operations, providing broad situational awareness and proactive protection at all levels of the enterprise.[5]

Göran N. Ericsson The introduction of "smart grid" solutions imposes that cyber security and power system communication systems must be dealt with extensively. These parts together are essential for proper electricity transmission, where the information infrastructure is critical. The development of communication capabilities, moving power control systems from "islands of automation" to totally integrated computer environments, have opened up new possibilities and vulnerabilities. Since several power control systems have been procured with "openness" requirements, cyber security threats become evident. For refurbishment of a SCADA/EMS system, a separation of the operational and administrative computer systems must be obtained. The paper treats cyber security issues, and it highlights access points in a substation. Also, information security domain modeling is treated. Cyber security issues are important for "smart grid" solutions. Broadband communications open up for smart meters, and the increasing use of wind power requires a "smart grid system."[6]

Evangelos Ladakis Keyloggers are a prominent class of malware that harvests sensitive data by recording any typed in information. Keylogger implementations strive to hide their presence using rootkit-like techniques to evade detection by antivirus and other system protections. In this paper, we present a new approach for implementing a stealthy keylogger: we explore the possibility of leveraging the graphics card as an alternative environment for hosting the operation of a keylogger. The key idea behind our approach is to monitor the system's keyboard buffer directly from the GPU via DMA, without any hooks or modifications in the kernel's code and data structures besides the page table. The evaluation of our prototype implementation shows that a GPU-based keylogger can effectively record all user keystrokes, store them in the memory space of the GPU, and even analyze the recorded data in-place, with negligible runtime overhead.[7]

VI. CONCLUSION

This paper mainly emphasize on the network security and some major issues that can affect network. Through this paper, we present our work where we create an anti-keylogger named KeyLog Detector specifically designed for the detection of any keystroke logger software along with an optional termination of the suspected process.

REFERENCES

[1] Siddharth Ghansela, "Network Security: Attacks, Tools and Techniques" *International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013*

[2] S. Vinothkumar, "Mobile Keylogger Detection by Using Machine Learning Technique" *International Journal of Engineering Development and Research, Conference Proceeding (NCETSE-2014)*

[3] Preeti Tuli, "System Monitoring and Security Using Keylogger" *International Journal Of Computer Science and Mobile Computing, Volume 2, Issue. 3, March 2013, pg.106 – 111*

[4] William Lopez et. Al., "Keyloggers", *EEL-4789, GROUP 2.*

[5] Terrye N. Schaetzel "Cyber Security: Designing and Maintaining Resilience" *White paper presented by: Georgia Tech Research Institute Cyber Technology and Information Security Laboratory*

[6] Göran N. Ericsson, "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure" *IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 25, NO. 3, JULY 2010 1501*

[7] Evangelos Ladakis, "You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger" *Institute of Computer Science, Foundation for Research and Technology—Hellas, Greece. Columbia University, USA.*

IJRRA

© 2016 IJRRA All Rights Reserved