KEYLOGGERS SOFTWARE DETECTION TECHNIQUES

A.Solairaj[1], S.C.Prabanand[2], J.Mathalairaj[3], C.Prathap[4] and L.S.Vignesh[5]

Assistant Professor [1, 2,3,4,5], Nadar Saraswathi College of Engineering and Technology

Abstract

Keyloggers is the action of recording the key stroke on a keyboard, typically in a covert manner. Software Keyloggers are detected based on the behavioral characteristics. They don't provide root privileges; detection is based on permission from kernel and prone to many attacks. Software Keyloggers is a software program that can be installed onto a computer, which monitors all the user activities on computer. Keyloggers steal the confidential information and they completely run in stealth mode. When Keyloggers is installed in a computer, it is not shown either in start-up icons or anywhere else on the computer that is being monitored. Software Keyloggers have posed a great threat to user privacy and security. Detection of Keyloggers is difficult because they run in hidden mode. Detection of Software Keyloggers is done using various technique namely Anti-Hook techniques, HoneyID: Spyware detection, bot detection, safe access to password protected accounts and dendritic cell algorithm. These algorithms are used to detect the existence of Keyloggers in computer, which strengthens user privacy and security.

Keywords: *Keylogger, HoneyID, Bot, Dendritic cell algorithm.*

1. INTRODUCTION

Keylogging Programs, commonly known as Keyloggers, are a type of malware that maliciously track user input from the keyboard in an attempt to retrieve personal and private information. The keyboard is the primary target for Keyloggers to retrieve user input from, because it is the most common user interface with a computer [1]. Although both software and hardware Keyloggers exist, software Keyloggers possesses a great threat if people have something valuable in their computer. Thus it is the focal point in this paper. But hardware Keyloggers also represents a serious threat to the privacy of computer users. For example, inexpensive hardware Keylogging devices such as the Spy Keylogger act as a medium between various computer components such as physical keyboards, USB adapter, motherboard and USB Port; as the "man in the middle attack". This device stealthily captures and stores all user keystrokes on its memory [2].

Software Keyloggers are applications that capture a computer user's keystrokes and then send this information back to a spying person [3]. Based on the availability of various online free software's, it is very easy to install Keyloggers on victim's computer without user's awareness. Unlike viruses and worms, the goal of Keyloggers is generally not to cause damage to the system or spread to other systems. Instead, Keylogger programs monitor the keystrokes and steal private information by capturing the activities done on a computer. Keyloggers capture keystrokes and saves this information in hidden log files, then sends it back to the attackers. In this process, Keyloggers will leave a small footprint in terms of memory and processor utilization. Some of them even do not show up in the 'Task Manager' or in the list of processes related to an application. The log files are hard to distinguish from operating system files even though directory's hidden files are listed. In other words, they are a master of disguise. In order to achieve their goal, they have to eventually execute the malicious behaviour's: Firstly, monitor keystrokes of the user. Secondly, leak the information captured (e.g. save the data to a file or transmit information to a remote host).

Most of the Keylogging detection techniques is based on signature-based detection and behaviour-based detection techniques. The biggest disadvantage with the signature-based technique is that it cannot detect novel Keyloggers. In behaviour-based detection technique, it analyzes the incoming file signature and detects the behaviour of that application.

This paper contains the following sections. Section 2 highlights the various Keylogging detection techniques. Section 3 discusses the recent attacks of Keyloggers. Section 4 and 5 includes conclusion and future work.

2. KEYLOGGING DETECTION TECHNIQUES

2.1 Anti-Hook Technique

Anti-Hook mechanism detects both known and unknown Keyloggers. This technique is based on the fact that each processes either hidden or on display uses hooks API for the purpose of hooking. Hooking spans a range of techniques which is used for altering the behaviour of an operating system or any applications. Hooking prevents function call or messages which pass through various software components. This technique can scan all the processes, static executables, DLLs (Dynamic Link Libraries) and detect suspicious processes or files, which uses hooks. On whole, this technique collects the complete details about that process or file which uses hooks. A windows hook i.e. events associated with desktop is the critical information required by Keyloggers as an input. The current technique can intercept events before they reach an application. The function can act on events, modify or discard them. Functions which receive the events are called filter functions; every filter function is classified by its type. Hooks provide powerful capabilities; process or modify every message; record or play back keyboard and mouse events; prevent another filter from being called; and many more capabilities [4].

Generally, there are two types of hooks: System-wide, and Thread-specific. The System-Wide hook is used for filtering messages of all applications and Thread-specific hook is used for filtering messages of a specific thread. In this approach, we enumerate all the hidden as well as visible process by index from task manager and then we enumerate the dynamic link libraries of each and every process. The command SetWindowHookEx is used to install the hook and this API lies under the banner of USER32.LIB. The technique disassembles entire running processes in search of SetWindowHookEx. If any process or dynamic link libraries use this API, the installation of hook will be detected as shown in figure 1 [4]. The goal of anti-hook technique is to find out SetWindowHookEx command in all type of processes and in their respective dynamic link libraries. Anti-hook technique sends all information to an anti-Keylogger, so that the user can witnesses all the activities done by the Anti-Hook technique. The advantages of this technique include user privacy and security. But this technique fails to detect all the types of attacks and also prone to false positives. The false positive says that erroneously a positive effect has been assumed [4].

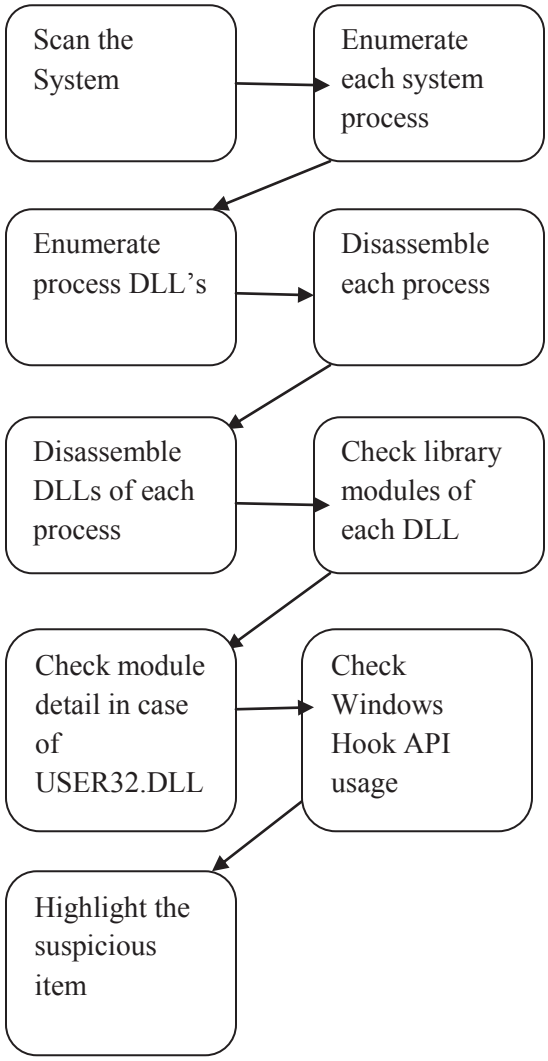

Figure 1: Anti-Hook Approach [4]

2.2 Safe Access to Password Protected Accounts

An Internet cafe machine can be easily running a Keylogger. The users operating their mail account from Internet cafe are unaware of the presence of Keyloggers and they have no alternative way apart from typing their password. To overcome this problem, the user can employ a simple trick for concealing the password. The string of keys sent to the browser will often contain domain names, followed by userid and password.

For example:

www.google.comsarah@gmail.comsnoopy2 [5]

The information is sent to the Keylogger as sarah@gmail.com has the Password "snoopy2" at Gmail. The approach used here is to insert a sequence of random characters between successive keys of the password. By applying this technique, the content viewed by the Keylogger will not affect normal login. The Keylogger can view everything, but cannot understand the generated keystrokes. The browser also views everything, but does not know what to do with keys that are typed anywhere other than the text fields. The Keylogger finds it difficult to detect the keys used by the browser. The Keylogger easily records all the keys or mouse events but fails to determine which applications used those events. The procedure used to detect the Keylogging events in Internet cafe is shown in figure 2 [5].

Navigate to the login page desired;

Type in the user id;

For (each password character)

Give focus to anywhere but the password field;

Type some random characters;

Give focus to the password field;

Type the next character of the password;

Submit:

Figure 2: Keylogger Detection Procedure [5]

The procedure involves typing random characters between successive characters of the password field using the mouse. For example, if the user types a password named "snoopy2". The Keylogger views the content as:

www.google.comsarah@gmail.comspqmlainsdgsosd gfsodgfdpuouuvnydg2

The actual password of the user consists of 7 characters. Using this technique, a total of 26 characters are inserted between the original password. The advantage of this technique includes concealing the password: since Keylogger can't differentiate keys typed in the text field and keys typed apart from the text field. The drawback includes Virtual keyboard: a screen capture at every keystroke will reveal which of the keys typed using this technique belong to the password [5].

2.3 HoneyID: Detecting Spyware

HoneyID is a Spyware detection mechanism, which can detect unknown spywares. This technique lures the attacker. Bogus events are generated in order to trigger the spyware's actions. The hidden spyware among running processes are detected. The basic concept of HoneyID is shown in figure 3 [6].

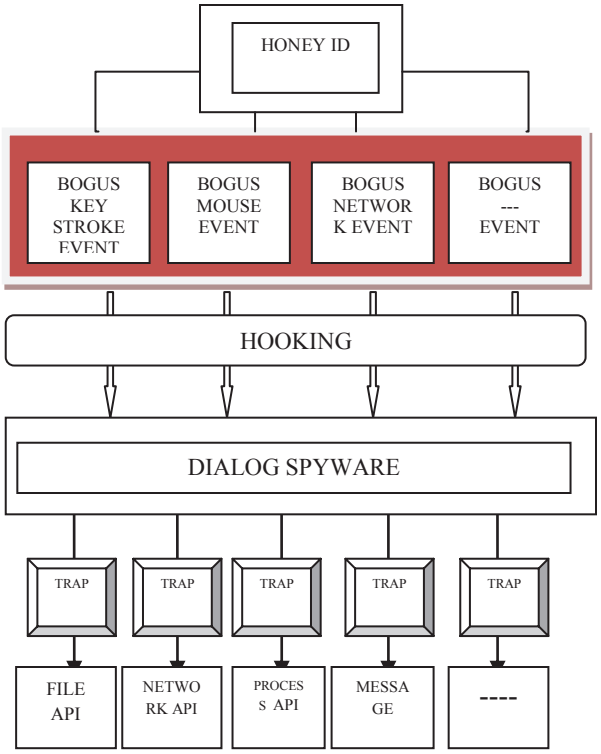

Figure 3: Basic concept of HoneyID [6]

HoneyID consists of the trap and bogus events. The trap component monitors the changes in each process and the bogus event is user events which can make the dialog spyware operate i.e. working using a specific user activity. HoneyID sets up a trap in the operating system by generating bogus events in order to detect the spyware process. The change of process is checked by HoneyID. If a process response to any generated bogus events, HoneyID identifies it as a dialog spyware. The HoneyID architecture consists of three modules namely trap manager, bogus event generator and spyware detector. The trap manager sets up traps in the operating system by gathering the number of jobs of each process. In response to the

commands from the spyware detector, the bogus events generator generates various bogus events. The spyware detector differentiates the normal process and the spyware process by measuring the process condition. It also controls the other two modules. The advantage of this technique includes detecting unknown spyware with high accuracy in terms of speed. The disadvantage of this technique is high implementation cost. This technique detects only privileged process.

2.4 Bots detection

A software named Bot, installed on user's computer without their knowledge. It is malicious in nature. The software communicates with the attacker (IRC) internet relay chat network as a communication channel. The software responds to the instructions sent by the attacker. These instructions direct the bot software on the infected machine to perform malicious activities. A bot spreads to other hosts by exploiting known vulnerabilities in operating system and other applications. The user's computer gets infected by different ways such as worms, emails viruses etc. The bot software installed on a user's computer, changes the system configuration each time the system boots. This software spreads itself by sending more emails across to various computers. This affects various computers. The bot connects to the IRC server to join the channel. The bot executes default commands or it waits for the botmaster commands. The botmaster and bot communicates through the IRC protocol. The advantage of IRC protocol is to provide flexibility in the management and control of bots. The bot software is controlled by the botmaster using various types of communication such as HTTP protocol or peer to peer networks [7].

Single bot can be detected using an algorithm named Spearman's Rank Correlation (SRC). This algorithm monitors and correlates various activities on the system by executing different API functions to detect the presence of bot software. This algorithm focuses on three types of bot behaviour namely Keylogging activity, file access and outgoing traffic. Spearman's rank correlation algorithm performs correlation between different behaviours of the bot such as capturing the user keystrokes and sending them directly to the IRC channel within the specified time limit. These correlated events indicate the presence of bot software in the system. The algorithm describing the bot detection is shown in Figure 4 [7]. This algorithm uses two data sets: set1 represents the byte sent and set2 represents the bytes written in the file. The detection algorithm is divided into four cases. No detection case represents the absence of Keylogging activities. Weak detection case represents low correlation seen in both data sets when Keylogging activity is detected. Normal detection case represents high correlation in one data set during the detection of Keylogging activity. Strong detection case represents high correlation noticed in both data sets [7].

Algorithm 1: Bot Detection Algorithm using Spearman's Rank Correlation(SRC)

```
if KeyboardState function(s) is executed
(i.e.keyloggingactivity)then
if SRC[KeyboardState,CommFunc]>Threshold and
[KeyboardState,FileAccess]>Threshold then
                Strong detection
else if SRC[KeyboardState,CommFunc]<SRC
[KeyboardState,FileAccess]>Threshold) then
                Weak detection
else if(SRC[KeyboardState,CommFunc]<Threshold
and
SRC[KeyboardState,FileAccess]>Threshold) or
(SRC[KeyboardState,CommFunc]> Threshold and
SRC[KeyboardState,FileAccess]<Threshold) then
                Normal detection
else
   No detection and normal activity is considered
end
```

Figure 4: Bot detection algorithm using Spearman's Rank Correlation (SRC) [7]

The merits of this algorithm include indicating the presence of bot software in the system within the specified time limit. It monitors various types of bot behaviours. It is effectively used to detect single bot. This algorithm performs bot detection based on Keylogging activity. This algorithm cannot detect Keylogging activity SYN attack or UDP attack. It effectively detects single bot within a specific time-window. The algorithm fails to detect, if the bot master waits for a random time to perform another task. Thus leading to weak detection decision [7].

2.5 Dendritic Cell Algorithm

The Dendritic Cell Algorithm (DCA) is used for detect Keyloggers installed on a user computer. The detection is based on correlation between different behaviours such as Keylogging, file access and network communication. DCA differentiates the Keylogger process from the normal process based on the behaviour point of view. The time-window of the correlation is not specified as the dendritic

correlations have different migration thresholds. This makes it difficult for the Keylogger to evade this technique. The major merits of this technique is high detection rate and low false alarm rate**.** The drawback includes low performance when long sentences are encountered [3].

3 CASE STUDIES

3.1 Researchers discover keyboard Keylogger attack via iPhone: Attack depends on exploiting Smartphone accelerometer

A research team from the Georgia Institute of Technology says that they have discovered a keyboard Keylogger attack that can be done through a compromised Apple iPhone. The attack relies on exploiting the iPhone accelerometer technology. The accelerometer helps you figure out the orientation of the device. It will adjust what's in the screen and you can use it to turn your phone to play games. The Georgia Tech researchers have found a way to exploit the accelerometer to capture keystroke data on a nearby computer keyboard if the iPhone is positioned within a few inches. The attack methodology relies on getting the victim to inadvertently install an iPhone app that is designed to collect this type of keyboard Keylogger data, or have the function included in another type of applications like playing a game. When the iPhone is positioned within a few inches of a computer keyboard, it can kinetically capture the keyboard's physical vibration. The attack method has so far shown an 80% success rate. Every time you touch a key you create a physical vibration and it's recorded by the accelerometer in the phone. If anyone is concerned that others may be trying something similar, they can simply move their Smartphone at least half a feet away from their keyboard, he notes, or stores it elsewhere [8].

3.2 Keyloggers in net banking

Welcome to Safe Bank's net banking. Please enter your net banking userid and password.

Userid: 15236523
Password: **********

Action = submit.jsp

And you have logged into net-banking application. You can now view your account balance, do third party funds transfer and much more.

Location:
C:\WINDOWS\system32\config.dll

File contents:
08-Aug-08: 08:00: Window title: Welcome to Safe Bank net banking
Userid: 15236523 [tab] Password: Welcome123! [9]
When you browsed to your net banking page and typed in your username and password to login into the online bank, there was a malicious program you were unaware of, named Keylogger running in the background logging all the keystrokes into a config.dll file located in C:\WINDOWS\system32 folder. This file contains all the keystrokes typed in. It contains the window title and all those things typed into that window along with few other details. This file will be uploaded to the attacker's website which he can use to his benefit [9].
These Keyloggers are easily and freely available on internet and also integrated with other programs like rookits making its detection very difficult. So your chance of being infected by such a malicious code even if you have an updated antivirus/anti-Spyware program is about 70% [9].

4 CONCLUSION

This paper mainly focuses on various software Keyloggers and its effects on computer system. Keyloggers records all the keystrokes and user activities on the computer, steals confidential information like password, credit card number and send to the attacker. Thus various detection techniques are discussed here with each of the techniques merits and demerits. All of these techniques strengthen the user privacy and security.

5 FUTURE ENHANCEMENT

Mobile Keyloggers is a software program that can be installed onto a mobile phone, which monitors all the user activities on mobile. Keyloggers steal the confidential information and they completely run in stealth mode. When Keyloggers is installed in a mobile, it is not shown either in start-up icons or anywhere else on the phone that is being monitored. Mobile Keyloggers have posed a great threat to user privacy and security. Detection of Keyloggers is difficult because they run in hidden mode. Detection of mobile Keyloggers is done using a new technique namely Support Vector Machine. Support vector machine is a supervised learning model with associated learning algorithm that analyzes data and recognizes patterns used for classification and regression analysis. Classification is a problem of identifying to which of a set of categories a new

observation belongs, on the basis of a training set of data containing observations whose category membership is known. Regression analysis is widely used for prediction and forecasting. Regression analysis focuses on the relationship between a dependent variable and one or more independent variable. This machine learning algorithm detects the existence of Keyloggers in mobile phones, which strengthens user privacy and security

REFERENCES

[1] "Keyloggers in Cybersecurity Education," Christopher A. Wood, Rajendra K. Raj, In Proceeding of the 2010 International Conference on Security and Management, pp. 293-299, July 12-15,2010.

[2] ThinkGeek.com [2010], "Spy Keylogger" [online], Available: http://www.thinkgeek.com/gadgets/security/c49f/ .

[3] "Detecting Software Keyloggers with Dendritic Cell Algorithm," Jun Fu, Yiwen Liang, Chengyu Tan, Xiaofei Xiong, In Proceeding of the 2010 International Conference on Communications and Mobile Computing, pp.111-115, April 12-14,2010.

[4] "Anti-Hook Shield against the Software Keyloggers," M. Aslam, R. Idrees, M. Baig and M. Arshad, In Proceeding of the 2004 National Conference on Emerging Technologies, pp.189-191, 2004.

[5] "How To Login From an Internet Café Without Worrying About Keyloggers," Cormac Herley, Dinei Florencio, In Proceeding of the Association for Computing Machinery, Inc, pp.2, July 2006.

[6] "HoneyID: Unveiling Hidden Spywares by Generating Bogus Events," J. Han, J. Kwon, H. Lee, In the Proceeding of IFIP 23rd International Information Security Conference, pp.669-673, 2008.

[7] "Detecting Bots Based on Keylogging Activities," Y. Al-Hammadi, U. Aickelin, In the Proceeding of 3rd International Conference on Availability, Reliability and Security, pp.896-902, 2008

[8] Ellen Messemer, Network World [Oct 18 2011], "Researchers discover keyboard Keylogger attack via iphones" [Online], Available: http://www.networkworld.com/news/2011/101811-Keylogger-iphone-252123.html.

[9] Santosh Jadhav, [Feb 2009], "Virtual Keyboard and the Fight against Keyloggers" [Online], Available: http://palpapers.plynt.com/issues/2009Feb/fight-against-keyloggers.