Detection and Prevention of Keylogger Spyware Attack

Miss.Suchita Yadav*, Prof.Ravi Randale.
Pillai Hoc College of Engineering & Technology,Rasayani
suchitayadav304@gmail.com

ABSTRACT

A Keylogger is also known as keystroke logger. It is a software or hardware device which monitors each and every key typed by user on user keyboard. User can not identify the presence of keylogger on user computer since it runs in background and also it is not listed in task manager or control panel. It can be used by parents to keep eye on their children's or company owner to spy on their employees. A keylogger is a type of surveillance software (considered to be either software or spyware) that has the capability to record every keystroke you make to a log file, usually encrypted. Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. It is very harmful for those systems which are used in daily transaction process i.e. online banking system. A keylogger spyware contains both scripts keylogger and spyware in a single program. We propose a detection and prevention technique for keylogger spyware attack capable of stealing the credentials and confidential information from the infected user's system. The detection is performed by the help of honeypot and keystroke agent. The prevention is performed by the help of encryption algorithm.

I. INTRODUCTION

Malware steals information from a computer or can cause damage. Type includes keylogger, spyware, adware, rootkit etc. In short we can say that it is a program that is intentionally developed to cause harm or exploit people computers especially which are connected to Internet [11]. The thing which makes them more hazardous is that they reinstall themselves again even after they have been removed and are difficult to be cleaned as they hide themselves deep within Windows [12]. It has become very crucial to provide efficient security solutions for these attacks. A keylogger spyware is a different kind of malware attack which uses two malwares program in a combined script. We propose a honeypot and keystroke agent based detection and encryption based prevention technique for the keylogger spyware attack.

We design a keystroke agent application to frequently generate random keystrokes, hoping that these keystrokes will be seen by the keylogger, but will not affect normal applications. Key agent is a keystroke base simulation program. The randomly generate keystroke are not visible to other applications only to keylogger. Keystroke agent synthesizes random keystroke to induce keyloggers and the key agent simulate keyboard event completely. A keylogger tracks keystroke of all application including key agent application in order to log sensitive data. A keylogger cannot analyze whether a keystroke are generated by real user or keyboard agent.

II. PROBLEM STATEMENT

Hackers use malware to breech the security of a system and when they get success it causes lots of trouble to security experts. Malware can be of many types (i.e. keylogger, spyware, rootkit etc). Keylogger is a software or hardware device which monitors each and every key typed by user on user keyboard.

User can not identify the presence of keylogger on user computer since it runs in background and also it is not listed in task manager or control panel. We propose a detection and prevention technique for keylogger spyware attack capable of stealing the credentials and confidential information from the infected user's system. The detection is performed by the help of honeypot and keystroke agent. The prevention is performed by the help of encryption algorithm.

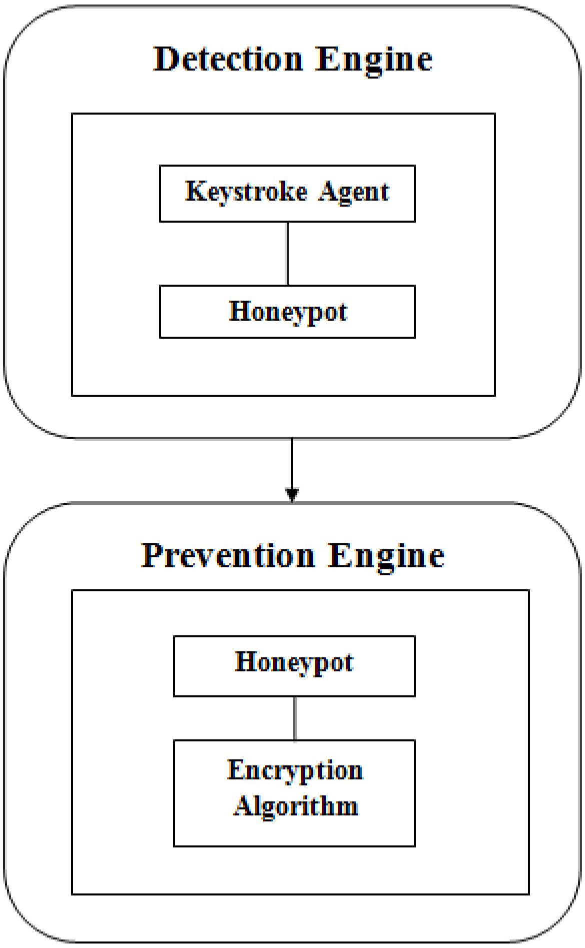


Fig: Architectural model of Keylogger

Above fig shows architectural model of keylogger. The model is divided in two parts Detection engine and Prevention engine. Detection engine contains keystroke agent and honeypot system and Prevention engine contains honeypot and encryption algorithm.

A. Detection Engine

Step 1: Keylogger Logfile Creation

A small, fairly simple program captures everything the user is doing - keystrokes, mouse clicks, files opened and closed, sites visited. A little more sophisticated programs of this kind also capture text from windows and make screenshots (record everything displayed on the screen) - so the information is captured even if the user doesn't type anything, just opens the views the file. These programs are called key logging Programs. When enter key pressed keylogger sends captured information to hacker using a randomly selected email id.

Step 2: Keylogger Retrieves user PC Network Information

This module retrieves user PC network information like IP address, Domain Information, LAN settings etc.

Step 3: Keystroke Agent Program

A keystroke Agent application which runs parallel in a client pc , generates random keystrokes hoping that these keystrokes can be seen by keylogger. The randomly generated Keystrokes are not visible to other application only to keylogger. In induction phase a keystroke agent synthesizes random keystrokes to induce keylogger. The keystroke agent simulates keyboard event completely.

Step 4: Keylogger Program Stores Keystrokes in a Log file

The key logger tracks keystrokes from all application including Keystroke Agent application in order to log sensitive data along with the time of entering keystrokes. The keylogger cannot analyse keystrokes generated by a real user or via Keystroke Agent.

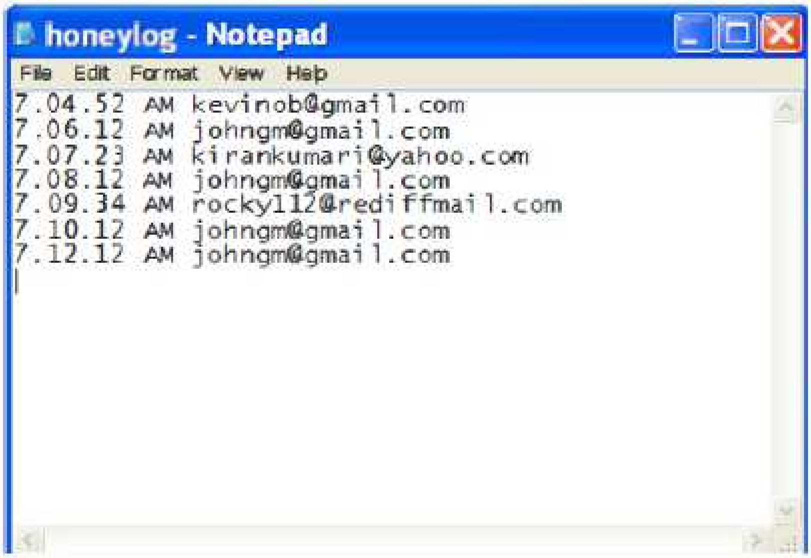
Step 5: Hacker's Email Settings File

Hacker sends this information (periodically) to randomly selected email id which are stored in a database.

B. Prevention Engine

Step 6: Spyware Detection Honeypot System

A spyware detection program also generates a log file and sends this file to honeypot server. At detection prevention server this file is inspected for threats. For example given below figure shows log file generated by honeypot system. An email was sent to kevinob@gmail.com is shown at 7.04. 52 AM time with that attached spy log file (having all). Thus keylogger spyware program continues its email sending process (i. e. at, 7.05. 52 AM, 7.06. 52 AM). The spyware detection program finds that emails are sent to kevinob@gmail.com after every 1 minute. It is traced out in the inspection process and marked as a suspicious item.



```
7.04.52 AM kevinob@gmail.com
7.06.12 AM johngm@gmail.com
7.07.23 AM kirankumari@yahoo.com
7.08.12 AM johngm@gmail.com
7.09.34 AM rocky112@rediffmail.com
7.10.12 AM johngm@gmail.com
7.12.12 AM johngm@gmail.com
```

Fig: Honeylog

Step 7: Encryption and Removal Process

After the detection of key logger spyware the work of prevention is started and then we run as encryption program to encrypt the log file. A honeypot prevention server removes the keylogger malicious program from user's system.

III. CONCLUSION

The discussed attacking scenario is very threatening as it is making a combination of two malwares i. e. keylogger and spyware. It can steal the credentials or any confidential information typed can be leaked. So the detection and prevention of this attack becomes very crucial. In this system the detection is performed by the help of honeypot and keystroke agent. The prevention is performed by the help of encryption algorithm. The log file now store data generated both from user and key agent. In parallel original log file is created only from user data by the keyboard agent. This original logfile encrypted and send to the honeypot system for further detection. After inspecting this logfile the honeypot system delete keylogger if required and finally keylogger program which sent to hacker is not original logfile but scrambled logfile.

IV. REFERENCES

[1] Mohmmad Wazid, AvitaKatal, R.H.Goudar,"A Framework for Detection and Prevention of Novel Keylogger Spyware Attacks.",7th International Conference on Intelligent System and Control(ISCO 2013).

[2] Zhen J.,Liu, Z, : New honeypot system and its application in security of employment network. In : IEEE Symposium on Robotics and Applications (2012).

[3] Liu, D., Zhang, Y.: An Intrusion Detection System Based on Honeypot Technology. In : ACM International Conference on Computer Science and Electrical Engineering (2012).

[4] Sanjeev, K., Rakesh, S: Bhatia J.S: Hybrid Honeypot Framework for Maleware Collection and analysis. In 7th IEEE International Conference on Industrial and Information Systems (2012).

[5] David, M., Rajeev, A,:A study of Methodologies used in Intrusion Detection and Prevention Systems(IDPS). In: Proceeding of IEEE Southeastcon(2012) .

[6] Yun, Y., Jia, M.: Design and implementation of distributed intrusion detection system based on honeypot. In 2nd IEEE International Conference on Computer Engineering and Technology(2010).

[7] Mohamed, N., Radu, S., Olivier, F.: VOIP Malware: Attack Tool & Attack Scenarios. In IEEE International Conference on Communications (2009).

[8] Li, S., Roland, S.: A Novel Anti-Phishing Framework Based on Honeypots. IEEE eCrime Researchers Summit (2009).

[9] Yao, Y., Lv, J-W., Gao, F-X., Yu, G., Deng, Q –X.: Detecting and Defending against Worm Attacks Using Bot-honeynet. In: 2nd IEEE International Symposium on Electrionic Commerce and Security (2009).

[10] Hassan, A., Haider, S., Malek, S., Iyad K., Zaid, A.M.: A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks. Elsevier Journal of Computer & Security 25(4), 274-288 (2006) Cross Ref.

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

[12] Malware in Information Security Available at www.infosecwriters. com/text resources/pdf/jdukes maleware.pdf

[13] J. Fu, Y. Liang, C. Tan, and X. Xiong, "Detecting Software Keyloggers with Dendritic Cell Algorithm", in Proc. of the International Conference on Communications and Mobile Computing, 2010 , pp. 111–115.