INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET)

ISSN 0976 – 6367(Print)
ISSN 0976 – 6375(Online)
Volume 5, Issue 12, December (2014), pp. 167-172
© IAEME: www.iaeme.com/IJCET.asp
Journal Impact Factor (2014): 8.5328 (Calculated by GISI)
www.jifactor.com

IJCET

© I A E M E

DETECTION AND PREVENTION OF KEYLOGGER SPYWARE ATTACKS

Akhil S, Neeraja M Nair, Asst Prof. Arun R

Department of Computer Science and Engineering
Sree Narayana Gurukulam College of Engineering, Kolenchery, Ernakulam, Kerala

ABSTRACT

The In cyber world the detection and prevention of malware attack is an important issue since malwares can disrupt computer operation, gather sensitive information, or gain access to private computer systems. The keylogger spyware is extremely harmful for system which are used in daily transaction processes. The keylogger records the key strokes pressed by system user and stores them in a log file and the spyware email this log file to the malicious user. Hence it is important to protect form these attacks. In this paper we propose a method for detecting and preventing keylogger spyware attack.

Keywords: Keylogger Spyware Attack, Keylogger Spyware Detection and Prevention System, IDS, DoS.

1. INTRODUCTION

Malware is used to disrupt computer operation, gather sensitive information, or gain access to private computer systems [10]. Key logger, spyware, adware, rootkit etc. are some types of malware. 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 [8]. 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 [9]. Unlike other types of malicious program, keyloggers present no threat to the system itself. Nevertheless, they can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, cyber criminals can get PIN codes and account numbers for e-payment systems, passwords to online gaming accounts, email addresses, user names, email passwords etc.[11]. Hence it is critical to protect a system from these types of attacks. Here we propose a method to protect the system from keylogger spyware attack in a network. The Section 2 describes the related work. In section 3 we have provided an overview of malwares and its types. Section 4 describes the proposed method for key logger detection and prevention. Then the conclusion is in section 5.

2. BACKGROUND AND RELATED WORKS

The paper [1] provides a framework for detecting and preventing keylogger spyware attacks. This method uses a honeypot which is applied in the network for monitoring the users system. A detection and prevention system is used for detecting keylogger and for removing it. This method can be vulnerable if the attacker uses database of email addresses for sending email of user key log to malicious user. The paper [2] includes a survey on the different techniques used for malware detection. The techniques discussed are obfuscation, fragmentation and session splicing, application specific violations, protocol violations, inserting traffic at IDS, DoS etc. It also discusses some mitigations such as sandboxing,

session reassembly, data execution prevention, address space layout randomization, control flow integrity. The paper [3] shows an integrated framework of malware collection and analysis. It uses the server honeypots and client honeypots. Here the analysis of the collected malwares using honeypots is done. The paper [4] proposes an Intelligent Intrusion Detection System for unknown malware attacks. The technique uses simple data mining method to process the network data. The system combines anomaly, misuse and host based detection. An attack classification method is proposed by which attacks are classified based on vulnerability. The classification results are arranged based on attack propagation skills and attack intentions. The paper [5] proposes a data mining algorithm, the PrejixSpan method. It aims to discover some frequent new sequential attack patterns of malware. The PrejixSpan is implemented for analysing the malware footprints. The result of analysis shows that within a short amount of time the attacks are performed by multiple sequential attack patterns. A new type of malware attack for VoIP infrastructures and services is mentioned in paper [6]. These malwares can cause damage to the VoIP architectures. The "VoIP bots" are introduced which support attacks such as SPIT, DDoS etc. They are also tested with several VoIP platforms. The paper [7] describes an analysis framework specifically developed to which provides insight into honeynet data. The aim of the procedure is to find, within an attack data set, groups of network traces sharing various kinds of similar patterns. Thy seek to design a clustering tool, in exploratory data analysis, that can be applied in a systematic way for characterizing the attacks. The application of the method is illustrated in it by analysing one specific aspect of the honeynet data, i. e. the time series of the attacks. An alternative user authentication based on images that is resistant to keylogger spyware is presented in paper [8].To secure passwords cryptographic hash function is used .This design is highly resistant to brute force attacks while prone to Dictionary attack, allowing users to retrieve their passwords from any location.

3. OVERVIEW OF MALWARES

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems [10].Malware is classified into various categories such as: adware, spyware, dialers and toolbars [9].

3.1 Adware

Adwares are those which are mainly used for advertisement purposes. They are usually placed as pop-ups on web pages .The pop-up stoppers are embedded in Internet Explorer but they cannot block many block pop-ups. These pop-ups may show up while the user is playing online game, listening online music etc. It mostly shows the advertisement which is relating to what the user is surfing or the web page user visits.

3.2 Spyware

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 [12]. Spywares can have different tasks such as sending URL information, sending information you type, searching hard drives and reporting back programs installed, stealing contents of email address books etc. Useful information about the user such as login names, passwords, credit card numbers, phone numbers, address etc can be easily stolen.

3.3 Hijackers

Hijackers take control of various parts of web browser including the home page, search pages and Asearch bar. These attacks may cause the user to visit some website by mistyping of address so as to prevent user from visiting websites used to combat malware. Some even redirect to their own search engine when user search is made.

3.4 Toolbars

Toolbars are those which provides functionalities like pop up blockers or search forums and they are plugged into the browser. They may look and function like legitimate tool bars like google. They are harmful and have characteristics of malware.

3.5 Dialers

Dialers are those programs which are basically used to connect to 1-900. Dialers are installed silently and cause users to have huge bills.

3.6 Keylogger

Keylogger or keystroke logger can be software or hardware device used to monitor the keys user types on the keyboard. Usually it runs in background and its presence can't be detected. Its information is not present in the task manager or control panel. It can take very sensitive information such as username passwords etc.

The malware attacking scenario is more effective if combination of above discussed types is used. Here, the key logger spyware attack is considered which is a combination of keylogger and spyware program. The keylogger script is used to store every keystroke into a file and then generate a log file then the spy script email this log file to the malicious user.

4. PROPOSED METHOD FOR KEYLOGGER DETECTION AND PREVENTION

Hackers make use of malwares to breach the security of a system. Malware can be key logger, spyware, rootkit etc. They can also come in combination i. e. key logger spyware as a common program. In this paper we have propose a method for detecting and preventing keylogger spyware attacks. The proposed method is expected to detect and defend against such kinds attacks. The following method in section 4.1 is used for the proposed framework. Initially a keylogger spyware attacking scenario can be considered as in section 4.1.

4.1 Keylogger Spyware Attack

The key logger spyware attack works as shown in Fig 1. In the figure there are 3 users accessing various services via internet such as online banking email etc. A malicious user is present hosting a key logger spyware which enters into the users system like any other application software. It may act as a legitimate software hence the user downloads and installs it which is actually a malicious program. As it is installed it starts capturing every keystroke and then generate a log file which contains all keystrokes. The spy script included will then email this log file to a specified email address of the attacker.

The red coloured arrows in Fig 1 represents the entry of Keylogger into users system. As the keylogger enters into users system, the automatic email process by spyware script takes place as shown in figure 2. The blue arrows shows this process in Fig 2

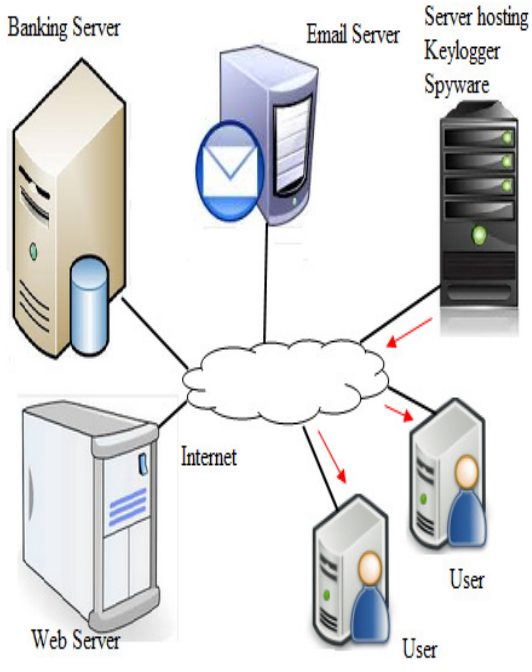

Fig 1: Keylogger Spyware attack on Users

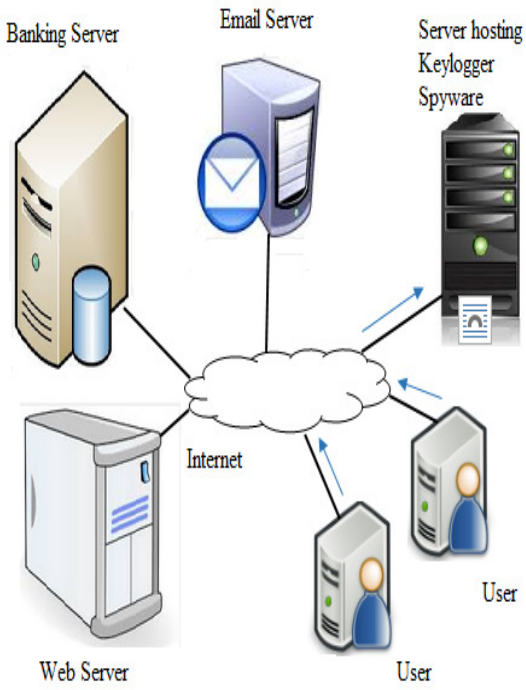

Fig 2: Transfer of email containing confidential information from users system

The key logger spyware remains hidden such that the users are not aware of the functioning of malicious program. They might login into online banking account, email account etc using their system. When the user types using keyboard the keystrokes are captured and stored in a log file(i.e. spy log shown in Fig 3). This log file will be further emailed to the malicious user periodically (i.e. after every 2 minutes).The log file may contain sensitive information and hence the user can lose entire money from banking account or the users email account can be easily hacked.

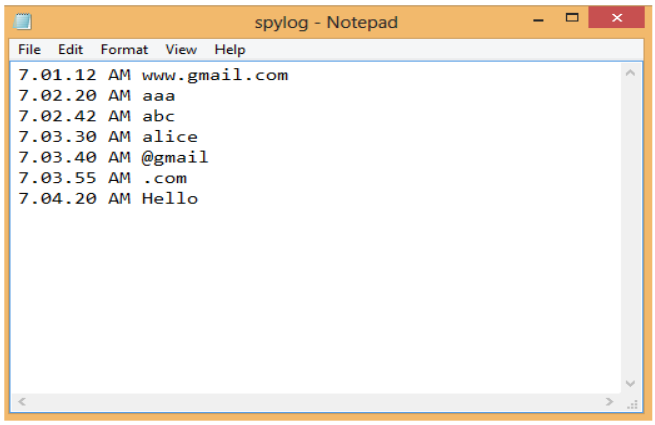

Fig 3: Log file generated by Keylogger

Fig 4 is a snapshot which shows email sent to alice@gmail.com by a user who is one of the user of system having key logger spyware program. The entire message is captured by keylogger and it is saved in generated spylog file as shown in Fig 3. Key logger generates the spy log file which shows every keystroke by the user. Here aaa and abc might be the credentials of users email account.

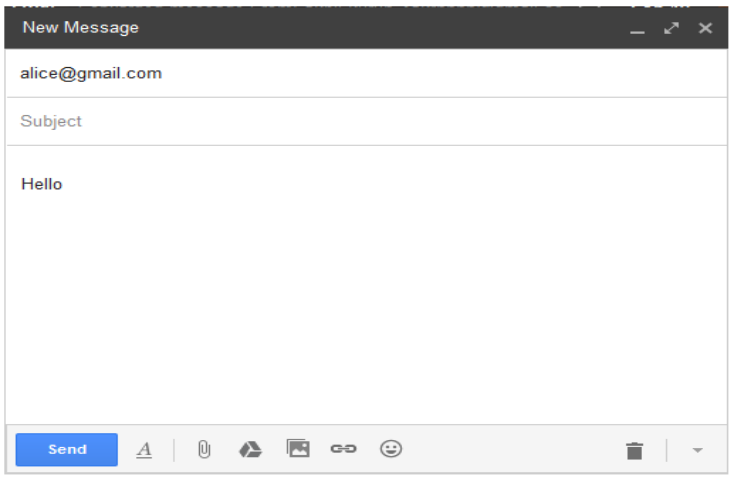

Fig 4: Email sent by user to Alice

4.2 Detection and Prevention System

Monitoring of such attacks can be done by using a detection and prevention server in the network of clients as shown in Fig 5. It should be designed such that it is not easily compromised and hackers are not able to detect it.

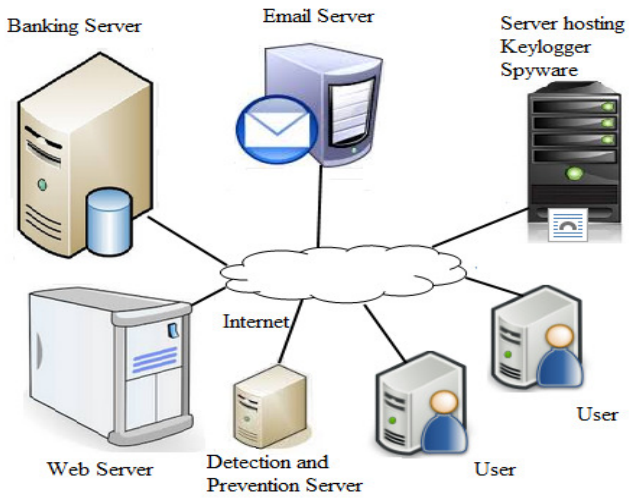

Fig 5: Monitoring System

The detection and prevention server should be designed in such a way that it captures all the traffic through the SMTP port of all the users in the network and creates a log file for each user as shown in Fig 6. This can be done by using a program which can be designed to run in background of the detection and prevention server . The log file (consider log.txt as log file of a particular user) will contain the details of all the mails sent from that particular system.

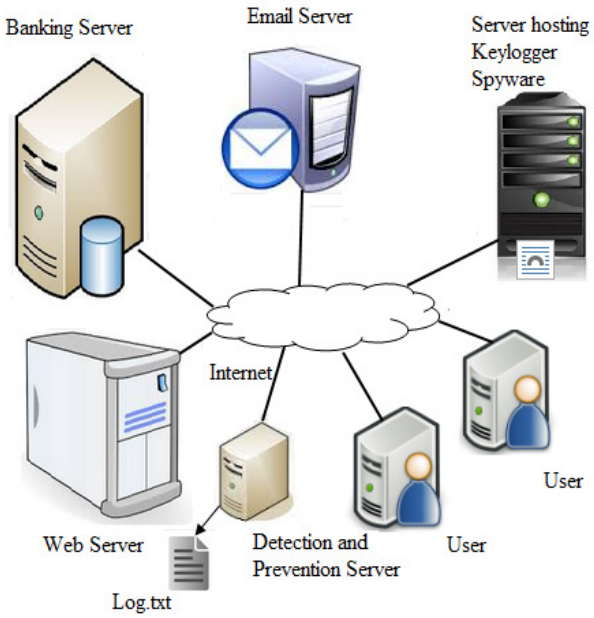

Fig 6: Log file generation by detection and prevention system

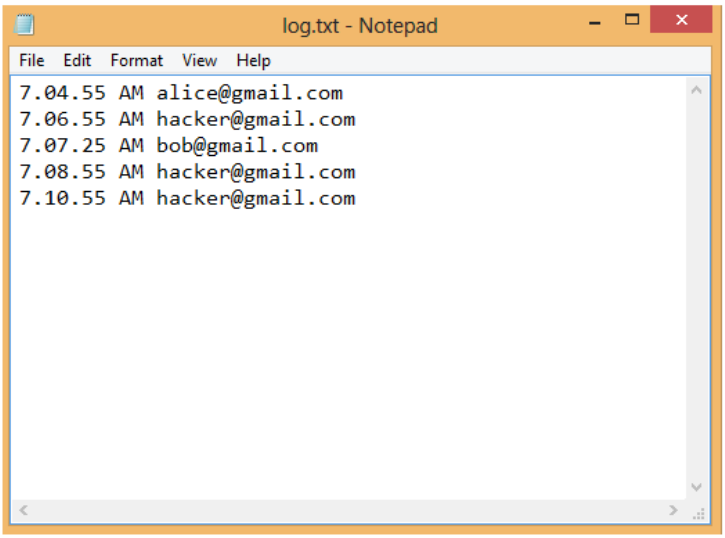

Fig 7: Log file generated for a user by detection and prevention server

Fig 7 shows log file generated by the detection and prevention server. Here, the email sent by user to alice@gmail.com is represented at 7.04.55 AM after which key logger spyware might sent its email to hacker@gmail.com in which it has attached the spy log file of that user. Thus they key logger spyware program will continue email sending process at regular interval.

The detection and prevention server inspects that log file to check for the presence of malicious program. It identifies a key logger spyware as soon as it finds the emails sent periodically to a particular mail id. In the above example we have email being sent to hacker@gmail.com which is done after evry 2 minutes. If the key logger spyware program is designed in such a way that it sends email to different users we can identify it by observing the behaviour of the emails being sent(for example time interval etc.).

After the presence of key logger spyware is detected, the prevention can be done. This can be done by blocking the emails being sent to the identified email id of the attacker. Further detailed analysis can be done in users system and remove the malicious program from the users system(Fig 8).

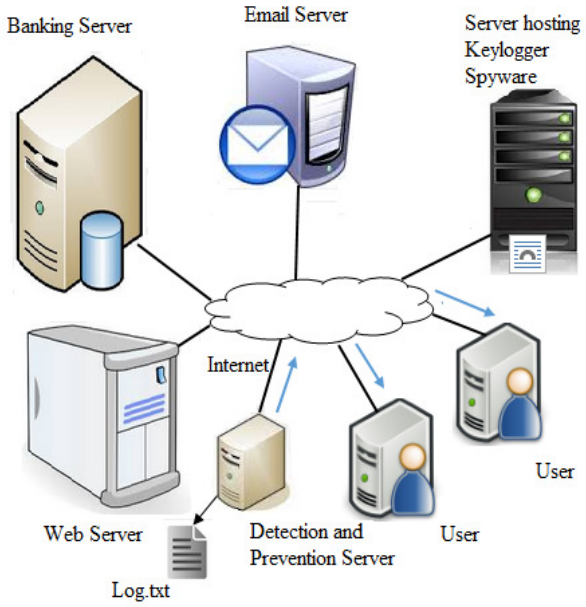

Fig 8: Removal of Keylogger Spyware

5. CONCLUSION

Malware attacks have become a threat many users. Key logger spywares can cause loss of highly confidential information. They are difficult to detect as they have the capability to hide themselves when they enter the system. Hence user cannot feel their presence. In the proposed method we have seen the key logger spyware attacking scenario and the detection and prevention of it in a network. This method can be effective in detecting this kinds of attacks.

REFERENCES

[1] 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).

[2] Jonathan A.P. Marpaung, Mangal Sain, Hoon-Jae Lee,"Survey on malware evasion techniques: state of the art and challenges", 14th IEEE International Conference on Advanced Communication Technology (ICACT), 2012.

[3] Sanjeev Kumar, Rakesh Sehgal, IS. Bhatia, "Hybrid Honeypot Framework for Malware Collection and analysis", 7th IEEE International Conference on Industrial and Information Systems (ICIIS), 2012.

[4] S. Murugan, K. Kuppusamy, "System and Methodology for Unknown Malware attack", 2nd IEEE International Conference on Sustainable Energy and Intelligent System (SEISCON 2011).

[5] Nur Rohman Rosyid, Masayuki Ohrui, Hiroaki Kikuchi, Pitikhate Sooraksat, Masato Terada, "A Discovery of Sequential Attack Patterns of Malware in Botnets", IEEE International Conference on Systems Man and Cybernetics. (SMC),2010.

[6] Mohamed Nassar, Radu State, Olivier Festor, "VoIP Malware: Attack Tool & Attack Scenarios", IEEE ICC 2009.

[7] Olivier Thonnard, Marc Dacier, "A framework for attack patterns' discovery in honeynet data", Elsevier Journal of Digital Investigation 5 (2008) SI28-S139.

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

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

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

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

[12] About spywares available at http://en.wikipedia.org/wiki/Spyware 18.

[13] Er.Abhijeet, Praveen Tripathi, Er.Anuja Priyam and Er.Vivek Kumar, "Implementation of Public Key Cryptography in Kerberos with Prevention of Security Attacks", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 248 - 253, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.