International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at :www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

Detection and Prevention of Attacks Due to Keylogger Spyware

Pushpa G

Senior Scale Lecturer, Department of Computer Science and Engineering, Government Polytechnic, Channasandra, Kadugodi, Bangalore, India

ARTICLEINFO

Article History:

Accepted: 10 Jan 2018

Published: 21 Feb 2018

Publication Issue :
Volume 4 Issue 1
Jan-Feb-2018

Page Number :
1854-1860

ABSTRACT

Cyber-attacks, particularly those involving malware, are becoming more sophisticated and frequent as the digital world becomes more integrated into our daily lives. This necessitates the development of novel defenses. One of the sneakiest kinds of assaults is key logger spyware, which combines key logging and spyware features. In order to gather sensitive information, including passwords and other personal data, this malicious program surreptitiously tracks and logs user keystrokes. This study presents a brand-new browser add-on made to successfully block key logger spyware assaults. A state-of-the-art algorithm that carefully examines input-related operations and quickly detects and flags any malicious activity serves as the foundation for the expansion. When an issue is detected, the plugin gives users the option to stop the questionable process right away or verify its legitimacy, giving them vital real-time control. The technique ensures the mobility and adaptability of the extension on a range of devices and platforms. The creation of the browser extension, from its first conceptual design to its thorough performance evaluation, is covered in great depth in this document. The findings demonstrate that the recommended modification significantly improves end users' defenses against online threats, making web browsing safer. Through thorough analysis and testing, the study validates the extension's effectiveness and noteworthy potential in strengthening online security standards, proving that it can make web browsing safer.

Keywords : Key logger Spyware, Keystrokes, Routes, Keystroke logging, Threat detection.

I. INTRODUCTION

The distinction between convenience and security is becoming more and hazier in today's digitalized society. We expose ourselves to possible weaknesses while we welcome the ease of digital note-taking, online purchases, and immediate communication. The key logger is one such hidden weakness. A key logger, often known as a keystroke logger, is an advanced

instrument that can be a specialized hardware device or software program [1]. Its main objective? To secretly capture each key that a user presses. This data can contain more typical information like written chats and search searches, as well as more sensitive information like passwords, bank account details, and personal identification numbers. Imagine writing a heartfelt email to a loved one, only to find out later that an unknown third-party application secretly recorded and preserved the whole communication. Consider the following scenario: a corporate executive accesses private firm financial data online, but a key logger allows the information to end up in the hands of a rival. Despite a great deal of research and commercial initiatives [2–5] to prevent key loggers, they continue to pose a serious danger to the theft of financial and personal information.

Key loggers can be used for lawful and legal purposes in some situations. Key loggers, for instance, may be used in business settings to track worker productivity or make sure that no private information is being improperly shared. They may be used by parents to monitor their kids' internet activity and protect them from any dangers. They may be used in investigations to keep an eye on suspects by law enforcement organizations with the proper warrants. But key loggers' negative aspects frequently outweigh their beneficial use. They are commonly used by cybercriminals to gather enormous volumes of data, including sensitive financial and personal data as well as login credentials. The illicitly obtained information may subsequently be utilized in targeted phishing attempts, sold on the dark web, or used for identity fraud. People, companies, and governmental organizations were among the many victims targeted by key logger assaults. Key loggers were used by attackers to obtain a variety of private data, such as Social Security numbers, bank account numbers, credit card numbers, and passwords.

T-PIM (Trusted Password Input Method), a revolutionary password protection system, is proposed in the publication [6-8]. The suggested T-PIM mechanism offers consumers a safe way to enter passwords that protects them from malware that steals data. In Paper [9], the authors provide a game theory-based model that predicts when and when Mac malware will appear based on a manageable amount of quantifiable characteristics. The authors of the publication [10] outline an analytical approach designed especially to obtain insights into honey net data. The process looks for clusters of network traces that share a variety of related characteristics inside an assault data set. They want to provide a versatile clustering tool for exploratory data analysis that can be used methodically to various feature vectors that describe the assaults. By examining a single component of the honey net data—the attack time series—they demonstrate how to apply their methodology. An alternate method of user authentication based on images that is immune to keylogger malware is provided in paper [11-12]. A hash function in cryptography that protects passwords. Users may recover their passwords from any place thanks to the suggested design's strong resistance to brute force assaults and vulnerability to dictionary attacks.

II. BRIEF STUDY OF MALWARE

Malware is currently one of the largest hazards on the Internet. It has the ability to take over a browser, reroute search queries, display intrusive pop-up advertisements, monitor websites visited, and generally cause problems. In addition to inflicting additional havoc, malware programs render the user's machine unresponsive and slow [13]. There are several methods that malware may infiltrate computers. It has the ability to package itself with other programs, such as iMesh and Kazaa [14]. Pop-up advertising are one type of malware software that is used to generate income. The majority of malware requires the user to install it. Malware has the ability to spread once it is installed, making removal extremely challenging.

A. MALWARE CLASSIFICATION

Adware, spyware, hijackers, toolbars, and dialers are some of the categories into which malware is divided [13].

1. Adware: These are employed for the aim of advertising. On a web page, adware is often shown as pop-ups. Pop-ups cannot be blocked by Internet Explorer's built-in pop-up stoppers. They could appear when you're playing an online game, listening to music online, etc. Usually, it displays an advertising that is relevant to the content being browsed or that may be associated with the webpage being seen.

2. Spyware: Spyware applications deliver private data to a designated system. Some spyware programs are tasked with delivering URL data, or they could transfer data you enter in Internet Explorer. The file names that you download. Some of them have the ability to search your hard drive and report the applications you have installed. They can even steal the contents of your email address book, which they will then sell to spammers. It is simple to steal any other valuable information about you, like your name, internet history, credit card numbers, login names and passwords, phone number, and address.

3. Hijackers: The hijackers take over the home page, search pages, and search bar, among other areas of the online browser. They can trick you into visiting a website by inputting the address incorrectly, which will stop you from seeing specific websites, such as those that fight malware. When someone tries to search, some of them reroute to their own search engine.

4. Toolbars: These are connected to Internet Explorer and include features like search forms and pop-up blockers. They mimic the appearance and features of genuine toolbars, such as those found on Google and Yahoo. They always share traits with other malware. This includes toolbars that are installed underhanded.

5. Dialler's: These are the applications that are mostly used to dial 1-900 numbers. As a result, the user's bill is high. Dialler's are inserted covertly and undetectable.

6. Key logger: Also known as a key logger or keystroke logger, this hardware or software tool tracks the keystrokes on the keyboard. Since it operates in the background and its details are not displayed in the task manager or control panel's list of active applications, its existence is undetectable. In the event that you entered into your online bank account, it may be utilized to get extremely private information, such as usernames and passwords [15].

Combining the previously mentioned malware kinds has made the malware assault scenario extremely successful. We have created an attack scenario for key logger spyware, which is a mix of a key logger and a spyware application, in this work. Every keystroke is recorded by the key logger script, which also creates a log file. The spy script then emails the log file to the designer's designated email account.

III. DESIGN AND IMPLEMENTATION

Hackers employ malware to breach a system's security, and when they do, it causes security specialists a lot of problems. Malware may take many different forms, such as rootkits, spyware, and key loggers, and we can even combine them to create a common application. We have presented a system in this research for identifying and preventing new key logger spyware assaults. Such unique assaults may be detected and defended against using the suggested architecture.

We have used the following technique for the suggested job.

A. Spyware Attack on Keyloggers

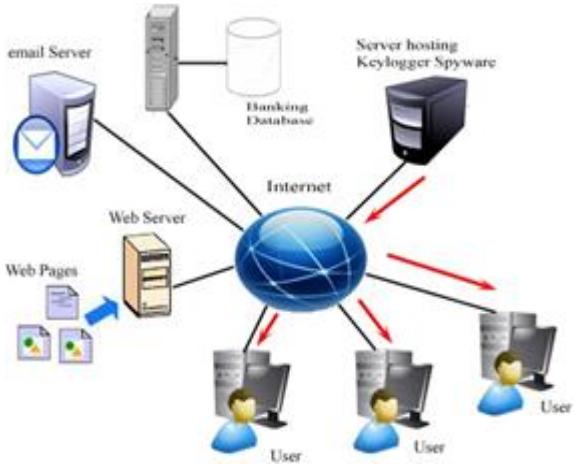

FIG. I: KEYLOGGER SPYWARE ATTACK ON USERS

As seen in Figure I, we have created an attacking scenario for a key logger spyware assault on a user's PC. As seen in Figure 1, there are three customers using the Internet to access a variety of services, such as email and online banking. Key logger malware, which infiltrates the system like application software (such as a mobile tracker), is hosted on a rogue server. The user will readily download and install mobile tracker, a dangerous software, without realizing it. As soon as it is installed, it begins recording each keystroke and creating a log file for each one.

The red colour arrows in Figure 1 show the entry of key logger spyware program into user's system.

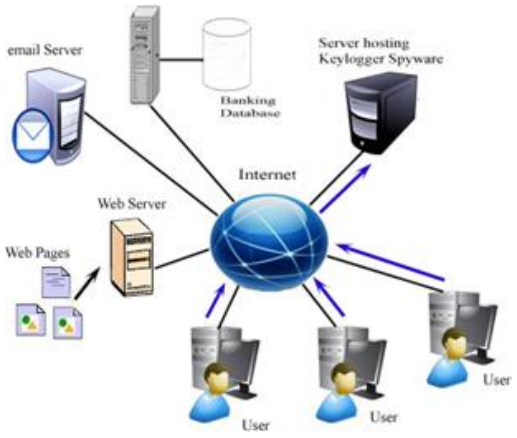

FIG. 2: TRANSFER (E-MAILING) OF CONFIDENTIAL INFORMATION FROM USER'S SYSTEM

The malware script's automated email operation is seen in Figure 2. In figure 2, it is depicted by blue arrows. The malicious program's operation is unknown to the end users. They are using their systems to log into their email and online banking accounts. Every keystroke users make while entering their credentials on the keyboard is recorded and saved in a log file (the spy log, as seen in figure 3). This will send more emails to the designated email address on a regular basis, such as every two minutes. If these credentials are used improperly, you risk losing all of your money in your bank account or having your email account compromised.

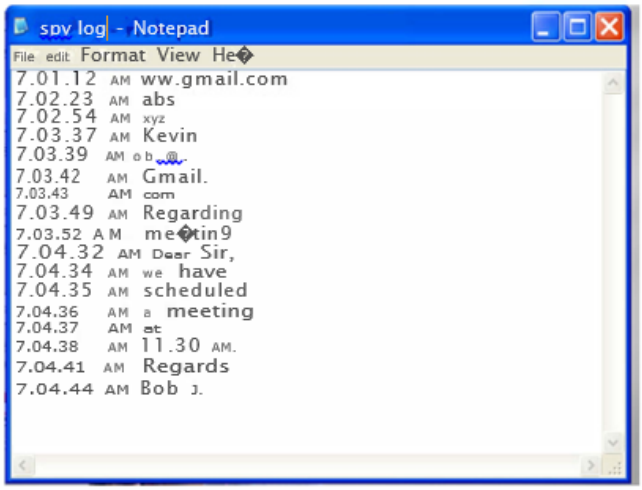

FIG. 3: GENERATED LOG FILE BY KEYLOGGER

The log file (spy log) produced by the key logger application is seen in Figure 3. This file contains all of the text that Bob J. typed. Where Bob J.'s email account credentials are abc and xyz.

B. Monitoring of Honeypot Bases

We have installed a honeypot on our client's network to detect such attempts. It is made in such a way that hackers cannot detect it and it is readily infiltrated. Key logger malware will infiltrate a honeypot system when it infiltrates a user's system. The honeypot system keeps an eye on this malware's activities. Additionally, a log file is created and sent to the

detection and prevention server. This file is examined for hazards at the detection prevention server.

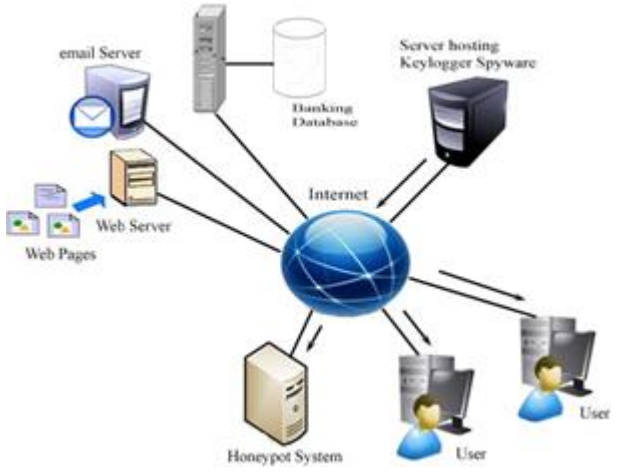

FIG. 4: HONEYPOT BASE MONITORING

Figure 4 shows key logger spyware monitoring process performed by honeypot system. The black arrows show the entry of key logger spyware into the user's system and honeypot system

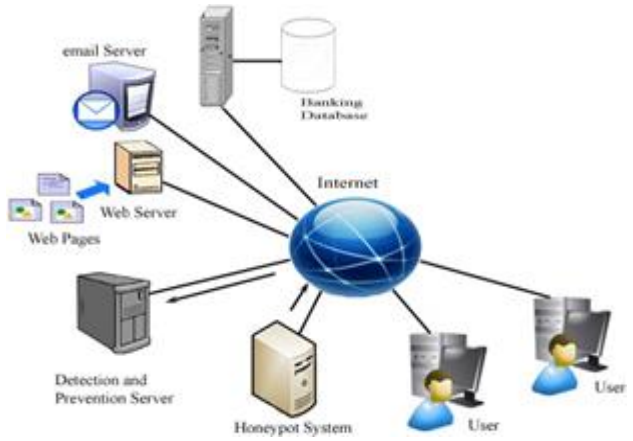

FIG. 5: TRANSFER OF ATTACK INFORMATION RELATED LOG FILE FROM HONEYPOT TO DETECTION PREVENTION SERVER

In monitoring process a log file is generated by honeypot system. In Figure 5, black arrow shows transfer of that log file from honeypot system to detection prevention server.

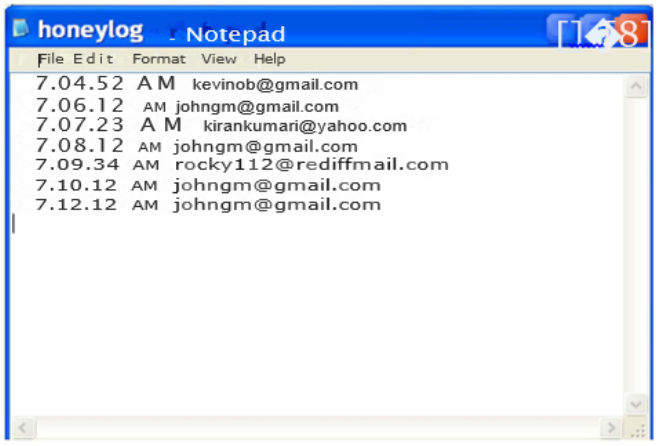

FIG. 6: GENERATED LOG FILE BY HONEYPOT

Figure 6 shows log file generated by honeypot system. An email sent byBob J. to kevinob@gmail.com is shown at7.04. 52 AM and after this email the keylogger spyware program sent its email to johngm@gmail.com (hacker's specified address) with that attached spylog file (having all information regarding email sent by Bob 1. to kevinob@gmail. com) at 7. 06.12 AM. Thus keylogger spyware program continues its email sending process (i. e. at 7.08. 12 AM etc)

IV.PROPOSED SYSTEM FOR KEYLOGGER SPYWARE DETECTION

To find dangerous programs, the detection and prevention system examines the log file (also known as the honeylog) that the honeypot sends. This keylogger malware works by sending information to a designated email address on a regular basis. The email address johngm@gmail.com, which is present in the log file seen in Figure 7, is where emails are delivered every two minutes. The inspection procedure traces it out. Following the identification of keylogger spyware, the prevention process begins, and with the assistance of a linked detection prevention server, we subsequently execute a removal program. The harmful malware will be eliminated from the user's PC.

FIG.7: REMOVAL PROCESS OF KEYLOGGER SPywARE PERFORMED BY DETECTION AND PREVENTION SERVER

Hackers often use malware to compromise system security. Malware can take various forms, such as keyloggers, spyware, and rootkits. Sometimes, these malicious programs combine, like a keylogger-spyware hybrid. In this paper, we propose a method to detect and prevent keylogger-spyware attacks. Our method aims to identify and defend against such threats effectively.

The keylogger spyware attack is illustrated in Fig 1. In the figure, three users are accessing various internet services such as online banking and email. A malicious user hosts a keylogger spyware that infiltrates the users' systems like any other application software. It may appear to be legitimate, leading the user to download and install it, unaware that it is actually malicious. Once installed, it begins capturing every keystroke and generates a log file containing all the keystrokes. The included spy script then emails this log file to a specified email address of the attacker.

The spyware remains hidden, making users unaware of its malicious activity. Users might log into online banking accounts, email accounts, and other services using their systems. As they type on the keyboard, the keystrokes are captured and stored in a log file. This log file is then periodically emailed to the malicious user. The log file may contain sensitive information, potentially leading to the user losing all their money from their banking account or having their email account easily hacked.

A snapshot shows an email sent to alice@gmail.com by a user whose system is infected with keylogger spyware. The entire message is captured by the keylogger and saved in the generated spy log file, as shown in Fig 3. The keylogger creates the spy log file, recording every keystroke made by the user. In this example, "aaa" and "abc" might be the credentials of the user's email account.

The detection and prevention server inspects the log file to check for the presence of malicious programs. It identifies keylogger spyware as soon as it detects emails being sent periodically to a specific email address. In the example above, emails are sent to hacker@gmail.com every 2 minutes. If the keylogger spyware is designed to send emails to different users, it can be identified by observing the behavior of the emails being sent, such as the time intervals between them.

Once the presence of keylogger spyware is detected, preventive measures can be taken. This includes blocking emails being sent to the identified attacker's email address. Additionally, a detailed analysis can be conducted on the user's system to remove the malicious program.

V. CONCLUSION

Malware attacks pose a significant threat to many users. Keylogger spyware can lead to the loss of highly confidential information. These programs are difficult to detect because they can hide themselves once they infiltrate a system, making their presence unnoticed by the user. In the proposed method, we have examined the keylogger spyware attack scenario and its detection and prevention within a network. This method can be effective in identifying and mitigating such attacks.

In this paper, we discussed keystroke logging, the characteristics of keyloggers, and the different types of keyloggers available. We also explored the various ways keyloggers spread. Finally, we analyzed how to detect keyloggers and discussed prevention techniques for keylogger spyware attacks that can steal credentials and confidential data from a victim's computer system. Our main aim is to raise awareness of existing threats, recognize them, and take countermeasures against them.

VI.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]. M. Wazid et al., "A framework for detection and prevention of novel keylogger spyware attacks," 2013 7th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2013, pp. 433-438, doi: 10.1109/ISCO.2013.6481194. keywords:

[9]. 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.

[10]. 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.

[11]. M.N. Doja, Naveen Kumar, Image Authentication Schemes against Key-Logger Spyware, 9th ACM ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2008 (SNPD '08).

[12]. 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.