ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

RECORD THE KEYSTROKES MADE BY USER USING KEYLOGGERS TO MONITOR THE SYSTEMS

Mrs. K. Vijayalakshmi M.E., Ph. D. HoD/CSE

Mr.P Vijay, Mr.A Sankar, Mr. A Jana, Mr. P RehithKumar(UG Students)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AVS College Of Technology,

Salem-636 106,

Tamil Nadu, India.

(e-mail: vijayperumal2020@gmail.com, asankarsmart@gmail.com)

Abstract-- Key loggers are a very popular tool often used in collecting sensitive information.The rapid growth of keyboard radio is the ability of programs running in the user's space to monitor all the keystrokes the user types.

It's a type of rootkit malware that attempts to retrieve sensitive information by secretly capturing user input by monitoring keystrokes and then sends that information to others, often for malicious purposes, and intercepts sensitive information such as usernames, PINs, and passwords.

key logger poses a huge threat to both business and personal activities such as online transactions, online banking, email or chatting.

To deal with these types of threats, not only users need to be aware of this type of malware, but software professionals and students as well.

Our proposed system provides an overview of key logger programs,discusses key logger design, implementation, and usage.

Keywords– cyber Security, Keylogger ,Malware , Key Stokes ,Honeypot Base Monitoring.

1.INTRODUCTION

Malware steals information from a computer or can cause damage. Type includes key logger, 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.

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. In its quarterly "Threats Report," Intel subsidiary McAfee quoted that it had found more than 8 million new kinds of malware in the second quarter 2012.

2.INTRODUCTIONOF MALWARE

These days one of the biggest threats on Internet is mal ware. It can hijack the browser, redirect search attempts, serve up nasty pop-up ads, track the web sites visited, and generally screw things up. Malware programs make the computer slow and unstable which is unbearable to the user along with causing other wrecks Malware can infect computers in many a ways. It can bundle itself with other programs like Kazaa. Some malware programs like pop-up ads are used for earning revenue from the ads. Majority of malware needs to get installed by the user.

It is very difficult to get rid of mal ware because they have the tendency to multiply once they get installed. The paper includes a survey on the different techniques used in mal ware to evade detection by security systems. The discussed evasion techniques are obfuscation, fragmentation and session splicing, application specific violations, protocol violations, inserting traffic at IDS, DoS etc. Some mitigations such as sandboxing, session reassembly, data execution prevention, address space layout randomization, control flow integrity etc. are also discussed.

The paper provides an integrated framework of malware collection and analysis using both of the technologies called server honeypots and client honeypots. The main objective was to do the analysis of collected malwares from honeypots. Authors in paper propose an Intelligent Intrusion Detection System, based on specific AI approach for unknown malware attacks. The techniques that are being investigated includes neural networks and fuzzy logic with network profiling, that uses simple data mining techniques to process the network data.

A hybrid system is introduced that combines anomaly, misuse and host based detection. An attack classification method is proposed for computer network security. The attacks are classified depending on vulnerability i.e. attack propagation skills and attack intentions. The classification results are arranged as per attack propagation skills and attack intentions.

3.KEYLOGGER

Keylogger is basically using keystroke logs to monitor the system and send the details to the admin through the mail server. Keyloggers provide the best solutions in case of such cases like; IT organizations can indicate their concerns by going after the culprit whose performance is deteriorating that of the whole organization, parents can maintain a check on their children's activities, a particular person's activities can bemonitored, storing passwords of various social media profiles.

Hackers and other third parties are always looking for the vulnerabilities present inside the system. To gain

knowledge about what they require from the organizations, they either gain access to the confidential data stored in the system and either cause harm to the integrity of data or may cause data loss. Another problem is that cyber crimes are increasing day by day.

If we will have the chat logs or keystroke logs of victim's laptop then we can easily analyse the entire planning of the victim which will provide the best solution to eradicate or solve the problem.

4.EXISTING METHOD

In existing system using key loggers only monitor the key strokes and not monitored by virtual key strokes.

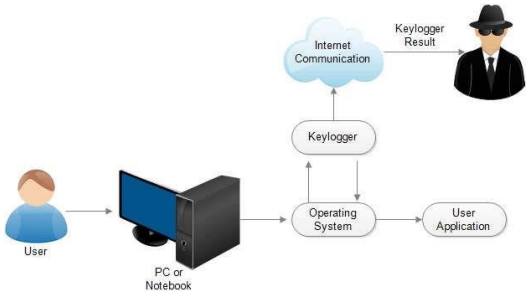

Fig.1.Diagram of Existing system

5.PROPOSED METHOD

In proposed system we added some futures like screenshot gathering system information and collecting clipboard information.

It helps to improve monitoring system in organization. is a type of surveillance technology used to monitor and record each keystroke on a specific computer. Keylogger software is also available for use on smartphones, such as the Windows and Android devices.

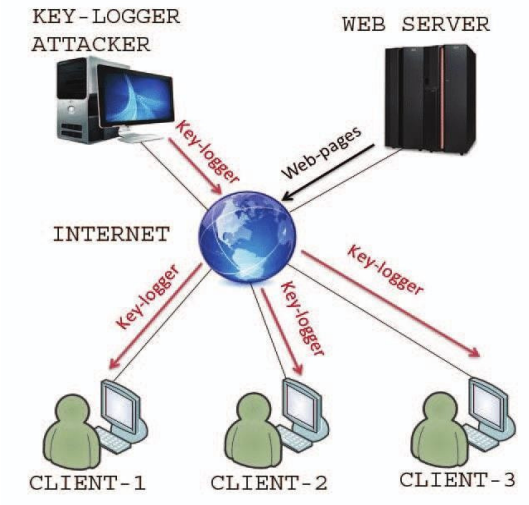

Fig.2.Diagram of Proposed system

6.KEYLOGGER MODULE

6.1.Smtplip Module

The module included in python defines an SMTP client session object that can be used to send mail to any internet machine with an SMTP listener daemon. SMTP define as (Simple Mail Transfer Protocol).

6.2.Threading Module

It is one of the modules provided with python includes a simple-to-implement locking mechanism that allows you to synchronize threads.

6.3.Python Input Module

This library allows the users to control and monitor input devices. e.g.;Python Input mouse, python Input keyboard. [2] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. [4] discussed that the activity related status data will be communicated consistently and shared among drivers through VANETs keeping in mind the end goal to enhance driving security and solace. Along these lines, Vehicular specially appointed systems (VANETs) require safeguarding and secure information correspondences.

7.CONCLUSION

In this paper, a new method approach for Monitoring The System keylogger Based. The proposed system demonstrates that the Monitoring the system has a high level of accuracy. This research described a system that is developed by using keylogger.

8.ACKNOWLEDGEMENT

The authors would like extend sincere Thanks to AVS College ofTechnology and Department of Computer ScienceEngineeringfor supporting both by knowledge and wealth. We also wish to thank our collaborators who stand always with us.

9.REFERENCES

[1] Yeboah-Ofori et al., "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," in IEEE Access, vol. 9, pp. 94318-94337, 2021, doi:10.1109/ACCESS.2021.3087109.

[2] Christo Ananth, M.Danya Priyadharshini, “A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks”, International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254).

[3] O. Mendsaikhan, H. Hasegawa, Y. Yamaguchi and H. Shimada, "Quantifying the Significance and Relevance of Cyber-Security Text Through Textual Similarity and Cyber-Security Knowledge Graph," in IEEE Access, vol. 8, pp. 177041-17.

[4] Christo Ananth, Dr.S. Selvakani, K. Vasumathi, “An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing”, Journal of Advanced Research in Dynamical and Control Systems, 15-Special Issue, December 2017,pp: 787-792