JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

MALWARE & SPYWARE ANALYSIS USING IMPLANTATION AND PREVENTION OF NOVEL KEYLOGGER

[1]Pradip Sable, [2]Kalpesh Nagare, [3]Chetan Sonawane, [4] Dr. Vivek N Waghmare

[1]B.E Scholar, [2]B.E Scholar, [3]B.E Scholar
[123]Information Technology
Sandip institute of Technology And Research Center, Nashik, India

Abstract :
The goal of this project is to detect the presence of keyloggers in the system and alert the user. Keystroke logging is the action of recording (logging) the keys pressed on the keyboard, usually hidden so that the person using the keyboard is unaware that his actions are being monitored. increase. The data can be obtained by the operator of the logging program. Keyloggers are either software or hardware. Keyloggers are most commonly used to steal passwords and other sensitive information. Focus on software-based keyloggers. The software keylogger works by setting up a Windows hook that tells the keylogger which keys are pressed, where the mouse is moved, and where the mouse is clicked, whenever the user presses a key or uses the mouse. To do. A software keylogger is created and implemented to simulate the attack, and a system to detect the keylogger is also created. We used Wireshark platform which is vastly popular for network monitoring and it is free & friendly to use. We ran Wireshark in host computer for 1hr without sending any email and type word or sentence with pressing the Backspace or Delete key in that computer and remember what was typed. We checked all the packets that has been generated within this 1hr through filtering HTTP or SMTP packets.

Keywords: Keylogger, HTTP, Wireshark, SMTP

I.INTRODUCTION

Keystroke logging, often referred to as **key-logging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A **key-logger** can be either software or hardware.

While the programs themselves are legal, with many of them being designed to allow employers to oversee the use of their computers, key-loggers are most often used for the purpose of stealing passwords and other confidential information.

Key-logging can also be used to study human–computer interaction. Numerous key-logging methods exist: they range from hardware and software-based approaches to acoustic analysis. These are computer programs designed to work on the target computer's software. Key-loggers are used in IT organisations to troubleshoot technical problems with computers and business networks. Families and business people use key-loggers legally to monitor network usage without their users' direct knowledge. Even Microsoft publicly admitted that Windows 10 operation system has a built-in key-logger in its final version –to improve typing and writing services‖. However, malicious individuals can use key-loggers on public computers to steal passwords or credit card information. Most key-loggers are not stopped by HTTPS encryption because that only protects data in transit between computers, thus the threat being from the user's computer.

II.OBJECTIVE:

1) The purpose of this framework is to keep tracks on every key that is typed through the keyboard and send it to the admin through the mail server in the time set or given.
2) Detecting the exiting key logger in the system.
3) Preventing system from further malware/spyware attack such as keylogger by analysing using wireshark

III.PROPOSED SYSTEM:

We have design an attacking scenario for key-logger spyware attack on user's system as shown in Figure (1). There are 3 users as shown in Figure (1) they are accessing various services via Internet i. e. online banking, email etc. There is a malicious server hosting key-logger spyware,
this program enters into the system like application software (i.e. mobile tracker).

User is not aware of it he will easily download and install mobile tracker which is a malicious program. When it installs it starts capturing every keystroke and generate log file corresponding to each and every keystrokes. The included spy script email this log file to the specified email address of the designer.

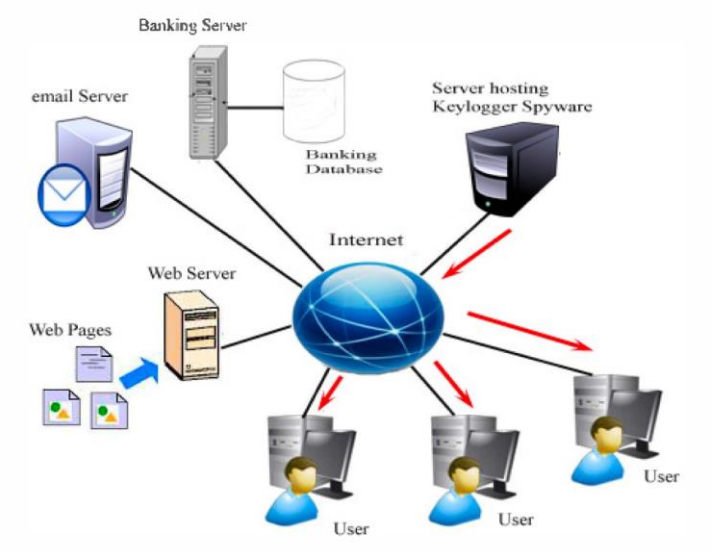

Figure 1: Key-logger spyware attack on user

The red coloured arrow in figure (1) shows the entry of key-logger spyware program intouser system.
Figure (2) shows automatic email process performed by the spyware script. It is shown by blue colored arrows in figure (2). The end users are not aware of the functioning of the malicious program. They are login into their online banking account, email account through their systems. When they type their credentials using keyboard every keystroke is captured and stores into log file (i.e. spy-log shown in figure (3)).
This will further email to the specified email address periodically i.e. after every 2 minutes. Where these credentials can be misused you can lose your entire money from your banking account or your email account can be easily hacked.

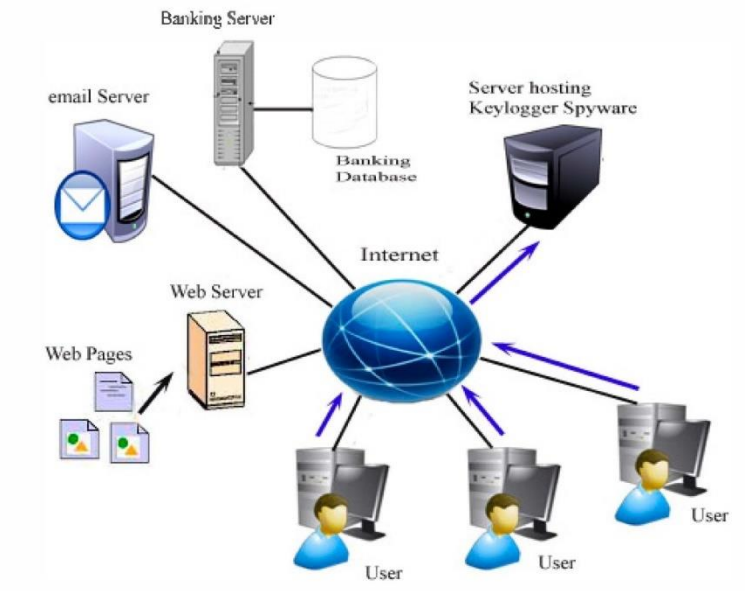

Figure 2: Transfer emailing of confidential information from user's system

Keylogger Detection using Memory Forensic and Network Monitoring

Memory Forensic

Memory Forensic, usually referred as memory analysis, is a process to analyze or deep digging in volatile memory of any system [9]. It allows investigator to search for suspicious malware in any computer or server. Since there exist some kind of malware that, they can hide themselves in such a way, they are completely untraceable. And also they could be the reason of compromised OS. Memory forensics are in highly demanded in this kind of situation. With this approach so many information could be retrieved through memory dump which is

1..All the running process information

2.All executable file info with their history

3.Network scanning (Packet, port, traffic)

4.User logging info

5.File data and their creation information

Advance level malware use modification of OS kernel for being undetected. For this reason, they have to use rootkits. There are two types of rootkits one is user level and another one is kernel mode rootkits. User level rootkits use modification of system libraries. In other cases, rootkits implement windows hooking, which is referring to execution in kernel internals. Through hooking mechanism access of API is possible, which should be permitted from user level [11]. With this process newly developed malware and eavesdropping viruses are making itself undetectable. They have to use volatile memory for their execution inside the system. Memory forensic is a very strong platform to identify this kind of suspicious object with a very deep searching

Network Monitoring

We used Wireshark platform which is vastly popular for network monitoring and it is free & friendly to use. We ran Wireshark in host computer for 1hr without sending any email and type word or sentence with pressing the Backspace or Delete key in that computer and remember what was typed. We checked all the packets that has been generated within this 1hr through filtering HTTP or SMTP packets.

We had to look all the HTTP packets if there is an attached file in the packet. Then we know that there is some process who is sending files to hacker.

Now what if we didn't get any HTTP packets with file attached but we got SMTP packets. SMTP packets is used by mailing agent to send an auto generated e-mail. Gmail use SMTP to send e-mail from a computer to its server.

When packet is generated it uses SSL/TLS encryption. Without this encryption google will not accept any e-mail. This packet has to go to Port 587 and outgoing mail server is: smtp.gmail.com

If we want to look at these packets we can't see anything because it's encrypted. But we know that we did not used SMTP to email anyone. We use Browsers to mail which use HTTP packet. Finding a SMTP packet while running traffic monitoring software create suspicion about having malicious mailing agent in host PC.

IV.CONCLUSION:

Using the above methodologies, we have successfully enabled a keystroke logger that keeps a log book of the key strokes of the user running a windows platform. The program is loaded on the machine and it runs 24x7 as a background process and keeps on running until the user uses task manager to end the program.
For detection and prevention purpose we place a detection prevention server which will automatically remove that key logger spyware program from the system when it is detected. This especially designed framework is very effective for these kinds of attacks.
Real time network monitoring can create an option to identify the running malicious process faster. If we can identify the culprit process earlier then we can work on removal. Still there is no valid process for removal of keylogger, many researchers have proposed detection mechanism but at the end the only solution is to format the syste

V.REFERENCES:

[1] "Keyloggers in Cyber security Education" Christopher A. Wood (Raj Department of Software Engineering, Rochester Institute of Technology, Rochester, New York, USA) and Rajendra K. (Department of Computer Science, Rochester Institute of Technology, Rochester, New York, USA)

[2] "A Framework for Detection and Prevention of Novel Keylogger Spyware Attacks" Mohammad Wazid, Avita Katal , R.H. Goudar, D.P. Singh and Asit Tyagi (Department of CSE, Graphic Era University, Dehradun, India) Robin Sharma and Priyanka Bhakuni (Department of IT, Graphic Era University, Dehradun, India)

[3] "Keylogger Is A Hacking Technique That Allows Threatening Information On Mobile Banking User" Adam Prayogo Kuncoro(Department of Informatics Engineering STMIK Amikom Purwokerto) , Bagus Adhi Kusuma(Department of Informatics Engineering STMIK Amikom Purwokerto)

[4] "Keyloggers Software Detecation Techniques" A.Solairaj , S.C.Prabanand , J.Mathalairaj , C.Prathap and L.S.Vignesh Assistant Professor (Nadar Saraswathi College of Engineering and Technology)

[5] "System Monitoring and Security Using Keylogger" Preeti Tuli (Reader, Department Of Computer Science Dimat, CSVTU, Raipur, Chhattisgarh, India), Priyanka Sahu (Tech scholar, Department Of Computer Science Dimat, CSVTU, Raipur, Chhattisgarh, India).

[6] "Mobile Keylogger Detection Using Machine Learning Technique" S.Gunalakshmii (LpG Scholar, Department ojComputer Science and Engineering) P.Ezlunnalai (2Projessor and Head, Department ojComputer Science and Engineering RlvlD Engineering College, Anna University, Kavaraipettai, Chennai)

[7] "Detecting Software Keyloggers with Dendritic Cell Algorithm" Jun Fu (Computer School Wuhan University Wuhan, China) Yiwen Liang (Computer School Wuhan University Wuhan, China) Chengyu Tan (Computer School Wuhan University Wuhan, China) Xiaofei Xiong (Computer School Wuhan University Wuhan, China)

[8] "Keyboard or Keylogger?: a security analysis of third-party keyboards on Android" Junsung Cho (Department of Computer Science and Engineering Sungkyunkwan University, Republic of Korea) Geumhwan Cho (Department of Computer Science and Engineering Sungkyunkwan University, Republic of Korea) Hyoungshick Kim (Department of Computer Science and Engineering Sungkyunkwan University, Republic of Korea)

[9] "Unprivileged Black-box Detection of User-space Keyloggers" Stefano Ortolani (MSc in Computer Science from the Ca' Foscari University, Venice, Italy) Cristiano Giuffrida (MEng in Computer Engineering from the University of Rome "Tor Vergata", Italy) Bruno Crispo (graphy, and security protocols. Crispo received a PhD in computer science from the University of Cambridge, United Kingdom. He is a senior member of the IEEE)

[10] "Virtual Machine Introspection for Anomaly-Based Keylogger Detection" Huseyn Huseynov , Kenichi Kourai , Tarek Saadawi and Obinna Igbe (Department of Electrical Engineering City University of New York, City College, New York, United States)

[11] "Keylogger for Windows using Python" Santripti Bhujel (Student, Master of Computer Application, Jain (Deemeed-to-be University), Bangalore, Karnataka, India) Mrs. N. Priya (Assistant Professor,Master of Computer Application, Jain (Deemeed-to-be University), Bangalore, Karnataka, India)

[12] "Bridging the Semantic Gap to Mitigate Kernel-level Keyloggers" Jesus Navarro(Computer Science Department Bowdoin College, Brunswick ME USA) Enrique Naudon(Computer Science Department Bowdoin College, Brunswick ME USA) Daniela Oliveira Computer Science Department Bowdoin College, Brunswick ME USA {jnavarro, enaudon, doliveir}@bowdoin.edu

[13] "Circumventing Keyloggers and Screendumps" Karan Sapra(Electrical and Computer Engineering, Clemson University, Clemson, SC USA), Benafsh Husain(Electrical and Computer Engineering, Clemson University, Clemson, SC USA) Richard Brooks(Electrical and Computer Engineering, Clemson University, Clemson, SC USA) and Melissa Smith(Electrical and Computer Engineering, Clemson University, Clemson, SC USA)

[14] "Integration of Kleptoware as Keyboard Keylogger for Input Recorder Using Teensy USB Development Board" Surya Michrandi Nasution(Electrical Engineering Faculty Telkom University Bandung, Indonesia) Yudha Purwanto(Electrical Engineering Faculty Telkom University Bandung, Indonesia) Agus Virgono(Electrical Engineering Faculty Telkom University Bandung, Indonesia) Girindra Chandra Alam(Electrical Engineering Faculty Telkom University Bandung, Indonesia)

[15] "Keylogger Detection using Memory Forensic and Network Monitoring" Md Bayzid Ahmed(Computer Science & Engineering East West University Dhaka, Bangladesh)Mohiuddin Shoikot(Computer Science & Engineering East West University Dhaka, Bangladesh) Jafrul Hossain(Computer Science & Engineering East West University Dhaka, Bangladesh) Anisur Rahman(Computer Science & Engineering East West University Dhaka, Bangladesh)

[16] "Random Multiple Layouts Keylogger Prevention Technique" Tasabeeh O. M. Ali tasabeeh_osama@outlook.com(University of Khartoum Khartoum - Sudan) Omer S. A. Awadelseed 11omermail@gmail.com(University of Khartoum Khartoum - Sudan) Abeer E. W. Eldewahi abeer.eldewahi@uofk.com (University of Khartoum Khartoum - Sudan)

[17] "Infringement of Prevention Technique against Keyloggers using Sift Attack" Arun Pratap Singh (Computer Science & Engineering The Right Click Services Pvt. Ltd. Bhopal, Madhya Pradesh, India) singhprataparun@gmail.com, Vaishali Singh (Electronics & Communication The Right Click Services Pvt. Ltd. Bhopal, Madhya Pradesh, India) vaishali.ec0709@gmail.com