iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41509

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Windows Post Exploitation [MSF] Keylogger for Security

Mr. Chandra Kant Bauri[1], Mr. Chetan Indulkar[2], Mr. Shantanu Jadhav[3], Prof. Anjali S. Khandagale[4]
[1, 2, 3]*Student, Department of Information Technology, AISSMS's Polytechnic, Pune, Maharashtra, India*
[4]*Lecturer, Department of Information Technology, AISSMS's Polytechnic, Pune, Maharashtra, India*

Abstract: ***Keyloggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Some keyloggers can also capture your screen at random intervals; these are known as screen recorders. Keylogger software typically stores your keystrokes in a small file, which is either accessed later or automatically emailed to the person monitoring your actions. You'll find the use of keyloggers in everything from Microsoft products to your own employer's computers and servers. In some cases, your spouse may have put a keylogger on your phone or laptop to confirm their suspicions of infidelity. Worse cases have shown criminals to implant legitimate websites, apps, and even USB drives with keylogger malware. Whether for malicious intent or legitimate uses, you should be aware of how keyloggers are affecting you. First, we'll further define keystroke logging before diving into how keyloggers work.***
Keywords: Keylogger, Reverse Shell, Post-Exploitation, Metasploit, Netcat, Intranet, privilege escalation.

I. INTRODUCTION

A keylogger is a device that captures every detail of your computer or smartphone screen every time you press a key on your keyboard or swipe on your touchscreen device. Keyloggers work by listening to you typing and recording everything into files that can later be accessed remotely over the Internet. One way they are used by business owners is to monitor productivity so they know if employees are doing their job correctly or not. There are many varieties of keyloggers available out there with varying price tags. Some keyloggers are small enough to be hidden somewhere on your person or built into your desk to secretly capture all the details of your typing and swiping. Some keyloggers are installed on USB flash drives and can be removed at any time without showing the presence of a USB drive in your computer.

Types of Keylogger

1) *Hardware Keylogger:* Hardware Keyloggers are small electronic devices used for capturing the data in between a keyboard device and I/O port. Usually, these devices have built-in memory where they store the keystrokes so this means they must be retrieved by the person who installed it to obtain the information. Hardware Keyloggers are undetectable by anti-viral software or scanners since it works on the hardware platform. Hardware Keylogger is much stronger than Software Keylogger but it has portability issues.
2) *Software Keylogger:* Keyloggers are activity-monitoring software programs that give hackers access to your data. Software keyloggers install on the computer when the user downloads an infected application. Once installed, it monitors the paths of the operating system that the keys you press on the keyboard have to go through. That's how software keyloggers track and record keystrokes.

Then it transmits the information to the hacker via a remote server.

II. PROBLEM STATEMENT

Stealing user confidential data serves many illegal purposes, such as identify theft, banking, and credit card frauds, software, and services theft just to name a few. This is achieved by keylogging, which is the eavesdropping, harvesting, and leakage of user-issued keystrokes. Key loggers are easy to implement and deploy. When deployed for fraud purposes as part of more elaborated criminal heists, the financial loss can be considerable. Table 1.1 shows some major keylogger-based incidents as reported. To address the general problem of malicious software, several models and techniques have been proposed over the years. However, when applied to the specific problem of detecting key loggers, all existing solutions are unsatisfactory. Signature-based solutions have limited applicability since they can easily be evaded and also require isolating and extracting a valid signature before being able to detect a new threat. As we show in the next phase, the implementation of a key logger hardly poses any challenge.

Even inexperienced programmers can easily develop new variants of existing key loggers, and thus make a previously valid signature ineffective. To design and implement an exe application that works with Windows operating system to capture keystrokes. The work also addresses the issue of malware handling in Cybersecurity.

III. ACTUAL METHODOLOGY

A A keylogger is a form of malware or hardware that keeps track of and records your keystrokes as you type. It takes the information and sends it to a hacker using a command-and-control (C&C) server. The hacker then analyses the keystrokes to locate usernames and passwords and uses them to hack into otherwise secure systems.

A. Requirements Used

1) Two machines:

a) Victim machine [Windows 7/8]

b) Attacker machine [Debian OS]

2) Tools required: Metasploit, Netcat

3) Software: VMware pro Workstation/Fusion

4) IDE: Visual Studio Code

The idea of the keylogger is to monitor/keep track of a mass number of people like MNC's employees, organizations, Terrorist groups or to track Suspicious targets It can also be used as parental control to monitor children's activity, to stop any cyber incidents. This proposed research work is to implement the proposed approach with multiple VMs. Also, we plan to explore the implications of keyloggers on computers from any malicious websites. In our proposed system we use to create an exe malware, to track the target's keystroke on the computer. The reverse shell will be used to interact with the victim's computer and activate the keylogger. A Reverse shell is a shell session established on a connection that is initiated from a remote machine. Embedding Keylogger and Reverse Shell into .exe file using Metasploit tool. Transfer of exe file to the target through online/offline medium. When Victim will run the exe file from his/her computer then a reverse shell session will be created on a particular port no. to the attacker's computer without interfering with his/her firewall. After getting the reverse shell from the victim, We will initiate the keylogger script. Then every keystroke will be recorded on the victim's Pc. Finally, we will dump the keystrokes data. The data we dumped is received from the victim's to the attacker's computer.

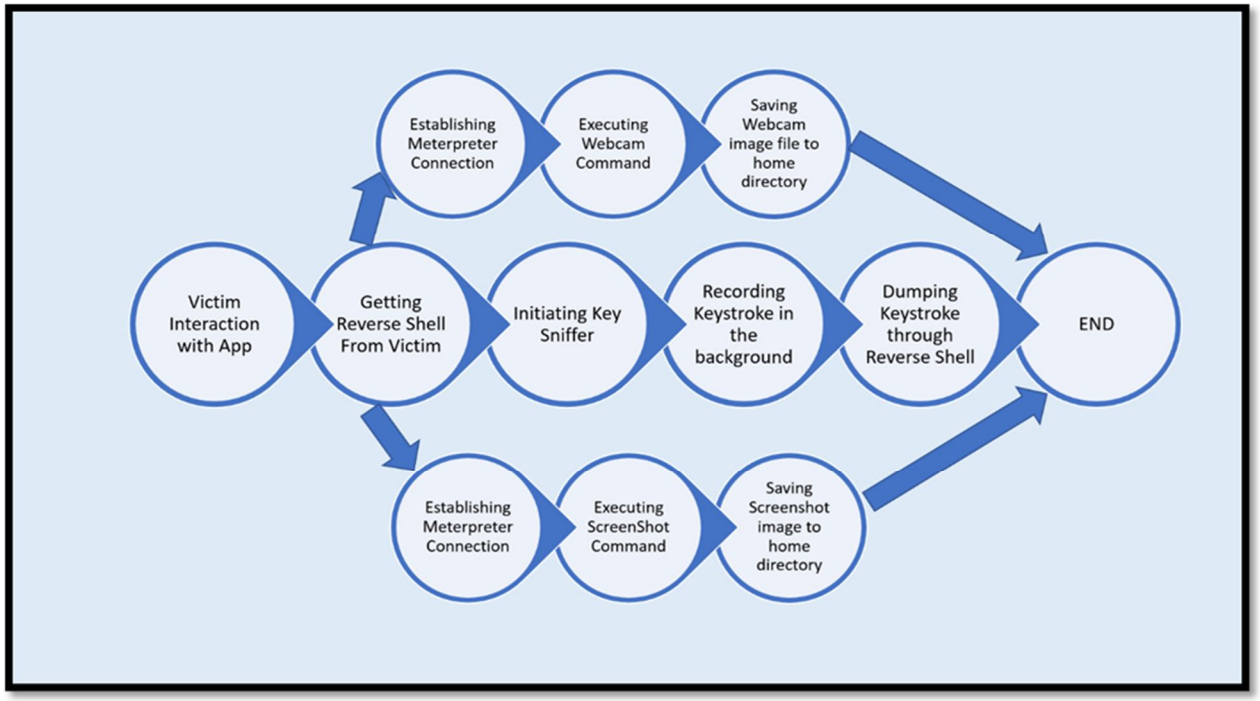


Fig. 3.1. The architecture of the Keylogger

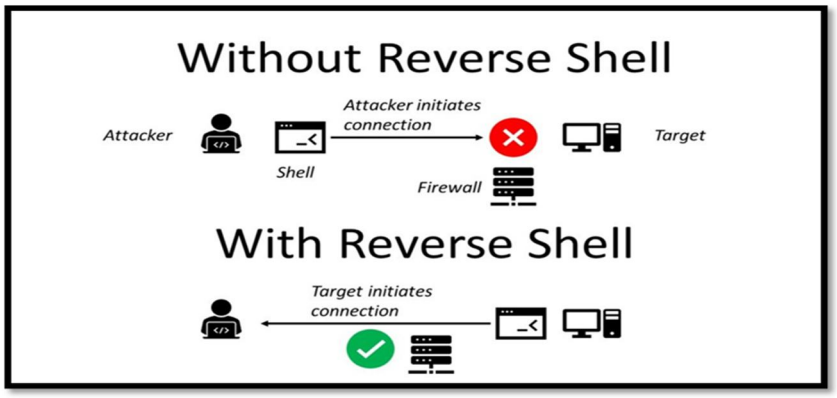


Fig. 3.2. Reverse Shell

IV. RESULT

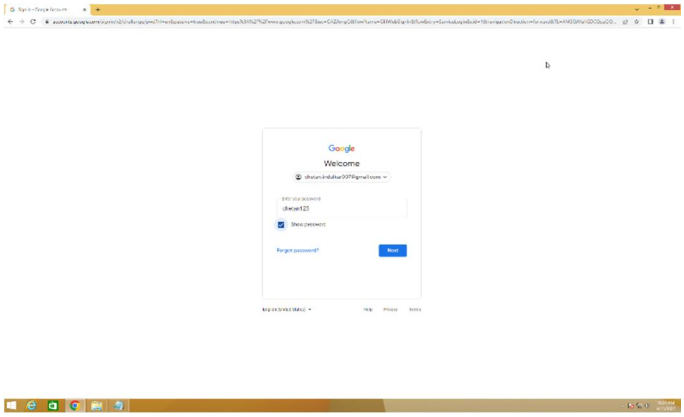
A. *Recording Keystrokes*

Attacker Screen

```
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
chetan.indulkar007<Shift>@gmail.comchetan123

meterpreter >
```

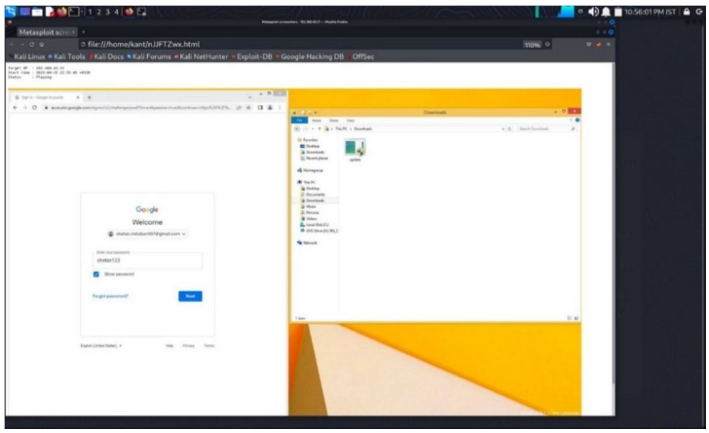
Victim Screen



In this function, the victim is trying to log in to his Google account without knowing that someone is recording his keystrokes. In attackers or authorized user's machines, as you can see the victim used his Email ID and password for login verification detail are visible to the attacker.

B. *Screen Streaming*

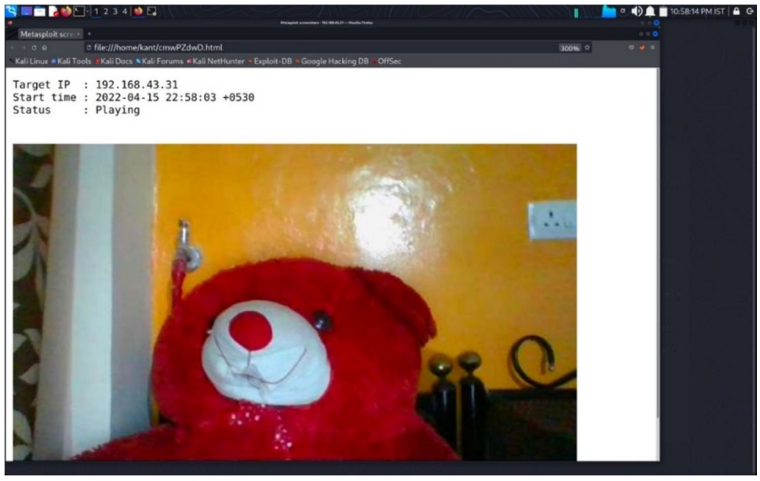
Attacker Screen



In this function, the attacker has initiated a screen-sharing module. Whatever victim performs a certain task will be monitored by an attacker or any authorized person.

C. Webcam Shot and Live Stream

Attacker Screen

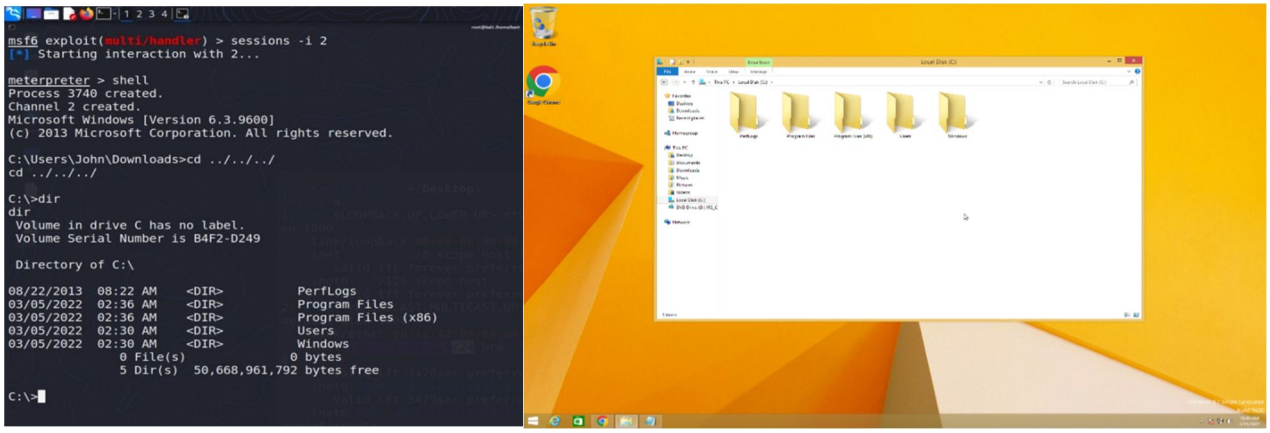


In this function, the attacker has initiated Webcam sharing and recorded webcam shots as well as a live stream of the webcam. He/She will be monitored without knowing that they are monitored.

D. File Access

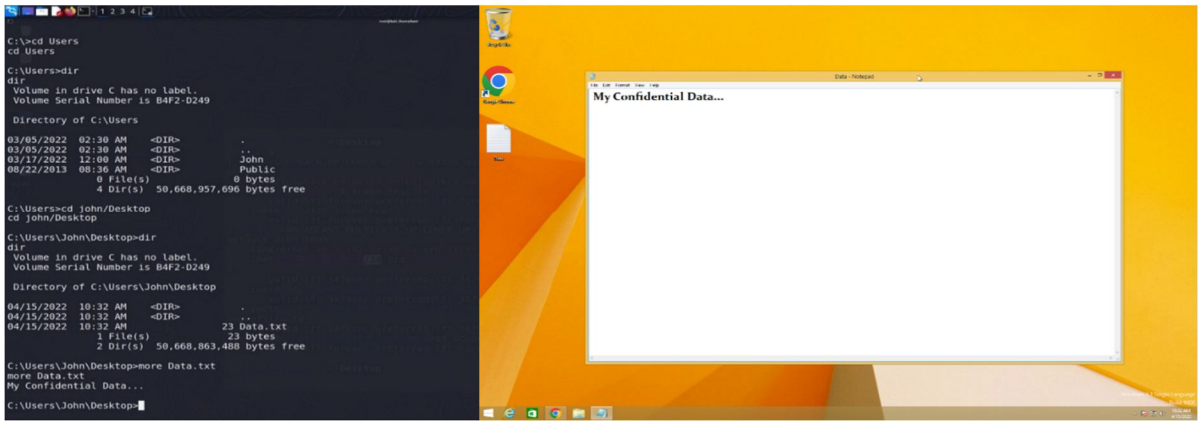
Attacker Screen

Victim Screen



Attacker Screen

Victim Screen



Here, we can access the file structure of the target machine without knowing he/she that someone can have access of your file structure or system.

V. CONCLUSION

Keylogger devices, both hardware, and software, with the evolution of technology and the pervasive spread of the computer in any private or industrial environment, represent a severe threat of cyber interception. Moreover, due to the ease with which they can be there and purchased via the Internet and at reasonable prices. The keylogger is a malicious program challenging to find and capable of reading and finding out anything present on the keyboard. Therefore, this survey paper is a complete guide that you must know about the keylogger software. Understanding if a keylogger is present on your device is not always easy. As far as hardware keyloggers are concerned, the only way to identify them is to check the keyboard, also internally, and the cables connected to it. Once you have found the device, remove it physically.

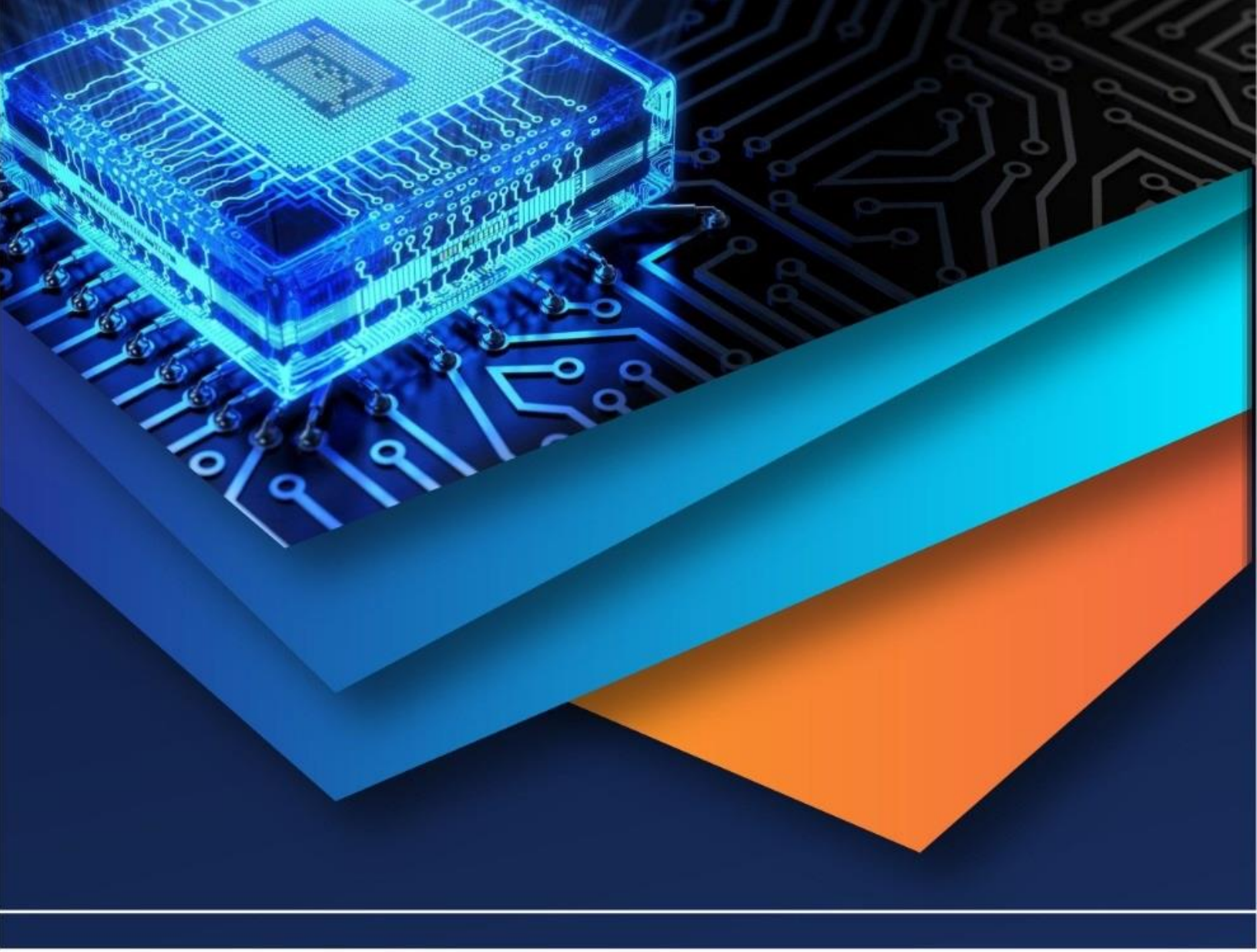
Therefore, this is the complete information that you must know about the Keyloggers.

VI. ACKNOWLEDGEMENT

I would like to express my deep gratitude to Professor Mrs. A.S. Khandagale, our project guide, for their patient guidance, enthusiastic encouragement, and useful critiques of this research work.
I would also like to thank Mrs. V.R. Palandurkar, for her advice and assistance in keeping my progress on schedule.
I would also like to extend my thanks to the technicians of the laboratory of the Information Technology department for their help in offering me the resources in running the program.
Finally, I wish to thank my parents for their support and encouragement throughout my study.

REFERENCES

[1] M. Aslam, R.N. Idrees, M.M. Baig, and M.A. Arshad. Anti-Hook Shield against the Software Key Loggers. In Proceedings of the 2004 National Conference on Emerging Technologies, pages 189–192, 2004.
[2] Martin Vuagnoux and Sylvain Pasini. Compromising electromagnetic emanations of wired and wireless keyboards. In Proceedings of the 18th conference on USENIX security symposium, SSYM ’09, pages 1–16, Berkeley, CA, USA, 2009. USENIX Association.
[3] Mihai Christodorescu and Somesh Jha. Testing malware detectors. In Proceedings of the 2004 ACM SIGSOFT International Symposium on Software Testing and Analysis, ISSTA ’04, pages 34–44, New York, NY, USA, 2004. ACM
[4] Manuel Egele, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. A survey on automated dynamic malwareanalysis techniques and tools. ACM Computing Surveys (CSUR), 44(2):6:1–6:42, March 2008. ISSN 0360-0300.
[5] Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christodorescu, and Engin Kirda. Accessminer: using system-centric models for malware protection. In Proceedings of the 17th ACM conference on Computer and communications security, CCS ’10.
[6] Kaspersky Lab. Key loggers: How they work and how to detect them. http://www.viruslist.com/en/analysis?pubid=204791931. Last accessed: Jan 2014.
[7] Engin Kirda, Christopher Kruegel, Greg Banks, Giovanni Vigna, and Richard A. Kemmerer. Behavior-based spyware detection. In Proceedings of the 15th conference on USENIX Security Symposium, SSYM ’06, Berkeley, CA, USA, 2006. USENIX Association.
[8] Anthony Cozzie, Frank Stratton, Hui Xue, and Samuel T. King. Digging for data structures. In Proceedings of the 8th USENIX conference on Operating systems design and implementation, OSDI ’08, pages 255– 266, Berkeley, CA, USA, 2008. USENIX Association.
[9] Security Technology Ltd. testing and reviews of key loggers, monitoring products and spy software. http://www.keylogger.org. Last accessed: Dec 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY