A Survey on Windows Post Exploitation [MSF] Keylogger for Security

IJRASET Publication

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: III Month of publication: March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40684

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 III Mar 2022- Available at www.ijraset.com

A Survey on 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]HOD, 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 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 for legitimate uses, you should be aware how keyloggers are affecting you. First, we'll further define keystroke logging before diving into how keyloggers work. Then you'll be able to better understand how to secure yourself from unwanted eyes. You might find legal keyloggers are in your daily life more than you realized. Fortunately, the power to control your data is often in your hands if the monitoring party has asked for access. Outside of employment, you can simply decline permission to the keyloggers if you so choose.

Keywords: Keylogger, Reverse Shell, Post-Exploitation, Metasploit, Netcat, Intranet, privilege escalation.

I. INTRODUCTION

In the past few years, the topic of personal data privacy has become a major concern in both America and Europe. Many people are now looking for ways to protect their personal data. This is where keylogger comes in handy. A keylogger is a program that runs in the background or hardware, recording all the keystrokes. So that the person using the keyboard is unaware that their actions are being monitored.[1] Keyloggers can be hardware installed to a computer or software that is used to collect sensitive information.

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. [2] 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 you 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.[1]

A. *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 in order 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 then Software Keylogger but it have portability issue.[3]
2) *Software Keylogger:* Keyloggers are activity-monitoring software programs that give hackers access to your personal 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. LITERATURE SURVEY

A. Keystroke Logging: Integrating Natural Language Processing Technique to Analyze Log Data

The research work is done by Disha H. Parekh, Nehal Adhvaryu, Vishal Dahiya. Cyberwarfare is observed very frequently as always some or the other country is targeting to ruin its enemy country by hacking confidential data from vital computer systems. This has led to dangerous international conflicts. Hence, to avoid illicit entry of other than military person or a government official several tools are being used today as spyware. Keyloggers are one of the prominent tools which are used in today's world to obtain secret or confidential data of a legitimate and contradictory a malicious user too. These keyloggers are advantageous and taken up positively for monitoring employee productivity, for law enforcement and the search for evidence of the crime. While it's negative illegitimate use includes data theft and passwords. The keylogger is today witnessed as a malicious attack and is looked upon as a security threat. But every coin has two sides. Keylogger actually helps in avoiding several security breaches and also aids in detecting several crimes across the net world followed by other fellow countries. This fact has motivated to write this paper and as a consequence, an experimental analysis too was carried out in order to conclude that keyloggers' log file helps identify the person by analysing proper pattern of the words entered in the file. This paper focuses majorly on the aspect of natural language processing, where a log file obtained thru keylogger software is thoroughly processed via the algorithm as described in the paper. The results yielded a fair understanding of the results obtained as one can easily identify the words used and on the basis of that can also know the type of person on the other end with his ideas, malicious one or of a legal kind

B. Keylogger for Windows using Python

The research work is done by Santripti Bhujel, Mrs. N. Priya. The proposed point Keylogger which is likewise called as keystroke logger is a product that tracks or logs the key struck on your console, regularly in a mystery way that you have no clue about that your activities are being observed. Most of the people tend to see only bad side of this particular software but it also has legitimate use. Aside from being utilized for vindictive purpose like gathering account data, Visa numbers, client names, passwords, and other private information, it can be used in office to check on your employees, at home to monitor your children's activities and by law enforcement to examine and follow occurrences connected to the utilization of PCs. The project will be completely based on Python where I will make use of pynput module which is not a standard python module and needs to be installed. The software that I am going to build should monitor the keyboard movement and stores the output in a file. To elevate the project I will also add a feature where the logs will be directly sent to the e-mail.

C. Keyloggers in Cybersecurity Education

The research work is done by Christopher A. Wood and Rajendra K. Raj. Keylogger programs attempt to retrieve confi- denial information by covertly capturing user input via keystroke monitoring and then relaying this information to others, often for malicious purposes. Keyloggers thus pose a major threat to business and personal activities such as Internet transactions, online banking, email, or chat. To deal with such threats, not only must users be made aware about this type of malware, but software practitioners and students must also be educated in the design, implementation, and monitoring of effective defenses against different keylogger attacks.

D. Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm

The research work is done by Robbi Rahim, Heri Nurdiyanto, Ansari Saleh, Dahlan Abdullah, Dedy Hartama and Darmawan Napitupulu. The development of technology is very fast, especially in the field of Internet technology that at any time experiencing significant changes, The development also supported by the ability of human resources, Keylogger is a tool that most developed because this application is very rarely recognized a malicious program by antivirus, keylogger will record all activities related to keystrokes, the recording process is accomplished by using string matching method. The application of string matching method in the process of recording the keyboard is to help the admin in knowing what the user accessed on the computer.

III. PROBLEM STATEMENT

Stealing user confidential data serves for 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 key logging, which is the eavesdropping, harvesting and leakage of user issued keystrokes. Key loggers are easy to implement and deploy. [3]When deployed for fraud purposes as part of more elaborated criminal heists, the financial loss can be considerable. Table 1.1 shows some major key logger based incidents as reported. To address the general problem of malicious software, a number of 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. [7] As we show next phase, implementation of a key logger hardly poses any challenge. Even unexperienced programmers can easily develop new variants of existing key loggers, and thus make a previously valid signature ineffective. To design and implement a exe application that works with windows operating system to capture keystrokes. The work also address the issue of malware handling in Cybersecurity.

A. Goal and Objectives

In this thesis, we investigate solutions to detect and tolerate key loggers. We also acknowledge that a common trade-off of any security solution is usability, which in our case roughly translates to “how deployable the proposed detection technique is”. For this reason we do not consider solutions entailing either virtualization or emulation of the underlying operating system. On the contrary, we also explore, where applicable, solutions requiring no privilege to be executed or deployed. Although the dissertation is primarily focused on detecting key logging behaviours, we do not overlook the scenario of users left with no other choice but to use a compromised machine.

In this context we propose a novel approach to tolerate key loggers while safeguarding the users’privacy.

Make a keylogger and reverse shell script. In the Virtual Scenario, we have to transfer the exe file containing keylogger and reverse shell to windows operating system.

Thus the main objective of this research work was to enhance the current cyber security situation and propose an Authentication Mechanism which could prevent the keyloggers from systems. Firewall can eliminate or suspect the specific keylogger based on malicious activity on different operating system.

All our approaches pivot around the idea of ignoring the key loggers’ internals, this to offer detection techniques that do not share the same limitation of signature-based approaches. On the other hand, unlike other approaches, we only focus on modelling the key logging behaviour, this to avoid false positives as much as possible. In addition to keeping the assumptions on the key logger to a minimum, we also aim at discarding any assumption on the underlying environment. In particular, in the context of key loggers implemented as browser add-ons, we investigate the feasibility and the challenges of a cross-browsers approach. The goals of this thesis can then be summarized in the following three research questions:

Question 1. Can we detect a key logger, either implemented as separate process or extension, by analysing its footprint on the system?

Question 2. To which extent are unprivileged solutions possible? What is the trade-off in terms of security and usability?

Question 3. Is it possible to tolerate the problem by “living together with a key logger” without putting the user’s privacy at danger?

B. Statement of scope

The main function of the project is to reduce manual paper work and developing a exe application which can record every keystrokes through reverse shell.

C. Software context

To develop this application we will require PYTHON or RUBY as development language. METASPLOIT and NETCAT will be used to interact with the victim and attacker computer. All this software’s are available on internet and they are free of cost.

D. Major constraints

This system is developed in an application, and this provide the great CLI to the system. This system also tested using testing tools. The Scripting a exe file of the system will be constrained by the availability of required software such as VMware pro workstation, and development tool. The availability of these tools will be governed by developer of the software. The most recent versions of software development tools may not be installed at the client side.

E. Methodologies of problem solving and efficiency issues

Most of the keylogger doesn’t have a reverse shell in it. Due to lack of connectivity, We are going to embed a Reverse Shell which make more convenient and efficient connectivity with the targeted device. Also, because of reverse shell, we can browse the directories/files of the target’s. Our keylogger will not only record the keystrokes but it will take snapshot, webcam shot and such more function.

IV. PROPOSED METHODOLOGY

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.

The idea of the keylogger is to monitor/keep track of mass number of people like MNC's employee, organisation, Terrorist groups or to track Suspicious targets It can also be used a parental control to monitor children activity, to stop any cyber incidents. In this proposed research work is to implement the proposed approach with multiple VMs. Also, we plan to explore the implications of keylogger on computers from any malicious websites. In our proposed system we use to create a exe malware, to track target's keystroke on the computer. A reverse will be used to interact with the victim computer and activating 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 attackers computer without interfering with the his/her firewall. After getting reverse shell from the victim, We will initiate keylogger script. Then every keystrokes will be recorded in victim's Pc. Finally we will dump the keystrokes data. The data we dumped is received from victim's to attacker's computer.

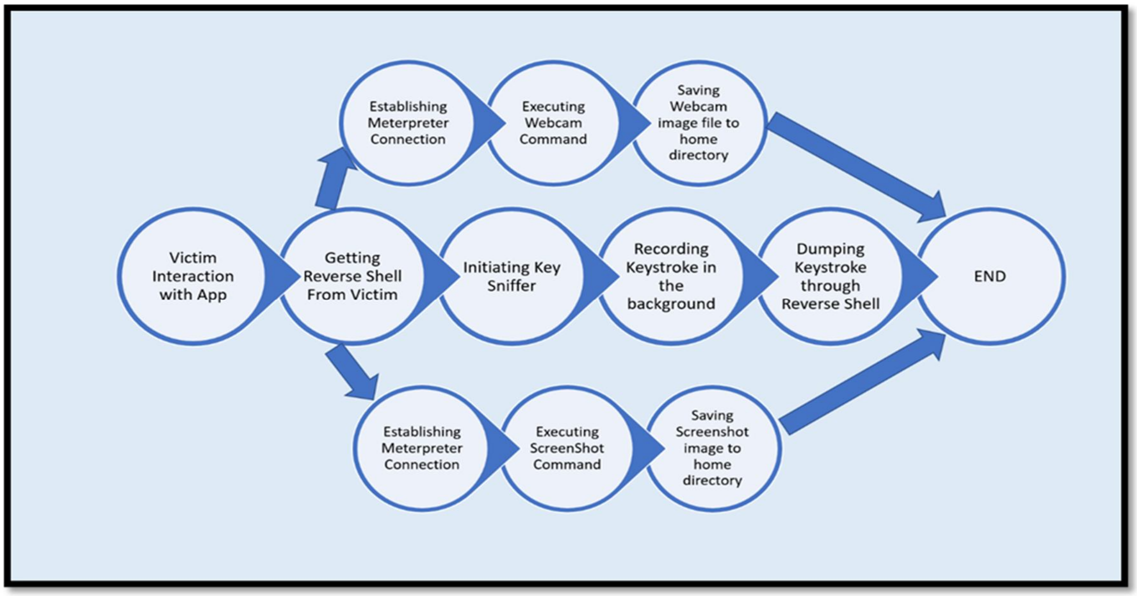
Establishing Meterpreter Connection
Executing Webcam Command
Saving Webcam image file to home directory
Victim Interaction with App
Getting Reverse Shell From Victim
Initiating Key Sniffer
Recording Keystroke in the background
Dumping Keystroke through Reverse Shell
END
Establishing Meterpreter Connection
Executing ScreenShot Command
Saving Screenshot image to home directory

Fig. 4.1. Architecture of the Keylogger

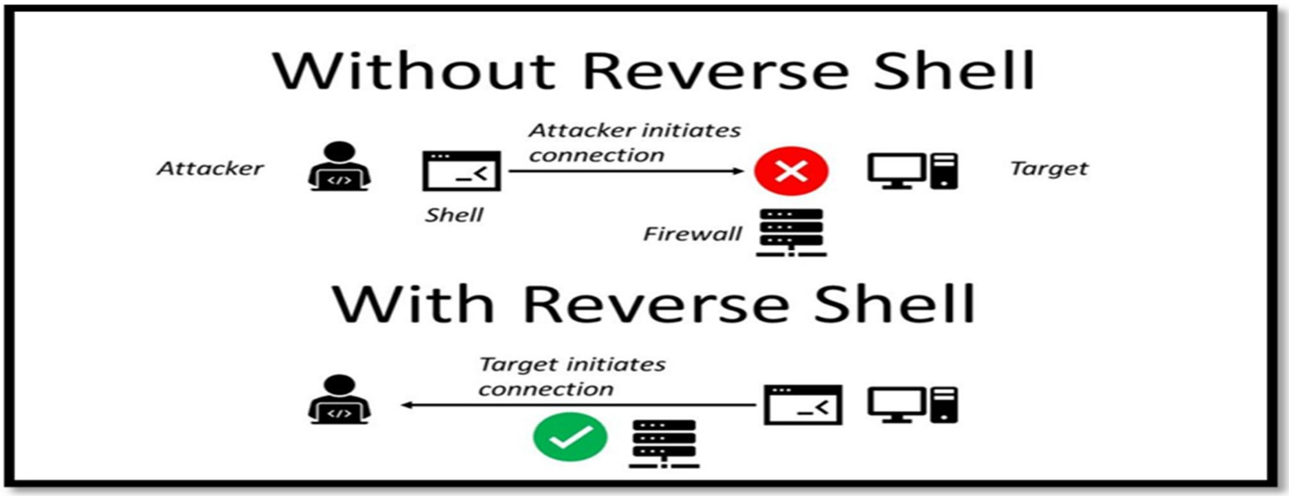

Fig. 4.2. Reverse Shell

V. PROJECT PURPOSE

A. Legal Consensual Keylogger Uses

Legal keylogger use requires the person or organization implementing it to:

Involve no criminal use of data. Be the product owner, manufacturer, or legal guardian of a child owning the product.

Use it in accordance with their location's governing laws. Consent is notably absent from this list. Keylogger users don't have to obtain consent unless laws the area of use require them to. Obviously, this is ethically questionable for uses where people are not made aware that they are being watched.

In consensual cases, you may allow keystroke logging under clear language within terms of service or a contract. This includes any time you click "accept" to use public Wi-Fi or when you sign an employer's contract.

Here are some common legitimate uses for keyloggers:

IT troubleshooting — to collect details on user problems and resolve accurately.

Computer product development — to gather user feedback and improve products.

Business server monitoring — to watch for unauthorized user activity on web servers.

Employee surveillance — to supervise safe use of company property on-the-clock.

You might find legal keyloggers are in your daily life more than you realized. Fortunately, the power to control your data is often in your hands if the monitoring party has asked for access. Outside of employment, you can simply decline permission to the keyloggers if you so choose.

B. Legal Ethically Ambiguous Keylogger Uses

Non-consensual legal keylogger use is more questionable. While it violates trust and privacy of those being watched, this type of use likely operates in the bounds of the laws in your area.

In other words, a keylogger user can monitor computer products they own or made. They can even monitor their children's devices legally. But they cannot surveil devices outside of their ownership. This leaves a bit of a grey area that can cause problems for all involved.

Without consent, people and organizations can use keyloggers for:

Parental supervision of kids — to protect their child in their online and social activities.

Tracking of a spouse — to collect activity on a device the user owns for proof of cheating.

Employee productivity monitoring — to watchdog employees use of company time.

Even consent that has been buried under legal jargon within a contract or terms of service can be questionable. However, this does not explicitly cross the line of legality either.

C. Criminal Keylogger Uses

Illegal keylogger use completely disregards consent, laws, and product ownership in favor of nefarious uses. Cybersecurity experts usually refer to this use case when discussing keyloggers.

When used for criminal purposes, keyloggers serve as malicious spyware meant to your capture sensitive information. Keyloggers record data like passwords or financial information, which is then sent to third-parties for criminal exploitation.

Criminal intent can apply in cases where keyloggers are used to:

Stalk a non-consenting person — such as an ex-partner, friend, or other individual.

Steal a spouse's online account info — to spy on social media activity or emails.

Intercept and steal personal info — such as credit card numbers and more.

Once the line has been crossed into criminal territory, keyloggers are regarded as malware. Security products account for the entire user case spectrum, so they may not label discovered keyloggers as immediate threats. Similarly to adware, the intent can be completely ambiguous.

VI. FUTURE ENHANCEMENT

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 for 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. Also, there are some advance feature which be developed later on in future. Those features are: Taking Screenshots, Screen Sharing Function, Accessing Webcam's, Accessing Data of Victim's computer

VII. 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 for 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.

VIII. 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.