A STUDY ON TECHNIQUES USING WINDOW KEYLOGGER IN THE PROFESSIONAL CAREER GROWTH.

Mr Aditya Rana[1], Mr KapishKumar[2], MrAzeemKhan[3]

[1, 2, 3]Department of Computer Science,

MIET, Greater Noida, Uttar Pradesh, India

ABSTRACT

A keylogger, also known as a keystroke logger, is a software program or hardware device that records actions (keys pressed) on the keyboard. Keylogger is a type of spyware that keeps the user unaware that their actions are being tracked. Keyloggers can be used for a variety of purposes, including gaining illegal access to your private information by hackers and monitoring employee activities by employers. Some keyloggers, known as screen recorders, can also capture your screen at random intervals. Keylogger software records your keystrokes in small files that can be accessed later or emailed to someone watching your activity. Keyloggers are used in everything from Microsoft products or in any company's computers and servers. Sometimes someone can install/connect a keylogger to your phone or laptop to verify a fraud report. Worse, criminals have been known to infiltrate legitimate websites, apps, and even USB drives with keylogger malware. You should be aware of how keyloggers affect you, whether for malicious or legitimate purposes. Before delving into how keyloggers work, we'll first define keystroke logging.

Keywords: *Keylogger, Discord, Post-Exploitation*

INTRODUCTION

Keylogger is a tool/software that records everything on your computer or smartphone screen when you press a key on your keyboard or swipe the touchscreen. Keyloggers operate by listening in on your typing and recording it all into files that can later be accessed remotely via the Internet. Business owners use them to monitor productivity, so they know if their employees are doing their jobs correctly or not.

There are many different types of keyloggers available, each with a different price tag. Some keyloggers are small enough to hide on your machine yourself, or are placed on your desk to hide all your typing and swiping movements.

Some keyloggers are installed on USB flash drives and other storage devices. Types of Keylogger

1) ***Hardware Keylogger****:* Hardware keyloggers are electronic devices designed to intercept data between a keyboard and an I/O port. These compact devices have an internal memory that stores keystrokes for later retrieval by the installer. Because they operate on the hardware platform, hardware keyloggers are undetectable by anti-viral software or scanners. Hardware keyloggers are far more powerful than software keyloggers, but they are less portable.

2) ***Software Keylogger****:* Keyloggers are activity-monitoring software programmes that allow hackers to access your data. When a user downloads an infected application, keylogger software is installed on the computer. It monitors the paths of the operating system that the keys you press on the keyboard must take once installed. This is how keylogger software tracks and records keystrokes. The information is then transmitted to the hacker via a remote server.

PROBLEM STATEMENT

Stealing user confidential data serves a variety of illegal purposes, including identity theft, banking and credit card fraud, and software andservice theft, to name a few. This is accomplished through keylogging, which can be considered eavesdropping, harvesting, and leakage of user-issued keystrokes. Keylogger is easy to install and use. When used for fraud purposes as part of more elaborate criminal heists, the financial loss can be significant. Signature-based solutions have limited applicability because they are easily evaded and also necessitate isolation. There is a lack of cyber security awareness among people regarding these attacks. Also, many keyloggerssoftware are paid.

ACTUAL METHODOLOGY

A keylogger is a type of malware or piece of hardware that monitors and records your The keylogger is designed to monitor people. It may also serve as parental supervision to monitor and prevent cyber incidents in kids. The purpose of this proposed research is to show how keyloggers log the victim's data and send it back to the attacker. we intend to keystrokes as you type. It uses a command-andcontrol (C&C) server to send the information toa hacker.

A. **Requirement**s:

1) **Two machines**:

   a) Victim machine

   b) Attacker machine

2) **Tools required**: Discord.

3) **Software**: VMwareWorkstation

4) **IDE**: Sublime Text Editor

Research the effect of keyloggers on our system. In the proposed system, we use an executable file to capture the target's keystrokes and used Discord as a command-and-control server to send the data to the attacker.

Figure 1: a flow diagram depicting the process of windows keylogger

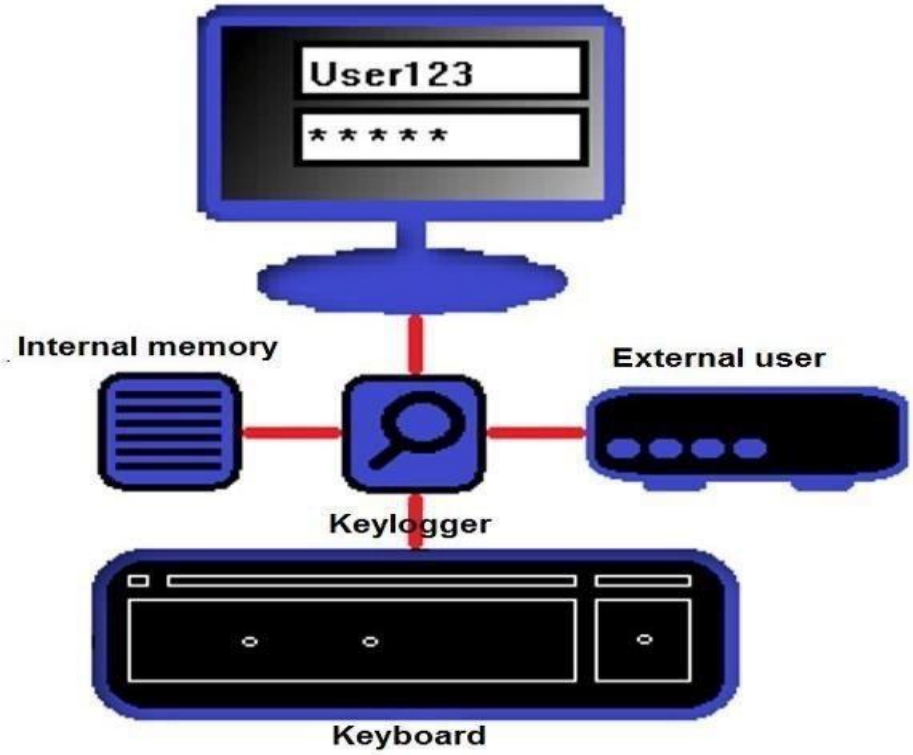

Figure 2: diagram of the log storage of keystrokes.

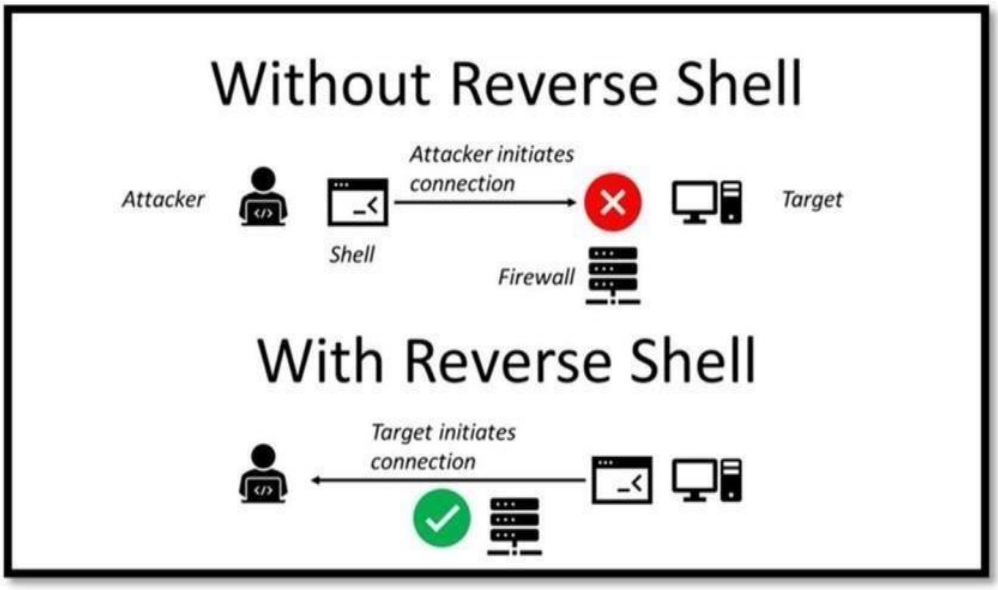

Figure 3: Reverse Shell

RESULTS

A. Attacker

Discord Server

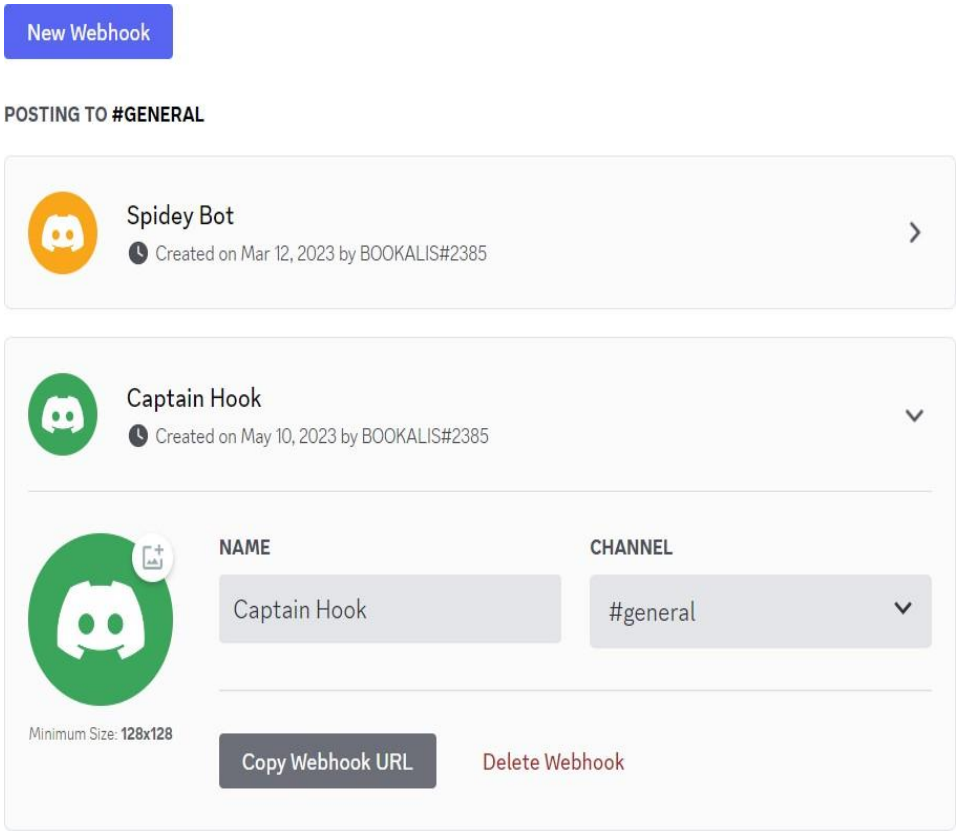

Figure 4: created a discord webhook to receive the keystroke data

In this, the attacker has created a discord server and webhook by which all the data can be received by an attacker on his c2 server.

B. Received Keystrokes of victim

Keystrokes of victim

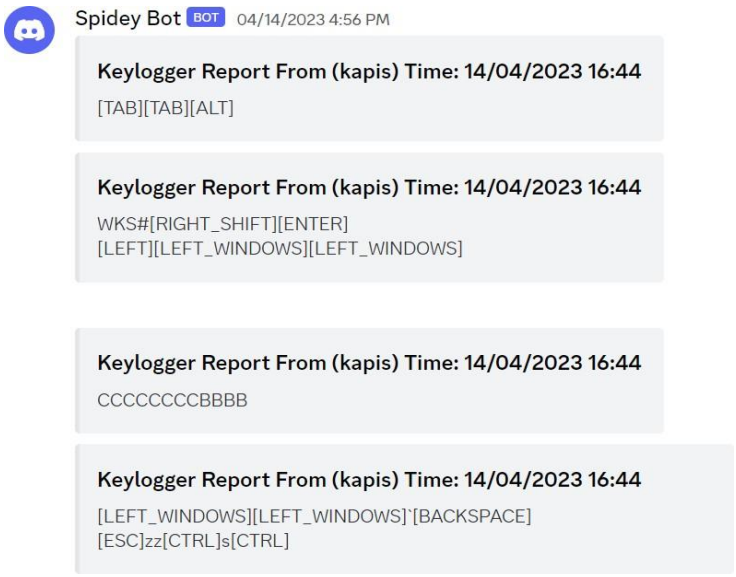

Figure 5: receiving the keystroke data into his control server.

In this, the attacker has received the keystrokes of the victim into his command-and-control server.

CONCLUSION

With the evolution of technology and the pervasiveness of computers in any private or industrial environment, keylogger devices, both hardware and software, pose a serious threat of cyber interception. Furthermore, because of the ease with which they can be found and purchased via the Internet at reasonable prices. The keylogger is a malicious programme that is difficult to detect and capable of reading and discovering anything on the keyboard. As a result, this survey paper is a comprehensive guide to everything you need to know about keylogger software. It's not always easy to tell if your device has a keylogger. In terms of hardware keyloggers, the only way to detect them is to inspect the keyboard, as well as the cables that connect to it.

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.