International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Keylogger

Rujuta Santosh Barve

Department of Computer
Rasiklal M Dhariwal Institute of Technology, Pune, Maharashtra, India
Email- rujutabarve20@gmail.com

ABSTRACT—

Keylogger is a software or hardware tool that is designed to monitor and record keystrokes on a computer or mobile device. This abstract explores the functionality of keyloggers, their various types, and potential applications in both legitimate and malicious contexts. Keyloggers can be used for various purposes such as monitoring employee productivity or parental control, but they also pose significant security risks when employed by cyber attackers for stealing sensitive information like passwords, credit card details that is personal credentials of the user. Understanding the mechanisms and implications of keyloggers is crucial for implementing effective cybersecurity measures and safeguarding digital privacy.

Keywords— Attack, Security, Keylogger, Keystrokes, Password

I. INTRODUCTION :

Keylogger represents a tool that can serve legitimate or kind or unpleasant and malicious purposes, depending on its application. A keylogger is a software or hardware mechanism designed to surreptitiously record every keystroke that is made on a computer or mobile device. A keylogger operates by intercepting and logging keystrokes entered by users. Whether it's typing a password, composing an email, or entering credit card information, every stroke of the keyboard is captured and stored. Initially conceived for legitimate purposes such as debugging software or monitoring employee productivity, keyloggers have also found impious applications in the hands of cyber attackers seeking to exploit vulnerabilities for personal gain.

II. BODY OF THE PAPER :

The evolution of keyloggers has mirrored the advancements in technology. From essential software programs to sophisticated malware capable of evading detection, keyloggers have become a potent tool in the arsenal of cyber attackers. They can be deployed through various vectors, including phishing emails, malicious websites, or compromised software installations, infiltrating systems with stealth and precision. As we delve deeper into the realm of keyloggers, it becomes evident that their implications extend far beyond mere keystroke logging. They represent a fundamental challenge to digital privacy and security, raising concerns about the safeguarding of sensitive information in an increasingly interconnected world. In this exploration of keyloggers, we will delve into their functionality, classification, detection methods, and the ethical considerations surrounding their use.

III.FUNCTIONALITY :

1. A keylogger is installed. (Can be installed from various sites like Github)
2. Each device has a default 3 key built in combination for keylogger. These keys by default are the K,B,S keys. These 3 keys are pressed simultaneously to trigger Flash Drive mode.
3. After a few seconds, the hardware keylogger will automatically get detected as a mass storage device.
4. The keylogger will run with the pre-defined settings.
5. The keylogger will run on the backend and the details entered by the user on the front end will be stored on the backend.
6. To view recorded keystrokes, type the chosen password on the keyboard

IV. KEYLOGGER OVERVIEW :

First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.

A] Software Keylogger:

A software keylogger is designed to record the keystrokes made by a user. While it may seem harmless, in the hands of a hacker, it becomes a dangerous tool. Hackers use software keyloggers to steal information from victims. This information can include confidential or personal details. Some companies also use software keyloggers to monitor employee activity. The keylogger can be installed as software on a computer, and it captures every keystroke made by the user. Software keylogger is easy to install. The only disadvantage of the software keylogger is that is cannot be detected by software antivirus. Software keylogger includes- JavaScript based key logger and Form Based Key loggers.

B] Hardware Keylogger:

A hardware keylogger is a physical device used for recording keystrokes. It starts functioning when plugged into a computer. The captured keystrokes are stored within the device, and to retrieve the data, users need physical access to the keylogger. Unlike software keyloggers, hardware keyloggers are undetectable by antivirus software. They appear as external devices attached to the computer, making them hard to detect. They can be installed inconspicuously at the back of a computer. Hardware keylogger can also act as evidence against the attacker. Hardware keylogger includes: USB keylogger and Smartphone sensors.

V. CASE STUDY :

Japanese Bank Attack

The attempted cyber-heist occurred at the Sumitomo Mitsui Bank in London. The bank detected the suspicious activity in October 2004 and promptly informed the police. The criminals aimed to transfer a staggering £229 million (approximately $437 million) from the bank. The attackers gained access to the bank's computer systems. They installed keyloggers in the systems. By capturing user's passwords through keylogging, the criminals planned to execute the unauthorized transfer.

Lessons learnt:

- Institutions should thoroughly review and check any new programs before installation.
- Altering details that might provide hints to keyloggers about passwords is crucial.
- Rigorous testing and debugging should precede full program installation.
- Implement security systems that respond to attempted crimes.
- Governments can impose restrictions and penalties on offenders.
- Educate and train personnel to avoid risky behaviour, such as clicking on suspicious links.

VI. THESIS STATEMENT :

Despite their dual nature as tools for both legitimate and malicious purposes, keyloggers fundamentally challenge digital privacy and security, necessitating comprehensive understanding, detection mechanisms, and ethical considerations to mitigate their risks and safeguard sensitive information in today's interconnected world.

VII.CONCLUSION :

Keyloggers represent a potent tool with dual potentialities. Serving both legitimate and malicious purposes. While they offer utility in monitoring employee activity, parental oversight, or law enforcement investigations. Legal and ethical considerations cannot be overstated. As technology evolves, so too must our defences against malicious actions. By understanding the workings of keyloggers, implementing effective countermeasures, and adhering to ethical principles, we can safeguard ourselves against the threat they pose, thereby fostering a safer digital ecosystem for all.

VI. REFERENCE :

1. Microsoft's Developer Network, "Operator Precedence and Associativity." Available at: http://msdn.microsoft.com/enus/library/126fe14k.aspx
2. Nikolay Grebennikov, "Keyloggers: Implementing keyloggers in Windows. Part Two." Available at: http://www.securelist.com/en/analysis/204792178/Keyloggers_ Implementing_keyloggers_in_Windows_Part_Two#13
3. http://www.parxy.com/hardware-based-keyloggers-vssoftware-based-keyloggers---what-s-the-difference-.html
4. Wikipedia, "Keystroke logging." Available at: http://en.wikipedia.org/wiki/Keystroke_logging 5. Nikolay Grebennikov, "Keyloggers: How they work and how to detect them (Part 1)." Available at: http://www.securelist.com/en/analysis?pubid=204791931 6. REFOG, "Benefits of Keylogger for Windows 7/8."
5. Available at: http://www.refog.com/keylogger-for-windows-78.html
6. https://github.com/topics/keylogger