Chapter 6
Key Logger and Prevention of Security Breaches

Aparna Datta
https://orcid.org/0009-0006-2552-9017
Meghnad Saha Institute of Technology, India

Akash Mondal
Meghnad Saha Institute of Technology, India

Arunima Sarkar
Meghnad Saha Institute of Technology, India

ABSTRACT

Keyloggers are malicious programs that record keystrokes and jeopardize the security of personal and business data. These sneaky malwares grab vital information while evading user discovery. Keyloggers conceal their existence by using techniques like rootkits to bypass antivirus and other security measures. Once installed, they are not visible on the process monitor . Attackers may unlawfully access sensitive information, such as banking credentials. One major worry regarding keyloggers is that around 90% of them now function in the user's environment without express authorization, leaving the user unaware that their device is being watched. Although there are hazards, addressing the keylogger threat necessitates preventative actions. This article proposes ways to improve the prevention of assaults, such as hacking. It advocates employing strong security tools and increasing cybersecurity awareness. Additionally, the following discussion suggests methods to understand the capabilities of keyloggers, develop detection methods, and rigorously evaluate countermeasures accordingly.

DOI: 10.4018/979-8-3693-9235-5.ch006

INTRODUCTION

A keystroke logger, often known as a keylogger, is a tool used to systematically track and document each keystroke entered on a device such as a computer or smartphone. It is engineered to surreptitiously record all keyboard interactions on the target device.

Keyloggers are a type of spyware; It is a type of malware designed to spy on users by recording their information without their permission. As spyware, keyloggers work very stealthily, making them difficult for users. It is designed to capture personal information that can be used for malicious purposes such as identity theft, illegal financial transactions, or participation in criminal activities. Keyloggers are regularly used in tandem with other malware to improve the effectiveness of cyberattacks. They are used for both monitoring and harmful activities. The threat of keylogging is not new to users; the first keyloggers were put in U.S. Embassy and Consulate buildings in various nations in the 1970s to collect information for counterterrorism activities in St. Petersburg (Wajahat et al., 2019).

There are many types of keyloggers on the market, such as hardware keyloggers and software keyloggers. Keylogger software is a sort of malware that infects one device and, if built, it can spread to other devices in the same network. Hardware keyloggers, unlike software keyloggers, cannot be transferred from one device to another; yet, they can still be collected by a hacker or group of hackers. This information can then be used to hack a computer or another device that requires authentication to gain access and steal sensitive information.

No physical access to the user's computer is required to install keylogging software programs. Software keyloggers can be classified according to their level of functionality and the way they interact with the system. The main types are kernel-type keyloggers and userspace keyloggers. Kernel-mode keyloggers operate at the kernel level of the system. They have the highest level of authority and can directly interact with hardware and memory. User space keyloggers operate in the user space of the operating system on which most applications run. They are less privileged than kernel-type keyloggers but are easier to create and distribute.

Keylogger software supports the hardware devices used to use keyloggers (Ortolani et al., 2013). Such software is installed on the target machine and is responsible for identifying the user's activity by hiding and storing all keystrokes and some instructions and sending them outside the third party (Zhuang et al., 2009).