Key Logger Defender

Dr. Arvind Prasad
Assistant Professor (CEA)
GLA University, Mathura

Hitansh Mangla (2115000473)
Nikunj Maheshwari (2115000672)
Amrendra Singh (2115000141)

Abstract

This research paper explores the detection and prevention of keyloggers, which remain a significant cybersecurity threat, compromising user privacy and sensitive data. Keyloggers, whether hardware- or software-based, covertly capture keystrokes, enabling unauthorized access to confidential information. Despite advancements in security mechanisms, keylogging attacks continue to pose risks in personal and enterprise environments. The system analyzes outgoing network traffic to detect suspicious data transmissions, effectively flagging potential breaches. Prevention strategies such as secure browsing, two-factor authentication, virtual keyboards, and endpoint security are also discussed to create a **comprehensive defensive framework**. The proposed solution aims to enhance security against keystroke logging attacks by proactively detecting and neutralizing threats before they compromise user data.

***Keywords**: Computer security, keylogging, software keylogger categories.*

INTRODUCTION

Keystroke loggers are tools that are primarily used for recording the typed words or keywords on a personal device. There are legitimate and legal uses for it, but most hackers and attackers take mischievous advantage of keyloggers with the intent to jeopardize other individuals' data and information. These attacks can be highly damaging, leading to the theft of sensitive information and significant financial losses.

Keyloggers can be installed on a computer by cybercriminals, usually through social engineering techniques, phishing emails, or malware downloads. Dark Hotel is one of the examples of it. Hackers target unsecured Wi-Fi hotels and prompt users to download the software. Once downloaded, Dark Hotel acts as a keylogger of recorded keystrokes. It is important to protect from those attacks and possess a threat to cybersecurity. Keystroke agent is one of the solutions. It is a base simulation program that generates random keystrokes that are only visible to the keyloggers. Keyloggers track keystroke of all applications and store it, but it cannot separate whether the information given is from the real user or the keystroke agent.

This research paper explores the detection and prevention of keylogger-based attacks, which continue to be a significant concern in cybersecurity and privacy protection. Keyloggers, whether hardware- or software-based, stealthily record user keystrokes, often operating undetected in the background. While keyloggers have legitimate applications in enterprise security and user monitoring, they are frequently exploited by cybercriminals to steal sensitive information such as passwords, financial credentials, and personal communications. The ability of keyloggers to operate covertly poses a serious risk to data integrity and user privacy.

To counteract these threats, this study presents Keylogger Defender, a hybrid detection and prevention framework that combines honeypot mechanisms, keystroke agents, and encryption techniques to proactively identify and neutralize keyloggers. Honeypots serve as decoys to detect keylogging attempts by baiting malicious software into capturing false keystrokes. Keystroke agents generate randomized keystroke data, rendering the logs collected by keyloggers unreliable. Additionally, encryption algorithms ensure that even if keylogging malware captures keystrokes, the data remains unreadable without proper decryption keys.

This paper provides an in-depth overview of various keylogger detection strategies, including signature-based detection, anomaly detection, and behavior-based analysis, while also discussing advanced countermeasures such as secure browsing, two-factor authentication, virtual keyboards, and endpoint security. Keyloggers, being a type of rootkit malware, can bypass traditional security mechanisms by embedding themselves into system processes, making early detection crucial.

Furthermore, this study examines previous research in the field, including the work of Y. Zhang et al. (2018), which explores keystroke dynamics and machine learning models for detecting suspicious keystroke patterns. Building on these methodologies, Keylogger Defender enhances traditional detection techniques by incorporating network traffic monitoring, identifying anomalous communication between infected devices and external servers—a key indicator of exfiltrated keystroke logs.

By integrating multiple detection and prevention strategies, Keylogger Defender aims to strengthen endpoint security, reduce the risks associated with keylogger-based attacks, and contribute to the development of a robust cybersecurity defense mechanism.

ALGORITHMS THAT CAN BE USED TO DETECT ANOMALIES IN KEYSTROKE PATTERNS

The study by **S.G. Bhat et al.** on "Detecting Keyloggers Using Hardware Performance Counters" explores an innovative method for detecting keyloggers at the **hardware level**, leveraging system performance metrics to identify anomalies triggered by malicious keystroke logging activities. This approach highlights the importance of **hardware-based anomaly detection** in cybersecurity. However, most existing research primarily focuses on detecting keystroke dynamics in **single-user environments**, whereas real-world scenarios often involve **multi-user systems**, such as corporate networks and shared workstations. Differentiating keystroke patterns across multiple users presents a challenge in anomaly detection and requires **advanced behavioral analysis techniques**.

This paper delves into various aspects of **malware analysis**, including **attack vectors, keylogger implementation, infection mechanisms, and system persistence strategies**. Additionally, it explores how modern malware **bypasses detection techniques by using stealth mechanisms**, making traditional detection methods less effective. **Commercial anti-malware solutions**, while effective against conventional keyloggers with identifiable signatures, struggle to detect **advanced keyloggers** that utilize **evasive tactics, polymorphic behavior, and dynamic execution patterns**.

To enhance keylogger detection, **machine learning-based anomaly detection algorithms** can be implemented. These algorithms analyze **keystroke timing, pressure sensitivity, and typing patterns** to identify irregularities indicative of malicious activity. Techniques such as **Hidden Markov Models (HMM), Neural Networks, and Support Vector Machines (SVM)** have shown promising results in recognizing deviations from normal user behavior. Furthermore, network-based anomaly detection systems can **monitor outbound traffic** for suspicious data exfiltration, a key indicator of keylogger activity.

This research contributes to the **development of robust anomaly detection frameworks** that not only differentiate between normal and malicious keystroke behavior but also improve cybersecurity defense mechanisms against sophisticated **keylogging threats**.

RELATED WORKS

Extensive research has been conducted on **keyloggers**, which can exist as **software-based, hardware-based, or network-based** threats that record user keystrokes, often with **malicious intent**. Various studies have explored **detection and prevention techniques** to mitigate the risks posed by keyloggers.

M. A. Al-Hajj and A. Kayssi, in their study **"A Survey of Keylogger Techniques,"** provide a **comprehensive classification** of keyloggers based on their mode of operation, including **software keyloggers, hardware keyloggers, and network-based keyloggers**. They emphasize how modern keyloggers exploit vulnerabilities in **operating systems and network protocols** to remain undetected.

K. G. Kwon et al., in **"Detecting Keyloggers Using Behavioral Biometrics,"** introduce an innovative approach based on **keystroke dynamics**. Their research highlights how **typing speed, key press duration, and transition time** between keys can be used to distinguish normal user behavior from keylogger-induced activity.

M. S. Al-Maolegi et al., in **"Keylogger Detection and Prevention Techniques: A Review,"** examine a range of **signature-based, behavior-based, and hybrid** detection methods. Their work explores how **signature-matching techniques** struggle against **polymorphic and dynamically generated keyloggers**, necessitating more advanced behavioral and heuristic approaches.

Y. Chen et al., in **"Design and Implementation of a Keylogger Detector,"** propose a **software-based detection tool** that monitors **system calls and user input events** to identify suspicious behavior. Their approach focuses on **real-time anomaly detection**, reducing the reliance on **static signature-based detection**, which often fails against newly developed malware.

S. K. Sood et al., in **"Hardware Keyloggers: A Review of Technology and Countermeasures,"** provide an extensive analysis of **hardware-based keyloggers**, discussing countermeasures such as **physical inspection, encrypted input devices, and software-based detection methods**. Their findings highlight how hardware keyloggers, despite being harder to detect, can be mitigated using **secure input hardware and encrypted communication channels**.

Miss Suchitra and Prof. Ravi Randle propose an advanced detection system that **combines a detection engine with a honeypot mechanism** to **trap keyloggers and analyze their behavior** before they can cause harm. This hybrid approach **enhances detection accuracy** and prevents keyloggers from **successfully recording sensitive keystrokes**.

Pratik Hiralal Santoki introduces a **new architectural model** for identifying keyloggers available in the market. His approach **focuses on keystroke pattern analysis and the evasive behavior of keyloggers**, making it **effective against stealthy keyloggers that avoid detection through traditional security measures**.

These studies emphasize the **evolving nature of keyloggers** and the **need for continuous advancements** in detection techniques. The combination of **behavioral analysis, anomaly detection, and hardware-level security** provides a **comprehensive defense** against modern keylogging threats.

.

WORKING OF KEYLOGGER

The Keylogger work is to sniff the keystrokes without affecting other applications. It both contains software and hardware tools and works in combination of both to capture the data and information that gets stored. [3] The information can be achieved by intercepting kernel functions, DLL functions in user mode, filter driver in the keyboard stack or by standard documented methods.

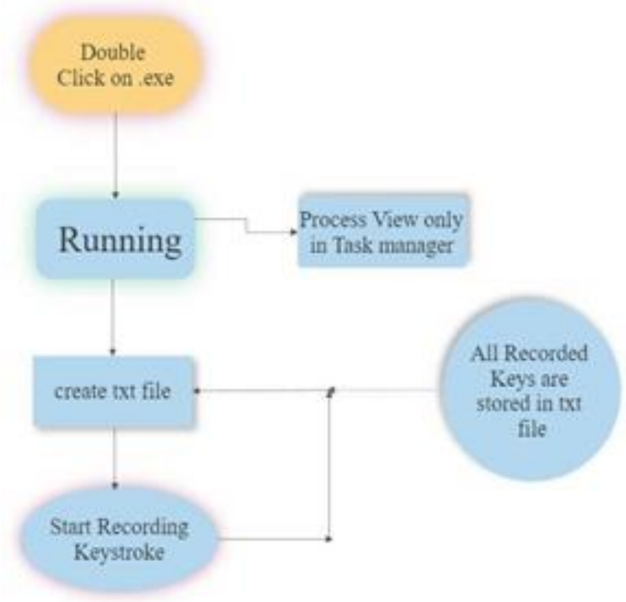

Double Click on .exe
Running
Process View only in Task manager
create txt file
All Recorded Keys are stored in txt file
Start Recording Keystroke

Fig. 1 Working of Keylogger

In general, the keylogger would be working on those processes. Keyloggers, which is a simple program, would be capture keystrokes. Any keystroke made on a computer or mobile device is recorded by a keylogger, which can be either software or hardware. A keylogger's primary function is to record sensitive data that users type on their device, including usernames, passwords, credit card numbers, and other private information.

Software-based keyloggers typically operate in the background of a device's operating system, capturing every keystroke made by the user and storing the data in a log file. They can be installed on a device via a Trojan virus or downloaded as a malicious program. Hardware-based keyloggers, on the other hand, are physical devices that are attached to the keyboard or USB port of a computer. They capture every keystroke made by the user and store the data in txt log file.

PREVENTION OF KEYSTROKE ATTACKS

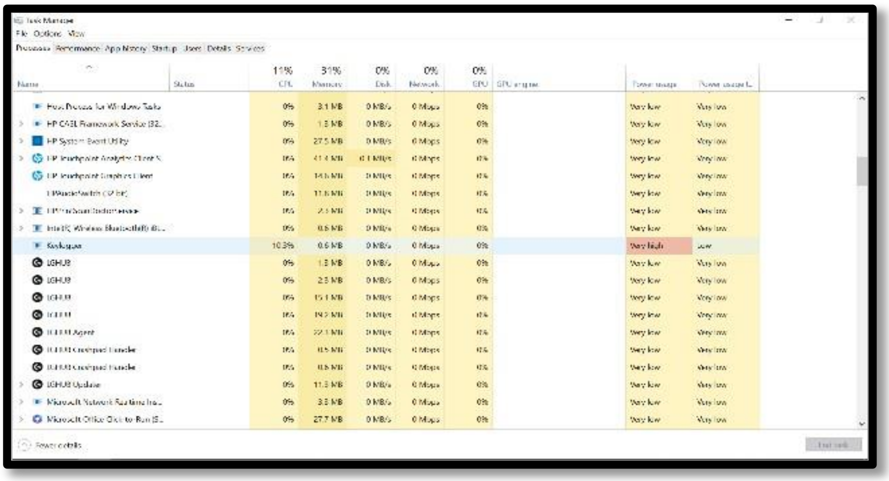
There are different ways to check whether the Keyloggers hide on our system and if they are stealing confidential or security related data such as passwords, PINs. The slowing of a system through intensive use of CPU resources shows the possible signs of intrusion and can be examined through the running process via the Task Manager. Checking for the startup processes as well gives a glance on if there are unusual software's that boots up during the startup. Hardware Keyloggers are however plugged in.

Keystroke logging attacks remain a significant threat in cybersecurity, allowing attackers to steal passwords, financial details, and other sensitive information without a user's knowledge. To counter such attacks, a combination of detection techniques, secure input methods, and preventive measures is necessary.

Preventing keystroke logging attacks requires a proactive approach that combines system monitoring, anti-spyware solutions, encryption methods, and secure input techniques. By implementing these measures, users can significantly reduce the risk of their sensitive data being compromised. As cyber threats continue to evolve, staying vigilant, keeping software updated, and practicing good cybersecurity hygiene are essential in defending against keyloggers.

IMPLEMENTATION

After executing the executable file, the keylogger process only appears in Task Manager.

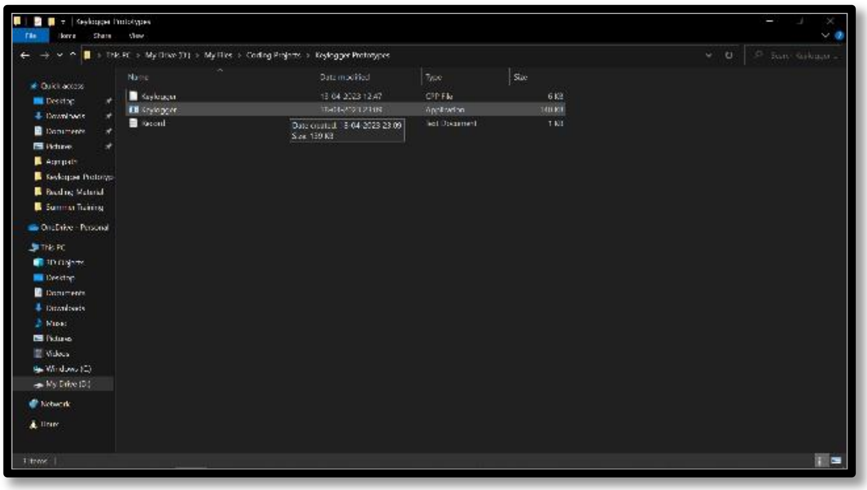


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

Name	Status	11% CPU	31% Memory	0% Disk	0% Network	0% GPU	GPU engine	Power usage	Power usage t...
Host Process for Windows Tasks		0%	3.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
HP CASL Framework Service (32...		0%	1.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
HP System Event Utility		0%	27.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
HP Touchpoint Analytics Client S...		0%	41.4 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
HP Touchpoint Graphics Client		0%	14.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
HPAudioSwitch (32 bit)		0%	11.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
[illegible]		0%	[illegible]	0 MB/s	0 Mbps	0%		Very low	Very low
Intel(R) Wireless Bluetooth(R) iBt...		0%	0.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Keylogger		10.3%	0.6 MB	0 MB/s	0 Mbps	0%		Very high	Low
LGHUB		0%	1.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
LGHUB		0%	2.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
LGHUB		0%	15.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
LGHUB		0%	19.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
LGHUB Agent		0%	22.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
LGHUB Crashpad Handler		0%	0.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
LGHUB Crashpad Handler		0%	0.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
LGHUB Updater		0%	11.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Microsoft Network Realtime Ins...		0%	3.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Microsoft Office Click-to-Run (S...		0%	27.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low

Fig. 1 Keylogger process appear in Task Manager

After executing keylogger.exe, the keylogger program automatically hides itself and simultaneously creates a Record.txt file in the Download folder of the C Drive. And in Rocord.txt, the keylogger starts recording keystrokes.

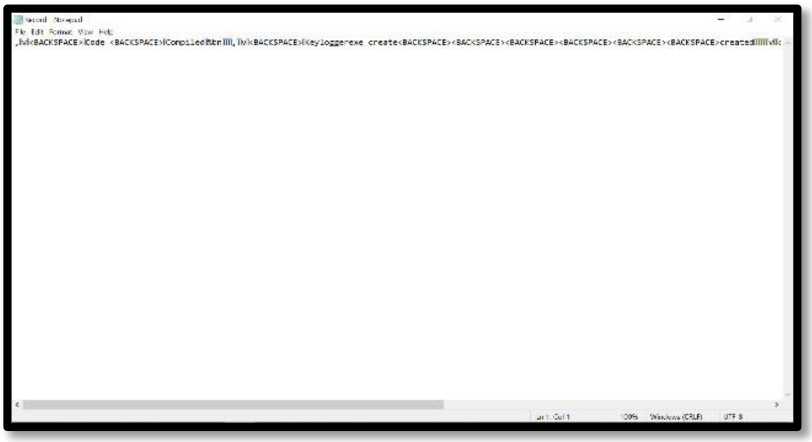


Name	Date modified	Type	Size
Keylogger	13-04-2023 12:47	CPP File	6 KB
Keylogger	13-04-2023 12:08	Application	140 KB
Record		Text Document	1 KB

Date created: 13-04-2023 23:09
Size: 139 KB

Fig. 2 Executable file created.

All keys pressed by the user are saved in the record.txt file.



```
,lvl<BACKSPACE>lCode <BACKSPACE>lCompiledlbtnllll, lvl<BACKSPACE>lKeyloggerexe create<BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE><BACKSPACE>createdllllllvllc
```

Fig. 3 Record.txt file created.

CONCLUSION

One of the reasons why keystroke logging attacks are so effective is because they can evade other security measures, thanks to their simple installation and implementation process. The research paper also suggests using encryption algorithms for prevention. The original file gets encrypted and sent to the honeypot system for further detection resulting in the scrambled log file instead of original file. Although some keyloggers are used legitimately, many keyloggers are used illegally by the inventor. This study has examined the most popular keylogger kinds and ways for hiding themselves while subverting a user's system. We also looked at the present situation of keyloggers and how they propagate. Finally, we examined current detection approaches and proposed some preventative measures.

Detecting keylogging technology inside an organisation is like managing other dangerous programmes or threats in that it requires general understanding and continuous monitoring. To prevent keyloggers from infecting your device, it's important to follow some preventive measures such as installing reputable antivirus software, keeping your device and software up to date, using strong passwords and enabling two-factor authentication, avoiding untrusted sources, and being cautious when entering sensitive information.

If you suspect that a keylogger is installed on your device, it's important to take immediate action to remove it and protect your sensitive information. This can include running a thorough antivirus scan, resetting your passwords, and enabling two-factor authentication on your accounts.

If a keylogger infection is suspected, immediate action is crucial. Running a thorough antivirus scan, inspecting running processes, resetting all sensitive passwords, and enabling multi-factor authentication on critical accounts can help minimize potential damage. In extreme cases, a complete system wipe and OS reinstallation may be necessary to fully eliminate the threat.

REFERENCES:

[1] Arjun Singh's "Keylogger Detection and Prevention" et al 2021 J. Phys.: Conf. Ser. 2007 012005

[2] Zhang, Y., Guan, Z., & Zhang, J. (2018). Keystroke dynamics: A survey of recent advances and challenges. IEEE Access, 6, 23793-23811.

[3] Bhat, S. G., Egele, M., & Kruegel, C. (2015). Detecting keyloggers using hardware performance counters. In Proceedings of the 24th USENIX Security Symposium (pp. 423-438). USENIX Association

[4] P. Mell, K. Kent, and J. Nusbaum, "Guide to malware incident prevention and handling," National Institute of Standards and Technology, Gaithersburg, MD,] P. Mell, K. Kent, and J. Nusbaum, "Guide to malware incident prevention and handling," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. 800-83, November 2005.

[5] Miss. Suchita Yadav, Prof. Ravi Randale. "Detection and Prevention of Keylogger Spyware Attack" (IJAFRSE, Vivruti 2015)

[6] M. Aslam, R.N. Idrees, M.aM. 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

[7] "Keylogger Detection and Prevention Techniques: A Review" by M. S. Al-Maolegi et al., which reviews various techniques for detecting and preventing keyloggers, including signature-based, behaviour-based, and hybrid approaches.

[8] Kumar, S., & Kumar, P. (2019). Prevention and detection of keylogger attacks: A review. Journal of Network and Computer Applications, 131, 54-72

[9] Host based Intrusion System Le at el. (2008) "Detecting Kernel Level Keyloggers Through Dynamic Taint Analysis".

[10] Pratik Hiralal Santoki (2014) "Design and Implementation of Detection of Keylogger" IJEDR, Volume 2, Issue 2 | ISSN: 2321-9939

[11] Le, Duy, et al. "Detecting kernel level keyloggers through dynamic taint analysis." College of William & Mary, Department of Computer Science, Williamsburg, VA, Tech. Rep. WM-CS-2008-05 (2008).

[12] Aslam, M., Idrees, R.N., Baig, M.M. and Arshad, M.A., 2004, December. Anti-hook shield against the software key loggers. In National Conference on Emerging Technologies (pp. 189-191).

[13] Wajahat, A; Imran, A; Latif, J; Nazir, A; Bilal, A. 'A novel approach of unprivileged keyloggers detection'. Second IEEE International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, Pakistan, 2019. DOI: 10.1109/ICOMET.2019.8673404.

[14] Kumar, S; Sehgal, R; Bhatia, J. 'Hybrid honeypot framework for malware collection and analyses. Seventh IEEE International Conference on Industrial and Information Systems (ICIIS), 2012.

[15] Murugan, S; Kuppusamy, K. 'System and methodology for unknown malware attack'. Second IEEE International Conference on Sustainable Energy and Intelligent System (SEISCON 2011).

[16] Wooguil, P; Youngrok, C; Sunki, Y. 'High accessible virtual keyboards for preventing keylogging'. Eighth IEEE International Conference on Ubiquitous and Future Networks (ICUFN), Vienna, Austria, 2016. Doi: 10.1109/ ICUFN.2016.7537017.

[17] Yewale, A; Singh, M. 'Malware detection based on opcode frequency'. IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, India, 2016. DOI: 10.1109/ ICACCCT.2016.7831719.

[18] Tasabeeh, A; Omer, A; Eldewahi A. 'Random multiple layouts: keyloggers prevention technique'. Conference of Basic Sciences and Engineering Studies (SGCAC), Khartoum, Sudan, 2016. DOI: 10.1109/ SGCAC.2016.7457997.

[19] Li, S; Schmitz, R; 'A novel anti-phishing framework based on honeypots. IEEE eCrime Researchers Summit (eCRIME 2009).