



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**

**WINTER SEMESTER - 2022**

# **Keystroke Logging (Keylogging)**

## **A PROJECT REPORT**

**Submitted by**

**Name of the candidate(s)**

**Ayush thakur-19BCE0885**

**Shashwat Choudhary-19BCE0056**

**CSE3502 - Information Security Management—  
J Component**

**Faculty Name - SIVA SHANMUGAM**

# **Keystroke Logging(Keylogging)**

## **A PROJECT REPORT**

### **Submitted by**

**Name of the candidate(s)**

**Ayush thakur-19BCE0885**

**Shashwat Choudhary-19BCE0056**

## **ABSTRACT**

Keyboard capturing is the action of recording the keys stroke on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

It is used to track the users which logs keystrokes; uses log files to retrieve information. In this keylogger project, whenever the user types something through the keyboard, the keystrokes are captured and mailed to the mail id of admin without the knowledge of the user within the time set.

## **OBJECTIVE**

The purpose of this application is to keep tracks on every key that is typed through the keyboard and send it to the admin through the mail server in the time set or given.

## **INTRODUCTION**

Cybercriminals have devised many methods to obtain sensitive information from your endpoint devices. However, few of them are as effective as keystroke logging. Keystroke logging, also known as keylogging, is the capture of typed characters. The data captured can include document content, passwords, user ID's, and other potentially sensitive bits of information. Using this approach, an attacker can obtain valuable data without cracking into a hardened database or file server.

Keylogging presents a special challenge to security managers. Unlike traditional worms and viruses, certain types of keyloggers are all but impossible to detect.

## How Keyboards Work ?

A keyboard consists of a matrix of circuits overlaid with keys. This matrix of circuits, known as a key matrix, can differ between keyboard manufacturers. See Figure 1. However, the key codes that are sent through the keyboard interface to a specific operating system are always the same.



**Figure 1: Key Matrix**  
(Wilson and Tyson, 2008)

Let's step through Figure 2 to trace the path between keystrokes and operating system (OS) or application.

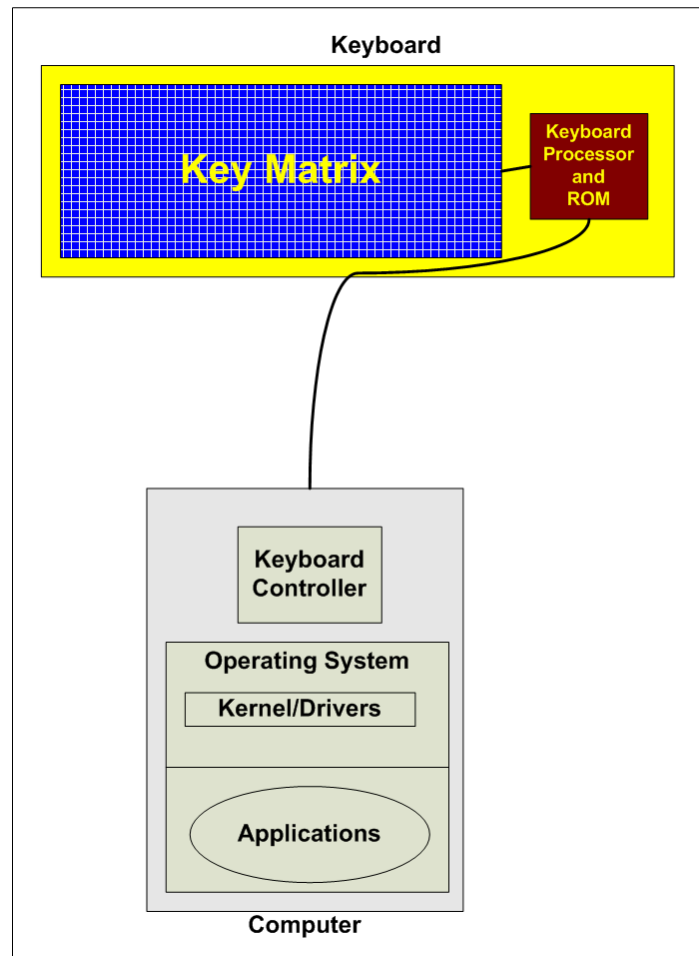


Figure 2: Keyboard/PC Layout

When the user presses a key, a circuit closes in the Key Matrix. The Keyboard Processor detects this event and captures the circuit location. Using a table stored in keyboard ROM, the processor translates the circuit location to a character or control code. Control codes are typically CTRL- or ALT- combinations.

The keyboard's memory buffer temporarily stores the translated character or control code and then sends it to the computer's keyboard interface. The computer's keyboard controller receives the incoming keyboard data and forwards it to the operating system. A keyboard driver is typically used to manage this part of the process. The operating system processes the keyboard input based on the current state of the OS and applications.

A keyboard interfaces with a computer via either a cable or a wireless connection. Common cable connections include the old PS2 standard and today's more common USB connector.

A popular wireless connection uses a 27 MHz signal with a range of about six feet. This type of connection is found in Microsoft and Logitech wireless keyboards. For solutions that require greater range, more robust wireless connections are available. These long range connections can reach about 100. One example is the wireless USB RF keyboard from Fentek Industries, Inc (<http://www.fentek-ind.com/rf-wireless-keyboard.htm#kbrftb100>).

With this high-level understanding of keyboard operation, let's move to a general discussion of how keystroke loggers work.

## How Keyloggers Work ?

Keyloggers are hardware or software tools that capture characters sent from the keyboard to an attached computer. They have both lawful/ethical and unlawful/unethical applications. Lawful applications include:

- Quality assurance testers analyzing sources of system errors;
- Developers and analysts studying user interaction with systems;
- Employee monitoring; and
- Law enforcement or private investigators looking for evidence of an ongoing crime or inappropriate behavior.

On the other side of the line between lawful and unlawful use, cybercriminals use keylogging technology to capture identities, confidential intellectual property, passwords, and any other marketable information.

Keyloggers fall into four categories: software, hardware, wireless intercept, and acoustic. Although they differ in how they are implemented and how information is captured, these four keystroke logging technologies have one thing in common. They store capture information in a log file. When software or hardware keyloggers are used, the log files are stored on the compromised machine. Remote capture technologies (i.e., wireless intercept and acoustic) typically store keystroke data on the collection device.

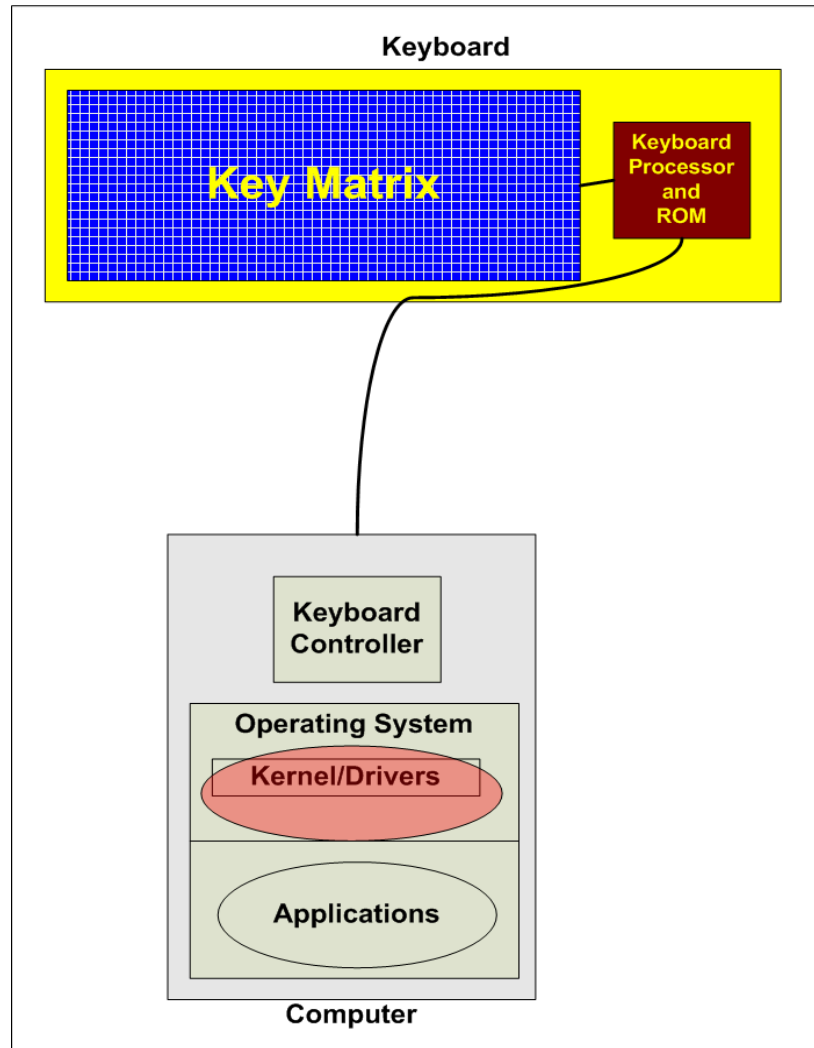
### *Software Keyloggers*

Software keyloggers capture keystroke information as it passes between the computer keyboard interface and the OS. They are implemented as traditional applications or kernel-based. In almost all malicious instances of this type of keylogger, users participated in some way in the software's installation.

Keylogging applications use a hooking mechanism (e.g., SetWindowsHookEx()) to capture keyboard data. Vendors often package solutions, like [Perfect Keylogger](#), as an executable or a DLL (Shetty, 2005).

Most kernel-based keyloggers are replacement keyboard device drivers. A portion of the logger resides in the OS kernel and receives data directly from the keyboard interface. It

replaces the kernel component that interprets keystrokes (Shetty, 2005). The red area in Figure 3 shows the location of a kernel-based keylogger in the keystroke-to-OS path.



**Figure 3: Kernel-based Keylogger**

Both types of software keyloggers intercept keyboard data, write a copy to a local—often encrypted—log file, and then forward the information to the operating system. To the unsuspecting user, everything looks normal.

Anti-malware, personal firewall, and host-based intrusion prevention (HIPS) solutions detect and remove application keyloggers. Kernel-based solutions are not so easy to find, although prevention controls like HIPS can prevent their implementation.

## **LITERATURE SURVEY**

[1] Keylogger technique

IEEE 2018

The forensic data is analyzed with the static method expected to obtain important information or data that can be used as digital evidence. Understanding the risks of Android third-party keyboards on user privacy and secrecy.

- Keyloggers -Android commander -Logger Application

The static forensic process is used to perform a detailed analysis phase and an app system review without being connected to the banking system over the network (offline). The research paper does not pertain to any modern softwares and applications.

## [2] Detecting cross-site scripting flaws in web applications

Journal of Computer Networks and Communications(2018)

CrawlerXSS performed better than other web vulnerability scanners in terms of accuracy and false-positive rate.

They prepare a background to identify any XSS or redirection vulnerabilities that could be initiated by using a maliciously crafted URL to introduce mischievous data into the DOM of inputted webpages (both statically and dynamically generated). If the data (or a manipulated form of them) are passed to one of the following application programming interfaces (APIs), the application may be vulnerable to XSS. We identify all uses of the APIs which may be used to access DOM data that can be controlled through crafted uniform resource locators (URLs). We created module checks for referrer header injection vulnerabilities by creating tags for all referrer headers to check whether there are altered requests. In this alteration, the module checks if the referrer is subject to XSS payload injection.

Needs more DOM-based features that could lead to detection of other code and server side injection vulnerabilities like SQL and cross-site request

## [3] Detecting Software Keyloggers with Dendritic Cell Algorithm.

IEEE (2010)

This method can differentiate the running keylogger process from the normal processes with a high detection rate and a low false alarm rate.

Dendritic Cell Algorithm implement a hook program to monitor API calls generated by running processes In the host and five signals to define the state of the system

Behaviour of keyloggers is the same as applications that hook the system message execution. All legitimate applications that hook the system would be detected as malicious.

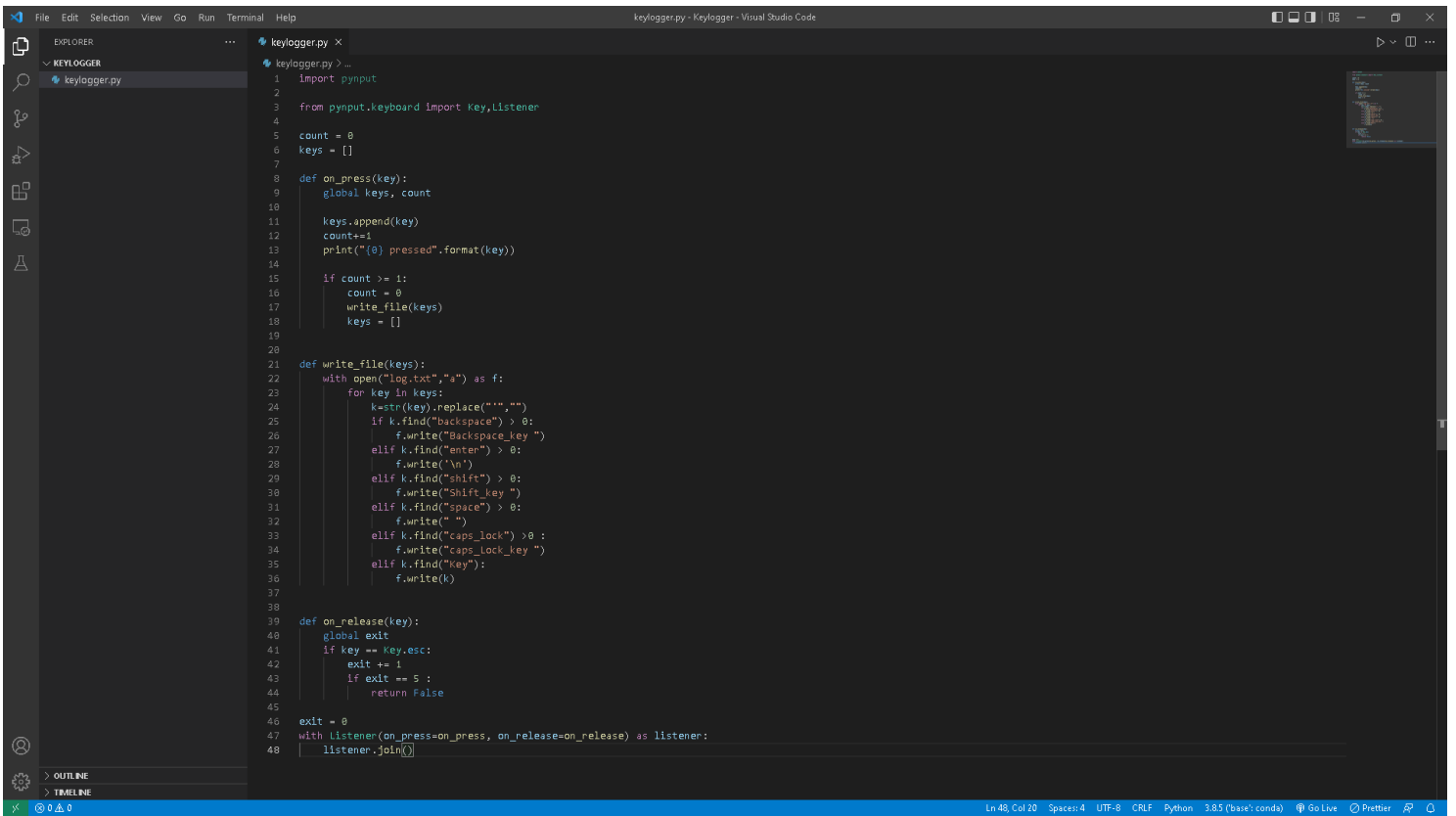
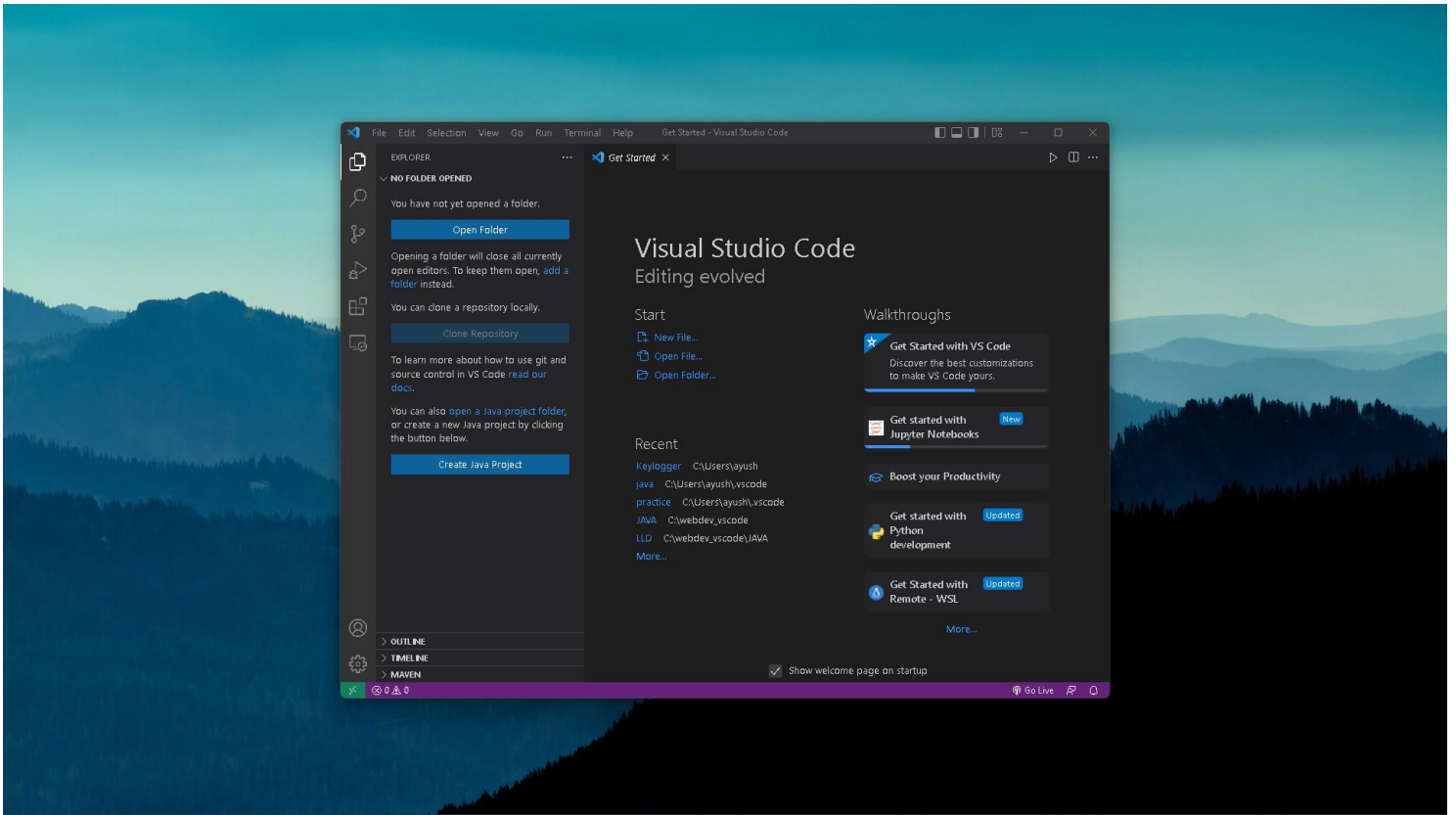
## [4] Detecting keyloggers based on traffic analysis with periodic Behaviour

Developing Keylogger for smartphones

Using the phone's motion sensors to detect vibrations from tapping the screen.

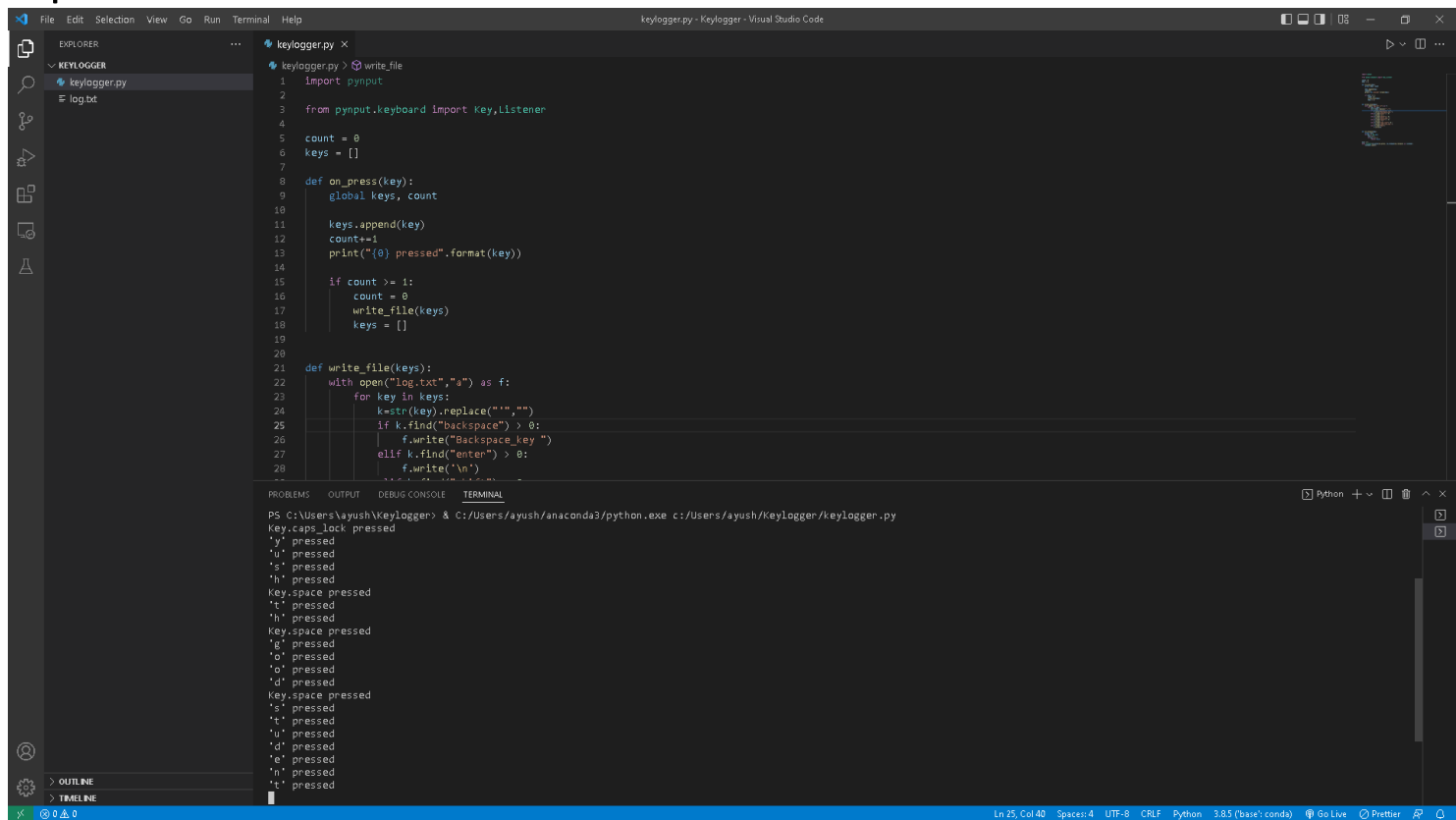
It is less accurate on a full alphanumeric keyboard. The motion sensor of the mobile phone should be good

# IMPLEMENTATION:

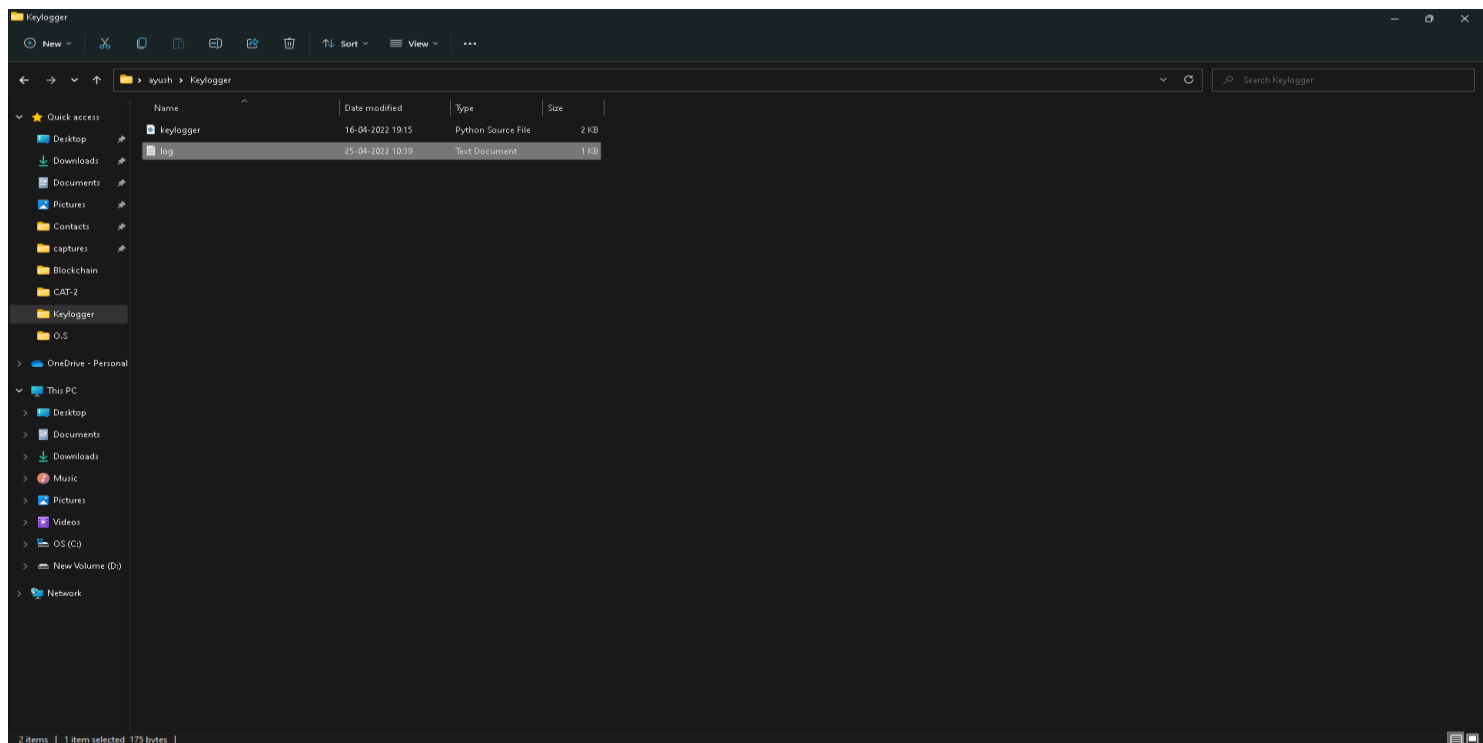




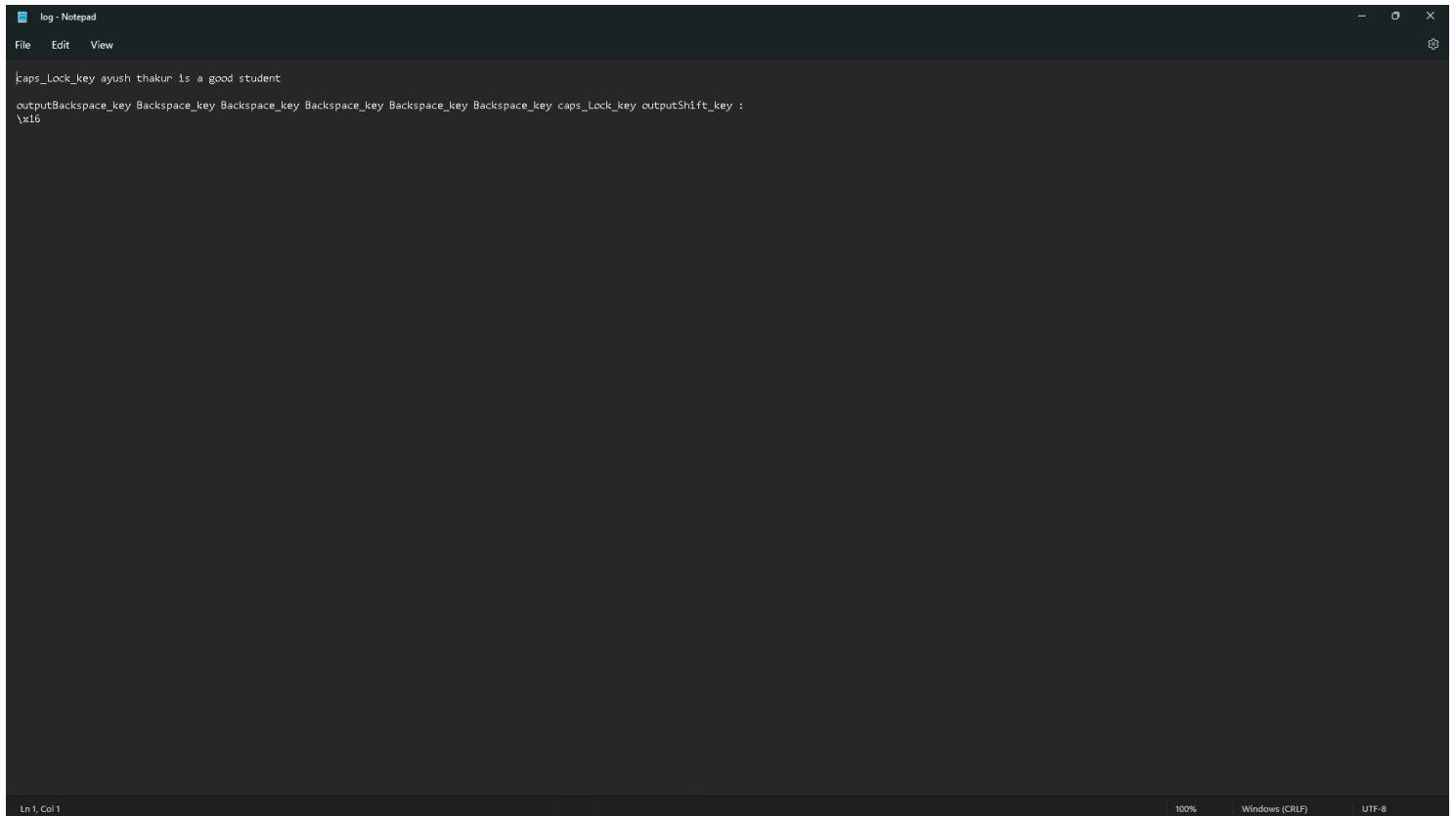
# Input:



# Log file generated-



Whatever we texted is in the log file-

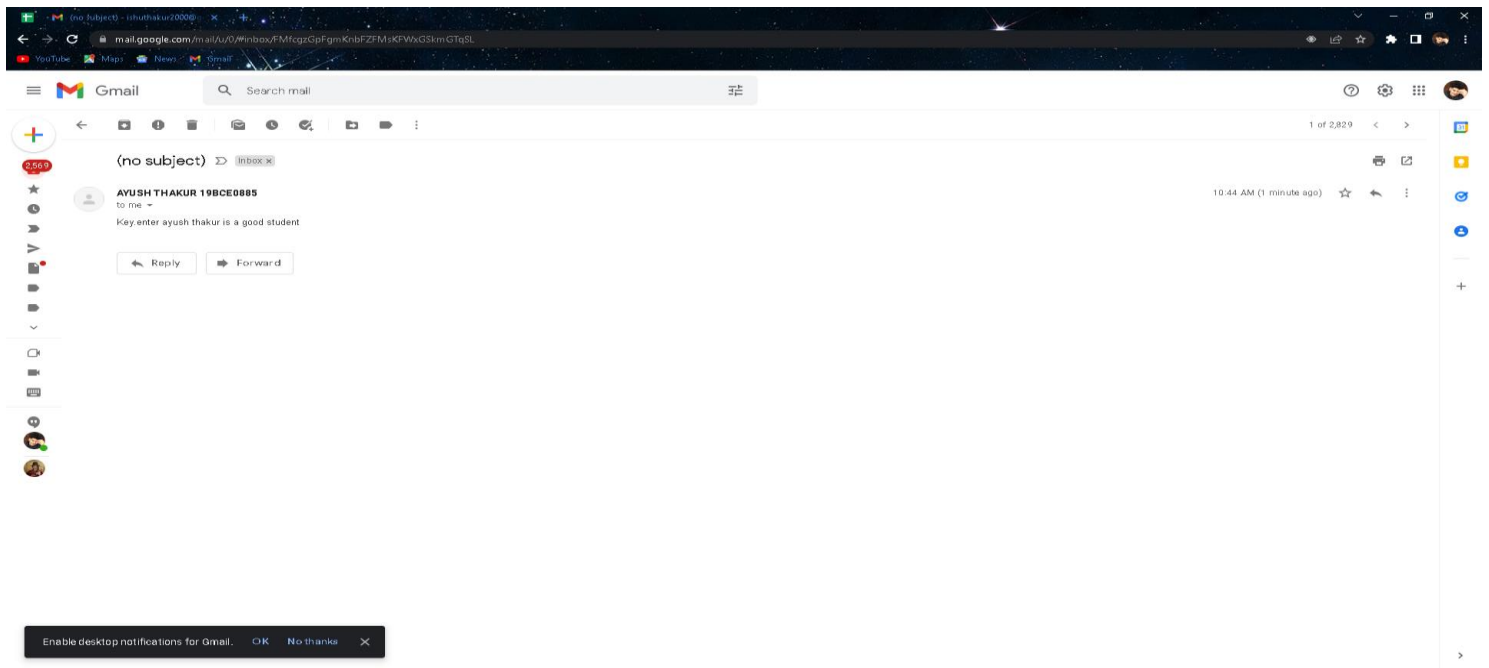


A screenshot of a Notepad window titled "log - Notepad". The window has a dark theme and a menu bar with "File", "Edit", and "View". The text content is as follows:

```
|caps_Lock_key ayush thakur is a good student  
outputBackspace_key Backspace_key Backspace_key Backspace_key Backspace_key Backspace_key caps_Lock_key outputShift_key :  
\\x16
```

The status bar at the bottom shows "Ln 1, Col 1", "100%", "Windows (CRLF)", and "UTF-8".

Got E-mail as the Output-



## Defending Against Keyloggers

Controls to defend against keyloggers are similar to those used to protect systems from other malware—particularly rootkits—including,

- Lock systems when not in use;
- Implement and enforce physical security controls;
- Enable safe-surfing
  - Use Web filtering to block access to known or suspected malicious sites;
  - Do not allow users local administrator access;
  - Deploy endpoint software policy controls (e.g., [WebSense CPM](#));
- Maintain a regularly updated and monitored anti-malware solution;
- Apply security patches as soon as reasonably possible;
- Purchase and use keylogger detection software to spot-check sensitive systems (e.g., [SnoopFree Privacy Shield](#)); and
- Allow only necessary protocols on endpoint devices, and block unauthorized sessions between endpoints and external sites.

These controls are reasonable and appropriate for most environments. However, security managers responsible for systems processing highly sensitive information should also consider the following:

- Screen-based virtual keyboards—Instead of entering data at the physical keyboard, users press keys displayed on their monitors. This bypasses the normal path taken by keyloggers, making it impossible for them to capture keystrokes.
- Automatic form filler programs.
- Encrypting keyboard input—Software solutions like GuardedID from StrikeForce encrypt keyboard input so keyloggers can't use it. See Figure 11. According to the vendor, the encryption solution protects against 95 to 96 percent of software related keylogger attacks. The downside is that this only works within a supported browser. StrikeForce is working on a version that works at the OS level.

If you believe one or more of your systems is compromised with a keylogger,

- Disconnect the system from the network and isolate it from physical access;
- If a software keylogger, locate the log file and retain it to identify potentially compromised information, re-image the system;
- If a hardware keylogger, remove it from the system and retain it to identify potentially compromised information;
- Change all passwords/PINS used by the users of the compromised system, including,
  - Local;
  - Network;
  - Web; and
- Notify management and recommend notification of affected,
  - Financial institutions;
  - Business partners;
  - Employees or customers if PII or ePHI might have been captured, in accordance with state or federal notification laws;

## **Conclusion**

Keystroke logging attacks bypass all other controls. They are easy to implement and manage, providing attackers with useful account, identity, and intellectual property information. On the other hand, they are useful investigative tools.

---

Controlling keylogging technology within your organization is no different than managing other threats and tools, requiring common sense and a layered defense. The key is to be aware they exist, understand how they're used, and implement ways to detect them, with keylogger detection and containment part of your incident response plan.

# REFERENCES

- Mosel, M. & Schrodel, P. (2008). *27MHz wireless keyboard analysis report aka "we know what you typed last summer."* Retrieved 3 April 2008 from [http://www.dreamlab.net/download/articles/27\\_Mhz\\_keyboard\\_insecurities.pdf](http://www.dreamlab.net/download/articles/27_Mhz_keyboard_insecurities.pdf)
- Shetty, S. (2005, April). *Introduction to spyware keyloggers*. SecurityFocus. Retrieved 27 March 2008 from <http://www.securityfocus.com/infocus/1829>
- StrikeForce (unknown). *GuardedID whitepaper*. Retrieved 4 April 2008 from [http://www.guardedid.com/PDF/GuardedID\\_white\\_paper.pdf](http://www.guardedid.com/PDF/GuardedID_white_paper.pdf)
- Wilson, T. V. & Tyson, J. (2008). *How computer keyboards work*. HowStuffWorks.com. Retrieved 25 March 2008 from <http://computer.howstuffworks.com/keyboard.htm>
- Zhuang, L, Zhou, F. & Tygar, J.D. (2005, November). *Keyboard acoustic emanations revisited*. Retrieved 3 April 2008 from <http://www.cs.berkeley.edu/~zf/papers/keyboard-ccs05.pdf>

**THANK YOU**

