KEYLOGGERS

PRISTILLA

Computer Science And Engineering

Universal College of Engineering and Technology

DEFINITION OF KEYLOGGERS

- Keyloggers are software programs or hardware devices designed to covertly monitor and record keystrokes made on a computer or mobile device.
- They capture and log all keyboard input, including text typed into applications, passwords, usernames, websites visited, and other sensitive information.
- Keyloggers can operate in the background without the user's knowledge, allowing unauthorized individuals to gather data stealthily.
- While some keyloggers may be installed for legitimate purposes, such as monitoring employee productivity or parental control, others are used for malicious activities such as identity theft or spying.
- Overall, keyloggers pose significant privacy and security risks when used without consent or for nefarious purposes.

PURPOSE OF KEYLOGGERS

- The purpose of keyloggers can vary depending on the intent of the individual or organization using them. Here are some common purposes for which keyloggers might be employed:
- **Surveillance and Monitoring:** Keyloggers can be used by employers to monitor employee activity on company-owned devices, ensuring compliance with company policies and detecting any unauthorized use. Similarly, parents might use keyloggers to monitor their children's online activities and ensure their safety.
- **Data Theft:** Malicious actors may use keyloggers to steal sensitive information such as usernames, passwords, credit card numbers, and other personal data entered by users. This information can then be used for identity theft, financial fraud, or other criminal activities.
- **Espionage and Surveillance:** Keyloggers can be deployed by individuals, organizations, or government agencies to gather intelligence on targets. This could include capturing sensitive communications, login credentials, or other confidential information.
- **Cybersecurity Testing:** Ethical hackers and security professionals may use keyloggers as part of penetration testing and security assessments to identify vulnerabilities in computer systems and networks. By simulating real-world attack scenarios, they can help organizations identify and mitigate potential security risks.
- **Law Enforcement:** In some cases, law enforcement agencies may use keyloggers as part of criminal investigations to gather evidence against suspects. This might involve monitoring communications, tracking online activities, or collecting evidence of criminal behavior.
- Overall, while keyloggers can serve legitimate purposes such as monitoring employee productivity or improving cybersecurity, they also pose significant privacy and security risks when used without consent or for malicious intent.

TYPES OF KEYLOGGERS

- **Software Keyloggers:** These are software programs installed on a computer or mobile device to monitor and log keystrokes. Software keyloggers can run in the background without the user's knowledge and typically store the captured data locally or transmit it to a remote server for later retrieval.
- **Hardware Keyloggers:** Hardware keyloggers are physical devices inserted between the keyboard and the computer or placed inline with the keyboard cable. They capture keystrokes directly from the keyboard hardware, making them difficult to detect through software-based security measures.
- **Wireless Keyloggers:** These keyloggers use wireless technologies such as Bluetooth or radio frequency (RF) to capture keystrokes remotely. They may be disguised as innocuous objects like USB chargers or dongles, allowing attackers to intercept keystrokes from a distance without physical access to the target device.

PREVENTION

- **Use Antivirus and Antimalware Software:** Install reputable antivirus and antimalware software on all devices and keep them updated regularly. These programs can detect and remove keyloggers and other types of malware.
- **Keep Software Updated:** Regularly update operating systems, applications, and software to patch known vulnerabilities that keyloggers might exploit. Enable automatic updates whenever possible.
- **Exercise Caution with Email Attachments and Downloads:** Avoid opening email attachments or downloading files from unknown or untrusted sources, as they may contain keyloggers or other malware.

DETECTION

- **Use Antivirus and Antimalware Scans:** Regularly scan your system with antivirus and antimalware software to detect and remove keyloggers and other malicious software.
- **Monitor System Performance:** Keep an eye on system performance, as keyloggers may cause noticeable slowdowns or unusual behavior. Monitor CPU and memory usage for any unexpected spikes that could indicate the presence of a keylogger.
- **Inspect Running Processes:** Use task manager or similar tools to inspect running processes and identify any unfamiliar or suspicious programs that may be running in the background.

THANK YOU