KEYLOGGERS

T.JEMILA

REG.NO 962721104401

UNIVERSAL COLLEGE OF ENGINEERING AND TECHNOLOGY

WHAT IS KEY LOGGER?

A keylogger is a type of software or hardware device that records every keystroke made by a user on a computer or mobile device. This includes capturing keyboard inputs such as passwords, usernames, messages, and other sensitive information. Keyloggers can be used for various purposes, such as monitoring computer activity, parental control, or in malicious activities like stealing confidential information.

TYPES OF KEYLOGGER

- A software keylogger is a form of malware that infects your device and, if programmed to do so, can spread to other devices the computer comes in contact with. While a hardware keylogger cannot spread from one device to another, like a software keylogger, it transmits information to the hacker or hacking organization, which they will then use to compromise your computer, network, or anything else that requires authentication to access

SOFTWARE KEYLOGGER

- Software keyloggers consist of applications that have to be installed on a computer to steal keystroke data. They are the most common method hackers use to access a user’s keystrokes.
- A software keylogger is put on a computer when the user downloads an infected application. Once installed, the keylogger monitors the keystrokes on the operating system you are using, checking the paths each keystroke goes through. In this way, a software keylogger can keep track of your keystrokes and record each one.
- After the keystrokes have been recorded, they are then automatically transferred to the hacker that set up the keylogger. This is done using a remote server that both the keylogger software and the hacker are connected to. The hacker retrieves the data gathered by the keylogger and then uses it to figure out the unsuspecting user’s passwords.
- The passwords stolen using the key logger may include email accounts, bank or investment accounts, or those that the target uses to access websites where their personal information can be seen. Therefore, the hacker’s end goal may not be to get into the account for which the password is used. Rather, gaining access to one or more accounts may pave the way for the theft of other data.

HARDWARE KEYLOGGER

- A hardware keylogger works much like its software counterpart. The biggest difference is hardware keyloggers have to be physically connected to the target computer to record the user's keystrokes. For this reason, it is important for an organization to carefully monitor who has access to the network and the devices connected to it.
- If an unauthorized individual is allowed to use a device on the network, they could install a hardware keylogger that may run undetected until it has already collected sensitive information. After hardware keystroke loggers have finished keylogging, they store the data, which the hacker has to download from the device.
- The downloading has to be performed only after the keylogger has finished logging keystrokes. This is because it is not possible for the hacker to get the data while the key logger is working. In some cases, the hacker may make the keylogging device accessible via Wi-Fi. This way, they do not have to physically walk up to the hacked computer to get the device and retrieve the data.

HOW ARE KEYLOGGERS CONSTRUCTED?

- The primary concept behind keyloggers is they must be placed between when a key gets depressed on a keyboard and when the information regarding that keystroke appears on the monitor. There are several ways to accomplish this.
- Some hackers use video surveillance to see the connection between the pressed keys and what appears on the monitor. A video camera with a view of the keyboard and the screen can be set up. Once it records a video of the keystrokes and the login or authentication screens the strokes have to get past, the hacker can play the video back, slow it down, and see which keys were pressed.
- An attacker can also put a hardware bug inside the keyboard itself. This would record each stroke made and send the information to be stored, either on a server or nearby physical device. It is possible for a keylogger to be placed within the wiring or inside the computer—as long as it is between the keyboard and the monitor.

- Additionally, keylogger software can be designed to intercept all input that comes from the keyboard. This can be done using a few different methods:
- The driver that facilitates the interaction between the keyboard and the computer can be replaced with one that logs each keystroke.
- A filter driver can be positioned within the keyboard stack.
- Kernel functions, which use similarities between data to assist machine learning, can be intercepted by software keyloggers and then used to derive the necessary keystrokes to perform authentication functions.
- The functions of the dynamic link library (DLL), which stores code used by more than one program, can be intercepted.

- The software, which is recognized as a form of spyware, is built using a few different methods. Here are the most common:
- A system hook, which is a technique for altering the operating system’s behavior, is used to intercept each notification generated whenever a key is pressed. This kind of software is typically built using the coding language C.
- A cyclical information request is set up that gathers information from the keyboard. These kinds of keyloggers are typically written using Visual Basic or Borland Delphi.
- A filter driver is written in C and installed inside the computer.
- As a sort of defense mechanism, some keyloggers, referred to as rootkits, have the ability to disguise themselves to slip manual or antivirus detection. They either mask in user mode or kernel mode.

HOW TO DETECT A KEYLOGGER ?

- The simplest way to detect a keylogger is to check your task manager. Here, you can see which processes are running. It can be tough to know which ones are legitimate and which could be caused by keyloggers, but you can differentiate the safe processes from the threats by looking at each process up on the internet. In some cases, you may find a warning written by another user regarding a process, or several processes, that indicate keylogger activity.
- To access the task manager in Windows, right-click on the taskbar, and then choose "Task Manager" from the menu.
- In this window, each program under the Apps section are the ones in use by your computer, which will appear in windows on your screen. You will not see a keylogger in this section. However, you may be able to find one by looking through the Background processes section.
- Another good place to look for keyloggers is under the Startup tab. Keyloggers get set up to run all the time on a computer, and to do that, they need to be started up with the operating system. As you peruse the Startup list, look for anything you cannot remember installing yourself. If something seems out of place, click on its line and then click on the Disable button on the lower-right side of the window.
- You can also check for keyloggers by examining your computer's internet usage report. To access this in Windows, press the Windows button and "I" at the same time. This will bring you to the settings screen. Here, you should choose "Network & Internet," then "Data usage." A list of the programs that your computer is using to access the internet will appear. If anything seems suspicious or you simply do not recognize it, do a search to investigate what it is. It may be a keylogger.

THANK YOU