

Forum:[Hack Forums](#)

Thread: [DLL injector doesn't work twice \[C++\]](#)

HardStoN - July 17, 2020, 4:58 am

so i created a dll injector and a dll that displays a messagebox.

Then i tested it on csgo and it worked once but then it never worked again no matter what i did.

how can i fix it?

thanks for the help!

4Txe4y33C9zvNhMj - July 17, 2020, 10:07 am

Might want to post your sourcecode here.

HardStoN - July 17, 2020, 12:08 pm

INJECTOR

```
Code #include <iostream>
#include <Windows.h>
#include <string>
#include <fstream>
#include <TIHelp32.h>
```

```
using namespace std;
```

```
void error(const char* title, const char* msg) {
    MessageBox(0, (LPCSTR)msg, (LPCSTR)title, 0);
    exit(-1);
}
```

```
BOOL __stdcall GetProcessID(const char* window_title, DWORD &proc_id)
{
    HWND hwnd = FindWindow(NULL, (LPCSTR>window_title);
    if (hwnd == NULL)
        error("Finding window", "Couldn't find window");

    if (!GetWindowThreadProcessId(hwnd, &proc_id))
        error("Process ID", "Couldn't find process ID");

    cout << "PROCESS ID: " << proc_id << endl;
    return TRUE;
}
```

```
int main()
{
    DWORD proc_id = NULL;
    const char* window_title = "Spotify Free";
    const char* dllName = "Test.dll";
```

```

char dllPath[MAX_PATH];

if (!GetFullPathName(dllName, MAX_PATH, dllPath, nullptr))
    error("DLL search", "Couldn't find DLL");

GetProcessID(window_title, proc_id);
if (proc_id == NULL)
    error("Process ID", "Couldn't find process ID **ERROR**");

HANDLE h_process = OpenProcess(PROCESS_ALL_ACCESS, NULL, proc_id);
if (h_process == NULL)
    error("Process Handle", "Couldn't find process HANDLE");

void* allocated_memory = VirtualAllocEx(h_process, nullptr, sizeof(dllPath), MEM_RESERVE |
MEM_COMMIT, PAGE_READWRITE);
if (!allocated_memory)
    error("Allocated memory", "Bad allocated memory");

cout << "ALLOCATED MEMORY addr: " << allocated_memory << endl;

if (!WriteProcessMemory(h_process, allocated_memory, dllPath, MAX_PATH, NULL))
    error("Writing process memory", "Error writing process memory");

HANDLE h_thread = CreateRemoteThread(h_process, nullptr, NULL,
LPTHREAD_START_ROUTINE(LoadLibraryA), allocated_memory, NULL, nullptr);
if (h_thread == NULL)
{
    cout << GetLastError() << endl;
    error("Creating remote thread", "Error creating remote thread");
}
CloseHandle(h_process);
VirtualFreeEx(h_process, allocated_memory, NULL, MEM_RELEASE);
MessageBox(0, "Successfully injected!", "Success!", 0);
}

```

DLL:

Code // dllmain.cpp : Defines the entry point for the DLL application.

```
#include "pch.h"
```

```

BOOL APIENTRY DllMain( HMODULE hModule,
                      DWORD ul_reason_for_call,
                      LPVOID lpReserved
                      )
{
    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
        MessageBox(0, "Hello from inside CSGO!", "MaMan!", 0);
    case DLL_THREAD_ATTACH:
        MessageBox(0, "Hello from inside CSGO! - THREAD", "MaMan!", 0);
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
        break;
    }
}

```

```
}  
return TRUE;  
}
```

Xora - July 18, 2020, 12:13 am

You restarted CS:GO in-between your attempts at injecting, right?

HardStoN - July 18, 2020, 3:49 am

yes i did. everytime injection didnt work i closed the injector and csgo then opened up csgo again and the injector and ran the injector and still nothing works...

incognito04 - July 18, 2020, 9:56 am

You should use WaitForSingleObject before closing the threads handle. I've heard something about vac adding some protection around loadlibrary so that could be the case.

spiderfruit - July 18, 2020, 1:33 pm

(Jul 17, 2020 04:58 AM)HardStoN Wrote: [\[CITE\]](#) so i created a dll injector and a dll that displays a messagebox.

Then i tested it on csgo and it worked once but then it never worked again no matter what i did.

how can i fix it?

thanks for the help!

vac did indeed got recently updated

<https://github.com/danielkrupinski/OneByteLdr> this fella explains how and where also if you're looking for game hacking scene, this forum isn't the best choice

DanketyDank - July 19, 2020, 5:14 am

(Jul 18, 2020 01:33 PM)spiderfruit Wrote: [\[CITE\]](#) vac did indeed got recently updated

<https://github.com/danielkrupinski/OneByteLdr> this fella explains how and where also if you're looking for game hacking scene, this forum isn't the best choice

This. Also OP look at manual mapping. For a ghetto fix just inject your dll from windows subfolder lol