

Keygenning4newbies CrackMe 1 coded by tHE ANALYST

int_0x80_: iop

xylitol: o/

int_0x80_: dis, je commence tout juste le reverse sous windows

int_0x80_: je tente un crack me niveau facile

int_0x80_: tu peux m'aider / me guider ?

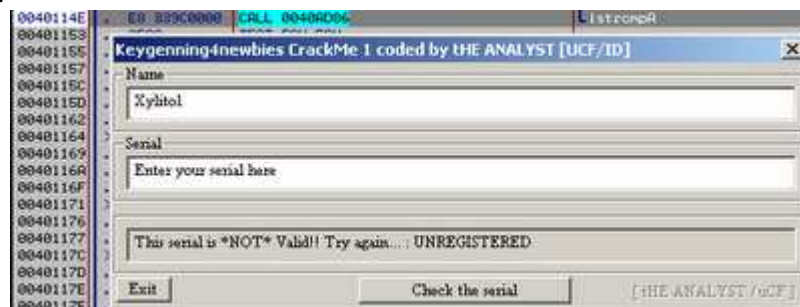
xylitol: heu wai si tu veut

int_0x80_: d'accord

int_0x80_: voilà celui que j'ia dl

int_0x80_: http://users.skynet.be/crisanar/defis/The_Analyst_k4n1.rar

et c'est parti.



routinz:

```
0040110C |> /0FBEB40D 48FF> /MOVX EAX, BYTE PTR SS:[EBP+ECX-B8]
00401114 |. |41 |INC ECX
00401115 |. |33C1 |XOR EAX, ECX
00401117 |. |03D8 |ADD EBX, EAX
00401119 |. |3B4D D8 |CMP ECX, DWORD PTR SS:[EBP-28]
0040111C |. ^\75 EE |JNZ SHORT 0040110C
0040111E |. |6BC0 06 |IMUL EAX, EAX, 6
00401121 |. |C1E3 07 |SHL EBX, 7
00401124 |. |03C3 |ADD EAX, EBX
```

bref pas bien compliqué, je te laisse cogiter sur les instructions

.asm:

.486

.model flat, stdcall

option casemap :none ; case sensitive

include base.inc

.data

format db "%X",0

.data?

szInput db 256 dup(?)

szOutput db 256 dup(?)

.code

start:

```

    invoke GetModuleHandle, NULL
    mov hInstance, eax
    invoke DialogBoxParam, hInstance, 101, 0, ADDR DlgProc, 0
    invoke ExitProcess, eax
; -----
DlgProc proc hWin :DWORD,
    uMsg :DWORD,
    wParam :DWORD,
    lParam :DWORD
    .if uMsg == WM_COMMAND
        .if wParam == IDC_OK
; -----
        invoke GetDlgItemText,hWin,1001,addr szInput,sizeof szInput
        MOV ESI,EAX
        lea EDX,szInput
        XOR ECX,ECX
L000:
        MOV AL,BYTE PTR DS:[EDX]
        INC ECX
        XOR EAX,ECX
        ADD EBX,EAX
        INC EDX
        CMP ECX,ESI
        JNZ L000
    @end:
    IMUL EAX,EAX,6
    SHL EBX,7
    ADD EAX,EBX
    invoke sprintf,addr szOutput,addr format,eax
    invoke SetDlgItemText,hWin,1002,addr szOutput
; -----
        .elseif wParam == IDC_IDCANCEL
            invoke EndDialog,hWin,0
        .endif
        .elseif uMsg == WM_CLOSE
            invoke EndDialog,hWin,0
        .endif
        xor eax,eax
        ret
DlgProc endp
end start

.inc:
include windows.inc
uselib MACRO libname
    include libname.inc
    includelib libname.lib

ENDM
uselib user32

```

uselib kernel32

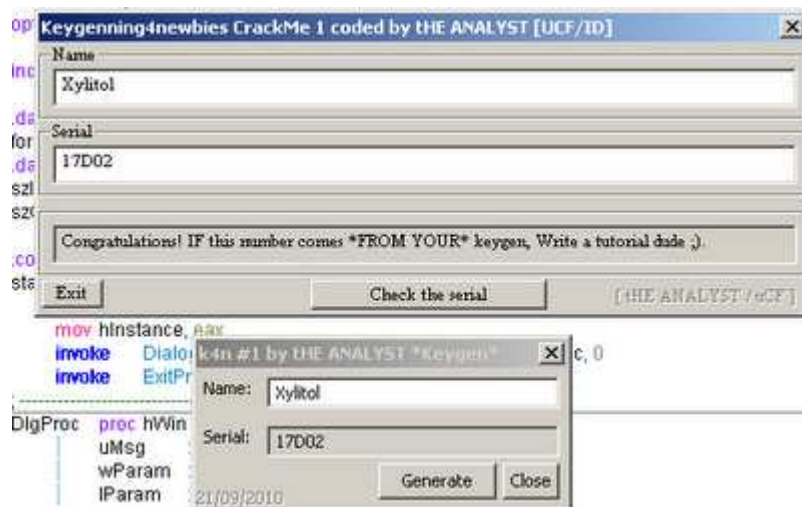
DlgProc PROTO :DWORD,:DWORD,:DWORD,:DWORD

IDC_OK equ 1003
IDC_IDCANCEL equ 1004

.data?
hInstance dd ? ;dd can be written as dword

.rc:
;This Resource Script was generated by WinAsm Studio.

```
#define IDC_OK 1003
#define IDC_CANCEL 1004
#define IDC_STATIC1006 1006
#define IDC_STATIC1007 1007
#define IDC_STATIC1008 1008
101 DIALOGEX 0,0,157,54
CAPTION "k4n #1 by tHE ANALYST *Keygen*"
FONT 8,"Tahoma"
STYLE 0x80c80880
EXSTYLE 0x00000008
BEGIN
    CONTROL "Generate",IDC_OK,"Button",0x10000001,77,37,50,14,0x00000000
    CONTROL "Close",IDC_CANCEL,"Button",0x10000000,130,37,24,14,0x00000000
    CONTROL "Xylitol",1001,"Edit",0x10000080,30,3,124,12,0x00000200
    CONTROL "",1002,"Edit",0x10000880,30,22,124,12,0x00000200
    CONTROL "Name:",IDC_STATIC1006,"Static",0x50000000,3,3,24,10,0x00000000
    CONTROL
"Serial:",IDC_STATIC1007,"Static",0x50000000,3,22,24,10,0x00000000
    CONTROL
"21/09/2010",IDC_STATIC1008,"Static",0x58000000,0,46,47,10,0x00000000
END
```



Code toi un keygen en C :)

Posted by Steven K at [21:59](#)

[Email This](#) [BlogThis!](#) [Share to Twitter](#) [Share to Facebook](#) [Share to Google Buzz](#)

Labels: [Keygenning4newbies](#) [CrackMe 1 coded by tHE ANALYST](#)