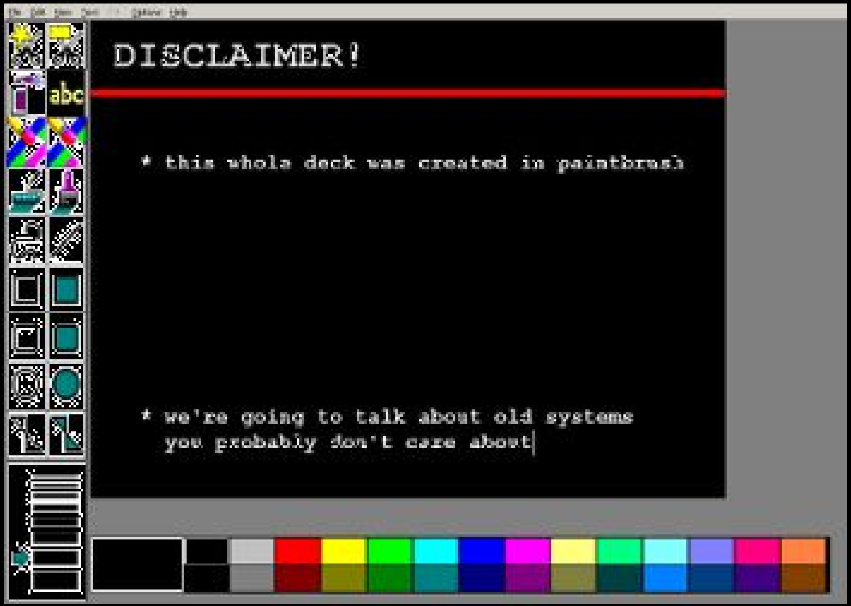
ANTIQUE EXPLOITATION

aka Terminator 3...
point one one
for workgroups

JON OBERHEIDE
jon@oberheide.org

DISCLAIMER!

* this whole deck was created in paintbrush



DISCLAIMER!

* this whole deck was created in paintbrush

* we're going to talk about old systems
  you probably don't care about

* we're going to talk about old systems
  you probably don't care about

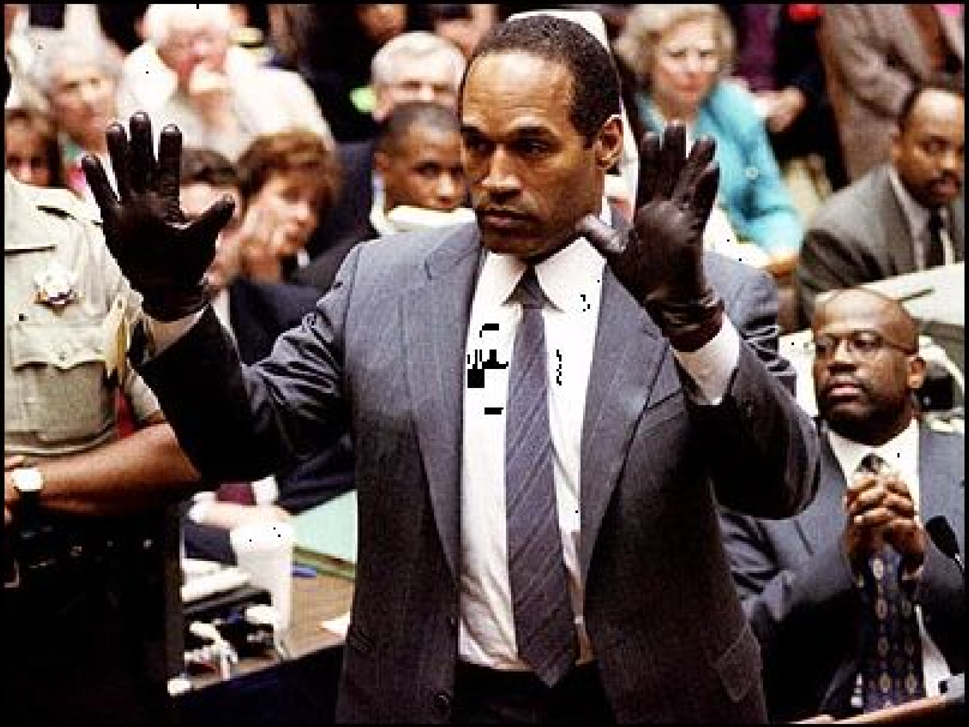
The Premise

* we've been sent back in time to eliminate the target

The Target

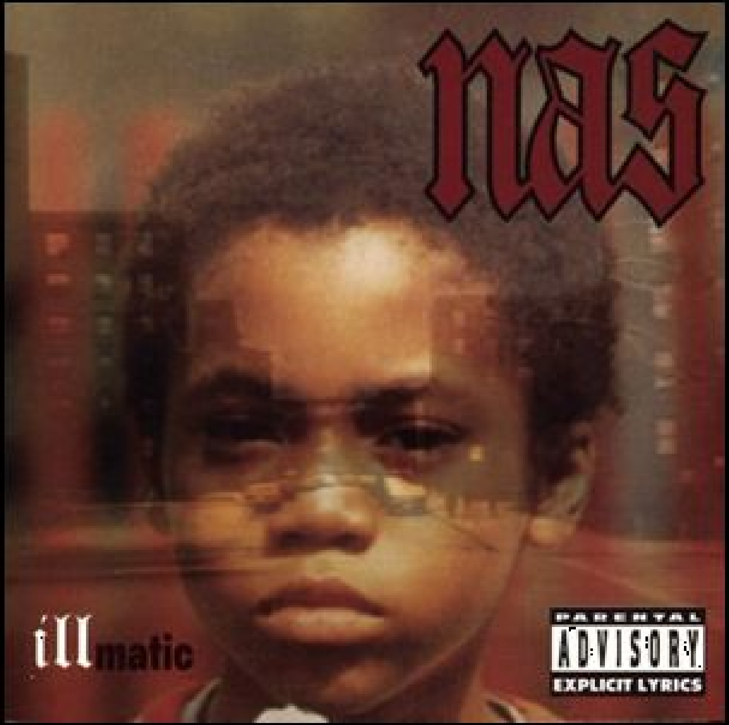
- * Junior Released in '94
- * THIS MOVIE MUST BE DESTROYED.
- * Set time machine to 1994!

1994



"if it doesn't fit, you must acquit"

1994

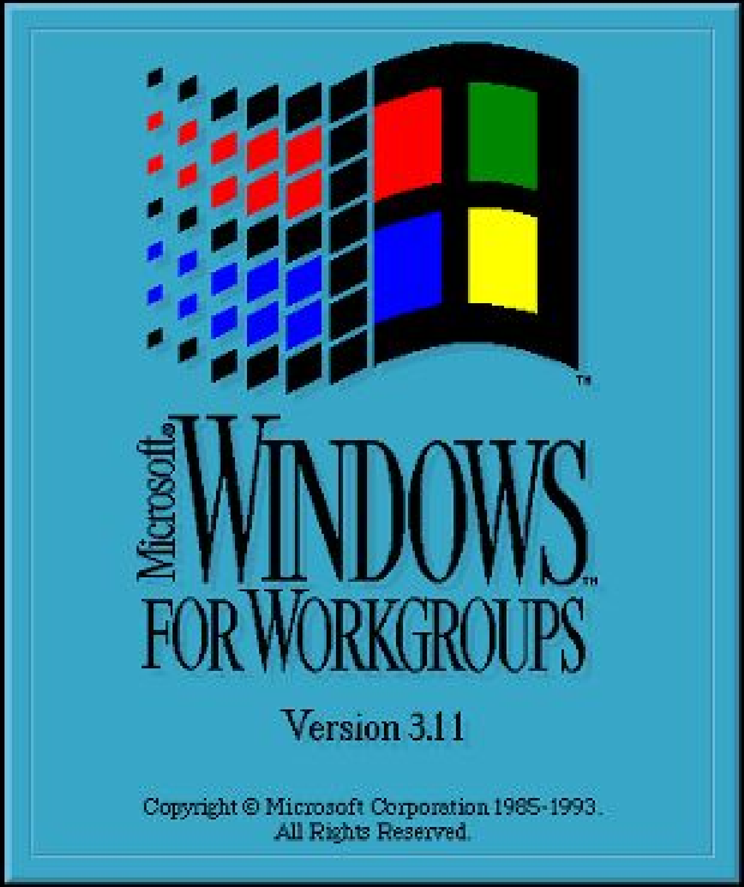


nas drops illmatic

1994

spencer pratt rumored to invent ROP

1994



Copyright © Microsoft Corporation 1985-1993.
All Rights Reserved.

windows 3.11 released!

Windows 3.11

* our attack target!

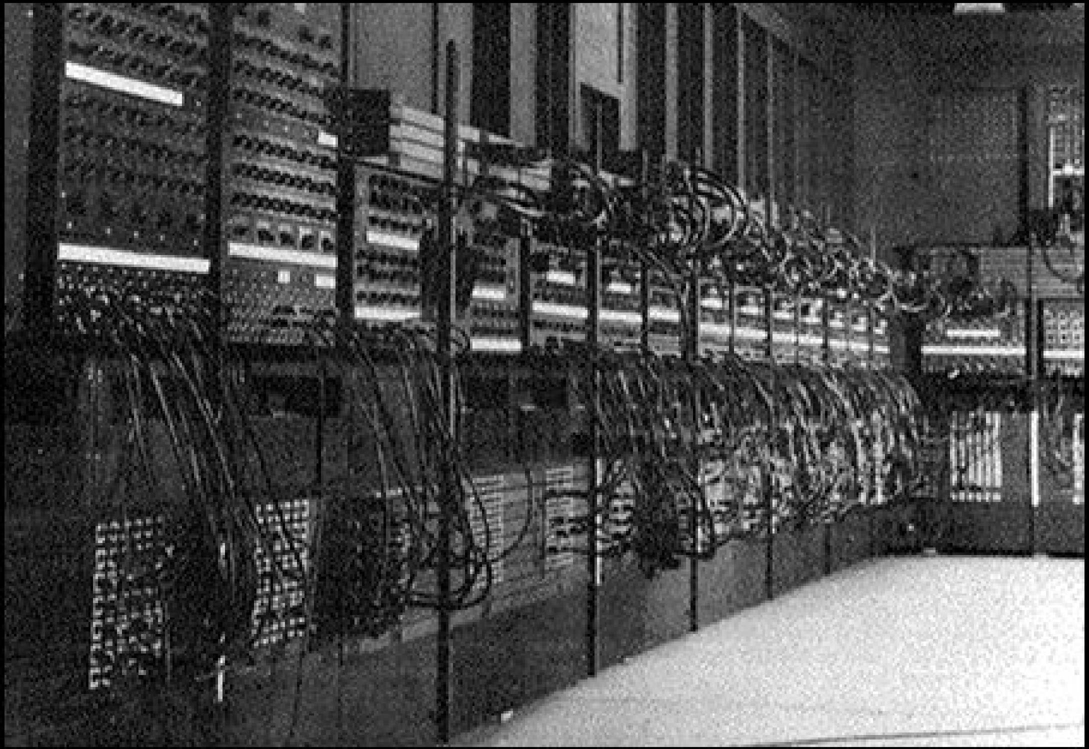
* 16-bit operating system

* but, 32-bit addressing in protected mode if 32-bit CPU (enhanced mode)

* WfW 3.11 had TCP/IP via Winsock!

Tools?

* we're in a whole different era



* can't use our normal tools to attack our target!

Debuggers?

not a chance!

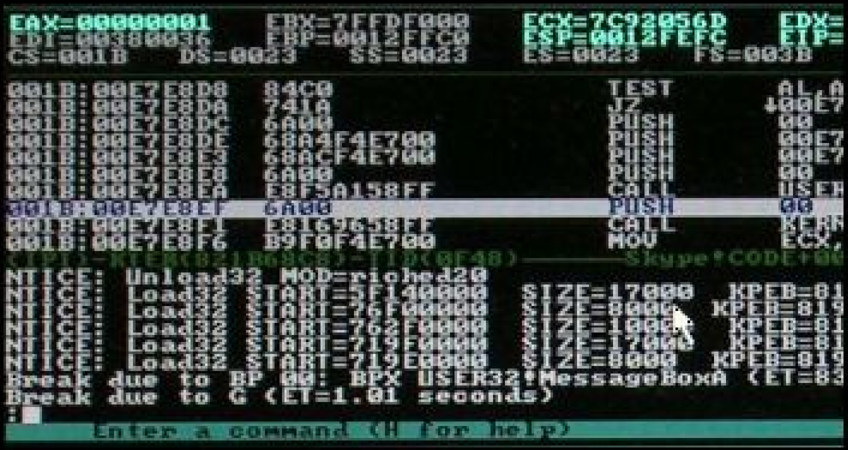
Debuggers?

Turbo Debugger for Windows

Version 5.0
Copyright (c) 1988,96
Borland International

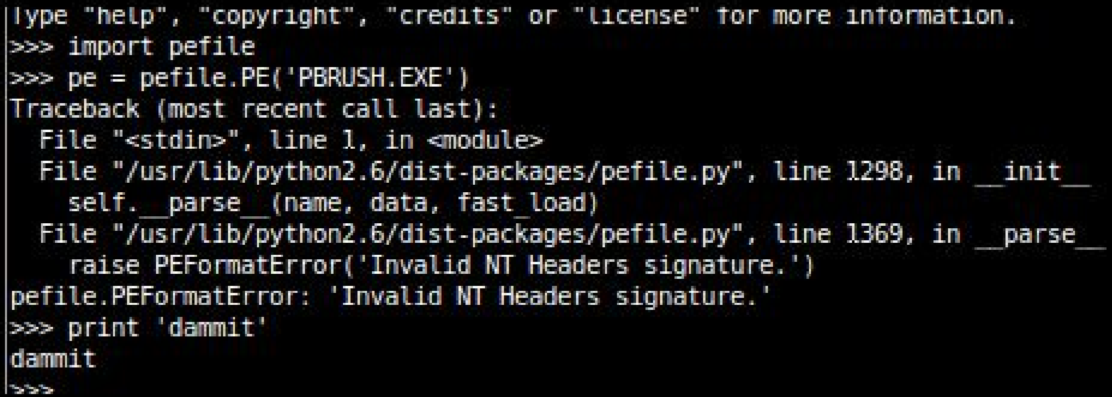
Borland
Turbo
Debugger

SoftICE

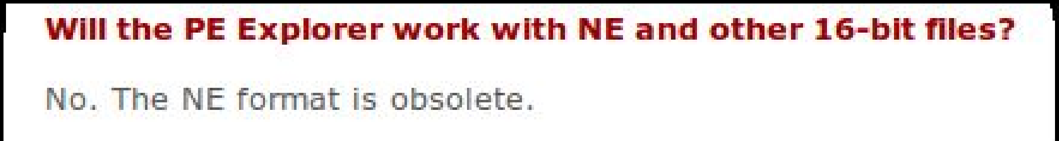


```
EAX=00000001   EBX=7FFDF000   ECX=7C92056D   EDX=
EDI=00380036   EBP=0012FFC0   ESP=0012FEFC   EIP=
CS=001B   DS=0023   SS=0023   ES=0023   FS=003B

001B:00E7E8D8  84C0                 TEST   AL,A
001B:00E7E8DA  741A                 JZ     ↓00E7
001B:00E7E8DC  6A00                 PUSH   00
001B:00E7E8DE  68A4F4E700           PUSH   00E7
001B:00E7E8E3  68ACF4E700           PUSH   00E7
001B:00E7E8E8  6A00                 PUSH   00
001B:00E7E8EA  E8F5A158FF           CALL   USER
001B:00E7E8EF  6A00                 PUSH   00
001B:00E7E8F1  E8169658FF           CALL   KERN
001B:00E7E8F6  B9F0F4E700           MOV    ECX,
(PI)-KTEB(821B68C8)-TID(0F48)————Skype!CODE+00
NTICE: Unload32 MOD=riched20
NTICE: Load32 START=5F140000 SIZE=17000  KPEB=81
NTICE: Load32 START=76F00000 SIZE=8000  KPEB=819
NTICE: Load32 START=762F0000 SIZE=1000  KPEB=81
NTICE: Load32 START=719F0000 SIZE=17000  KPEB=81
NTICE: Load32 START=719E0000 SIZE=8000  KPEB=819
Break due to BP 00: BPX USER32!MessageBoxA (ET=83
Break due to G (ET=1.01 seconds)
:
    Enter a command (H for help)
```

Reversing?



```
Type "help", "copyright", "credits" or "license" for more information.
>>> import pefile
>>> pe = pefile.PE('PBRUSH.EXE')
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "/usr/lib/python2.6/dist-packages/pefile.py", line 1298, in __init__
    self.__parse__(name, data, fast_load)
  File "/usr/lib/python2.6/dist-packages/pefile.py", line 1369, in __parse__
    raise PEFormatError('Invalid NT Headers signature.')
pefile.PEFormatError: 'Invalid NT Headers signature.'
>>> print 'dammit'
dammit
>>>
```



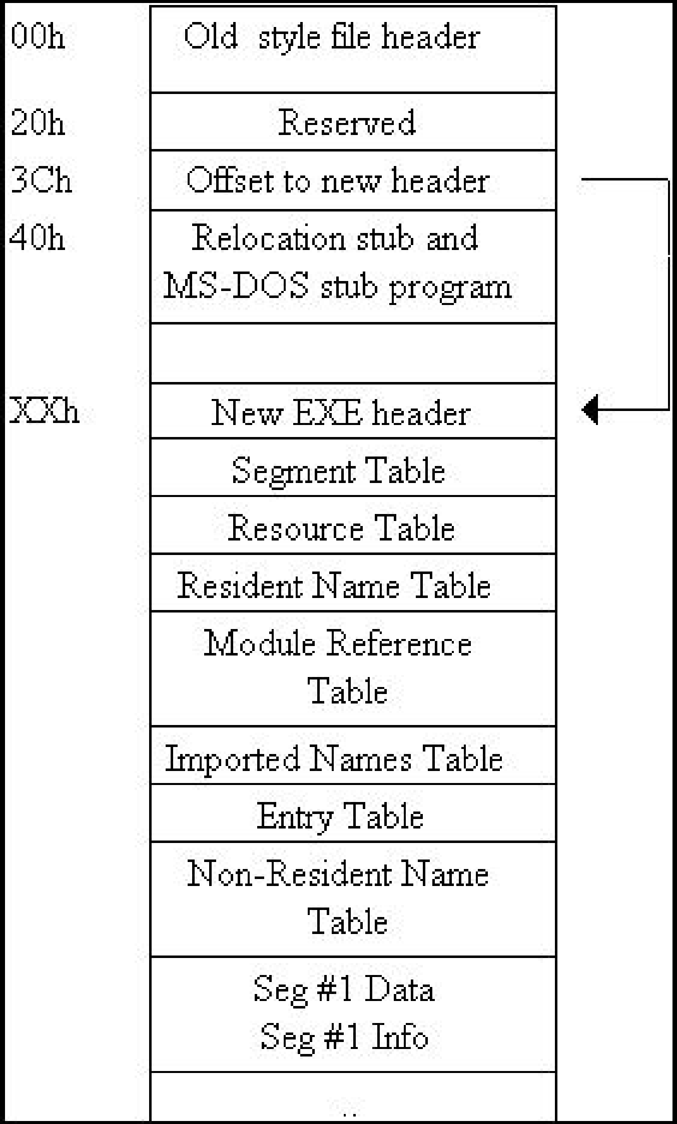
Will the PE Explorer work with NE and other 16-bit files?

No. The NE format is obsolete.

No love for NE!!!

NE: New Executable

- * exe format for 3.x
- * MZ -> NE -> PE
- * DOS and Win headers for compat err msgs
- * segmented executable layout



00h Old style file header

20h Reserved

3Ch Offset to new header

40h Relocation stub and MS-DOS stub program

XXh New EXE header

Segment Table

Resource Table

Resident Name Table

Module Reference Table

Imported Names Table

Entry Table

Non-Resident Name Table

Seg #1 Data
Seg #1 Info

..

Vuln Disco?

Sulley?

BFF?

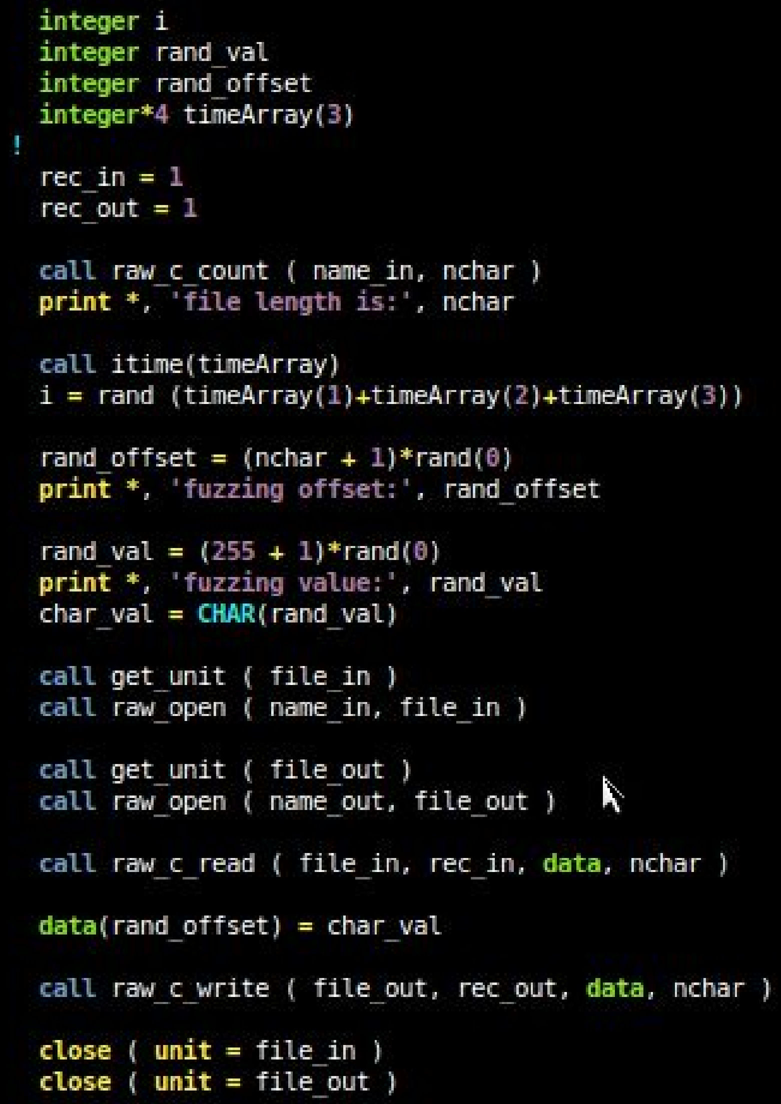
Peach?

Not fair!

Ancient Tools

we must paint ourselves with mud and fashion attack tools out of sticks

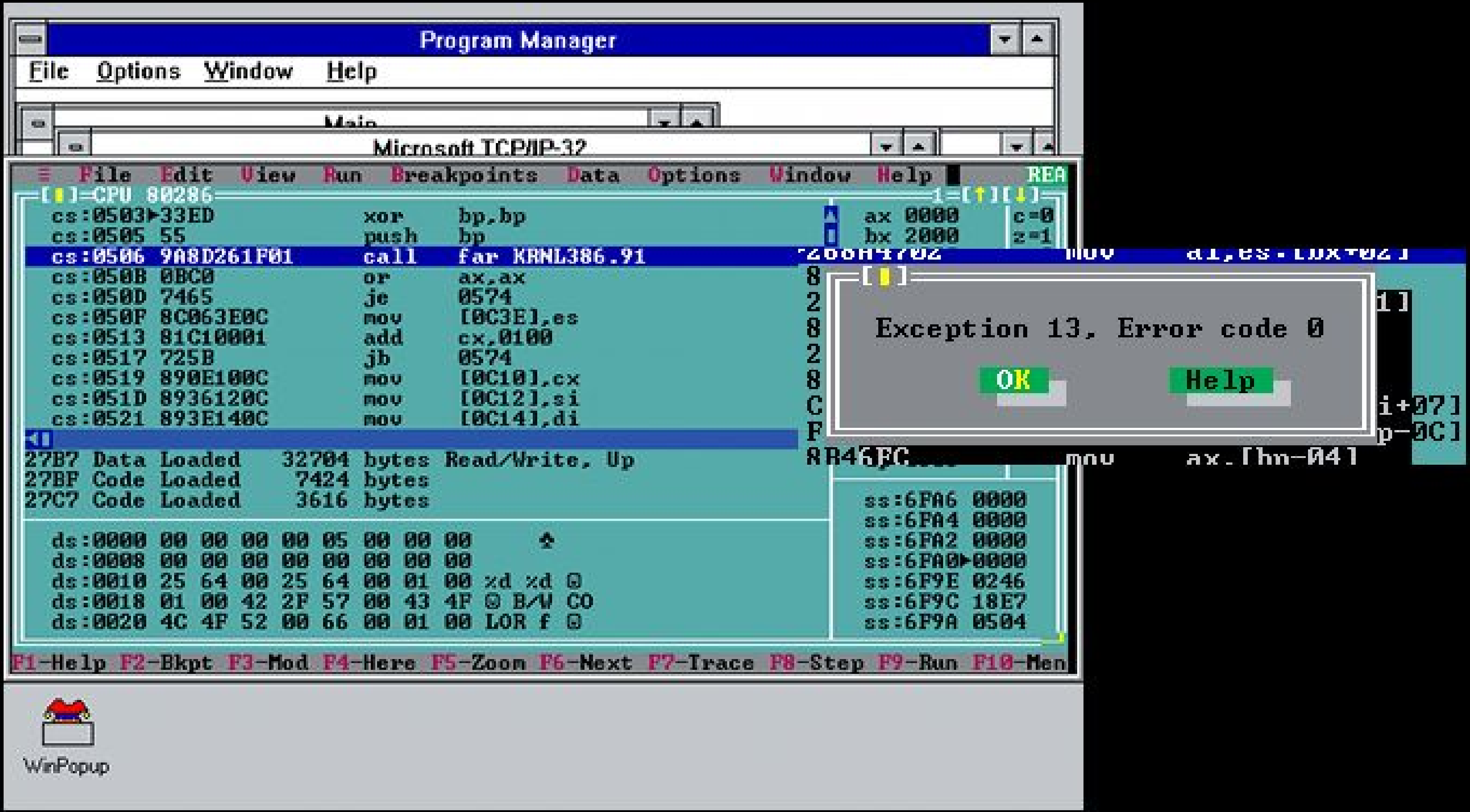
Fuzzing with FORTRAN



```
   integer i
   integer rand_val
   integer rand_offset
   integer*4 timeArray(3)
  !
   rec_in = 1
   rec_out = 1

   call raw_c_count ( name_in, nchar )
   print *, 'file length is:', nchar

   call itime(timeArray)
   i = rand (timeArray(1)+timeArray(2)+timeArray(3))

   rand_offset = (nchar + 1)*rand(0)
   print *, 'fuzzing offset:', rand_offset

   rand_val = (255 + 1)*rand(0)
   print *, 'fuzzing value:', rand_val
   char_val = CHAR(rand_val)

   call get_unit ( file_in )
   call raw_open ( name_in, file_in )

   call get_unit ( file_out )
   call raw_open ( name_out, file_out )

   call raw_c_read ( file_in, rec_in, data, nchar )

   data(rand_offset) = char_val

   call raw_c_write ( file_out, rec_out, data, nchar )

   close ( unit = file_in )
   close ( unit = file_out )
```

fuzz.f90

Triaging Samples


Program Manager
File Options Window Help
Main
Microsoft TCP/IP-32
≡ File Edit View Run Breakpoints Data Options Window Help
REA
F1-Help F2-Bkpt F3-Mod F4-Here F5-Zoom F6-Next F7-Trace F8-Step F9-Run F10-Men
OK
Help
WinPopup

```
[▮]=CPU 80286
  cs:0503▶33ED          xor     bp,bp                ax 0000   c=0
  cs:0505 55            push    bp                   bx 2000   z=1
  cs:0506 9A8D261F01    call    far KRNL386.91
  cs:050B 0BC0          or      ax,ax
  cs:050D 7465          je      0574
  cs:050F 8C063E0C      mov     [0C3E],es
  cs:0513 81C10001      add     cx,0100
  cs:0517 725B          jb      0574
  cs:0519 890E100C      mov     [0C10],cx
  cs:051D 8936120C      mov     [0C12],si
  cs:0521 893E140C      mov     [0C14],di
27B7 Data Loaded    32704 bytes Read/Write, Up
27BF Code Loaded     7424 bytes
27C7 Code Loaded     3616 bytes

  ds:0000 00 00 00 00 05 00 00 00      ♠           ss:6FA6  0000
  ds:0008 00 00 00 00 00 00 00 00                  ss:6FA4  0000
  ds:0010 25 64 00 25 64 00 01 00 %d %d ☺          ss:6FA2  0000
  ds:0018 01 00 42 2F 57 00 43 4F ☺ B/W CO         ss:6FA0▶0000
  ds:0020 4C 4F 52 00 66 00 01 00 LOR f ☺          ss:6F9E  0246
                                                   ss:6F9C  18E7
                                                   ss:6F9A  0504
```

```
Z66H4702     mov     al,es:[bx+02]
8B46FC       mov     ax,[bp-04]
```

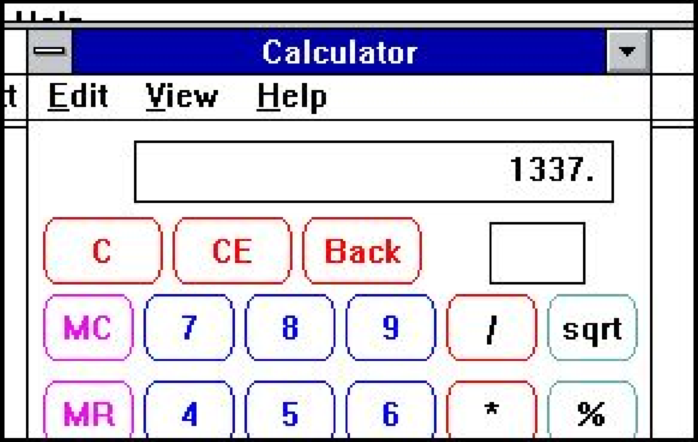
```
Exception 13, Error code 0
```

Exploit Nuances

* CreateProcess is Win32

* ShellExecute is acceptable though

* Lack of isolation -> lots o' crash



1337.

The Target

Other Random Bits

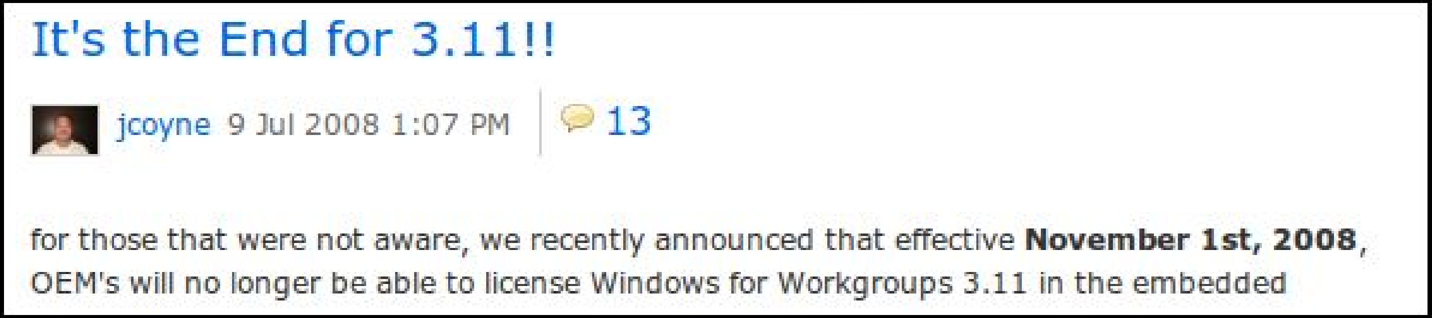
* ZDI did not meet my demands!
  (100k + accrued interest since '94)

* what were the devs thinking not opting in to DEP 10 years before it was introduced?!?

* demand EMET 2.0 compat from MS!

Legacy Systems

* legacy systems are still out there (see hdm's vxworks preso)



It's the End for 3.11!!

jcoyne 9 Jul 2008 1:07 PM | 13

for those that were not aware, we recently announced that effective **November 1st, 2008**, OEM's will no longer be able to license Windows for Workgroups 3.11 in the embedded

* win 3.11 just recently EOL'ed

* very popular for embedded platforms

Hasta La Vista, Baby

QUESTIONS?!?