ANTIQUE EXPLOITATION

aka Terminator 3...
point one one for workgroups

JON OBERHEIDE
jon@oberheide.org
DISCLAIMER!

* this whole deck was created in paintbrush

* 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

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?

Borland Turbo Debugger

SoftICE
Reversing?

```python
>>> 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
```
NE: New Executable

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

```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 )
```
Triaging Samples
Exploit Nuances

* CreateProcess is Win32
* ShellExecute is acceptable though
* Lack of isolation -> lots o' crash
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