PAKCON 2005

Malware: The Inside Story

Ahmad Elkhatib
Security Consultant
Pointsec Mobile Technologies

SeNe June 11th 2005

Agenda

- Malicious code prevalence
- The need to understand Malware
- Environment needed for analysis
- Reverse Engineering
- Conclusion

Definitions

- Malware : Malicious Software/Code
- Malicious Code : All and any programs (including macros and scripts) that are deliberately coded in order to cause an unexpected (and usually, unwanted) event on a PC or other system.

The menace to our networks

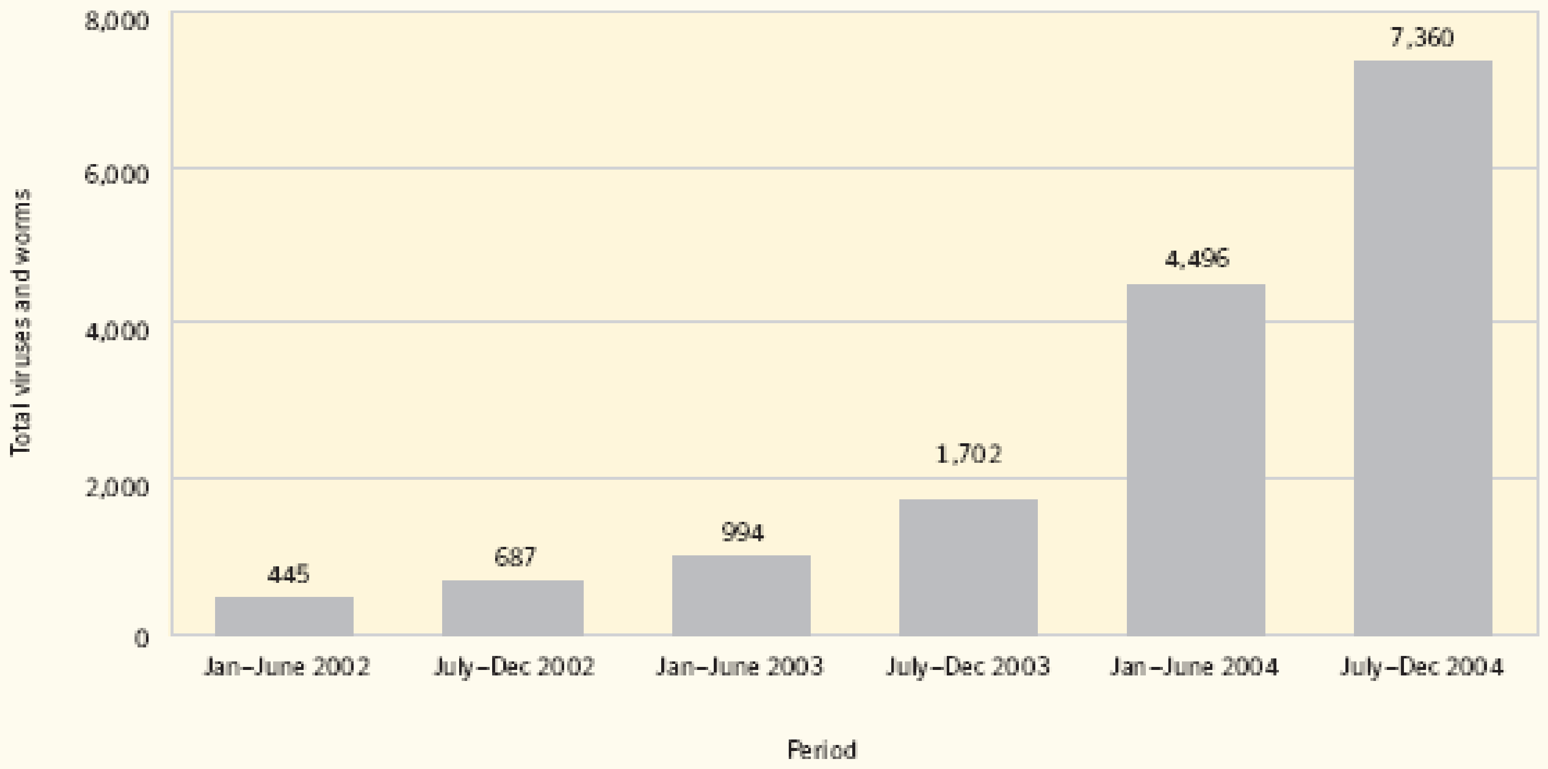


Figure 4. New Win32 viruses and worms by six-month period 2002–2004
Source: Symantec Corporation

The menace to our pockets

From Trend Micro, 16 Jan, 2004

Computer World Article :

“ It is estimated that PC Viruses cost businesses approximately $55 Billion in damages in 2003.

The same calculations in were done in 2002 and 2001, at $20-30 Billion and $13 Billion, respectively.”

What do we need to know ?

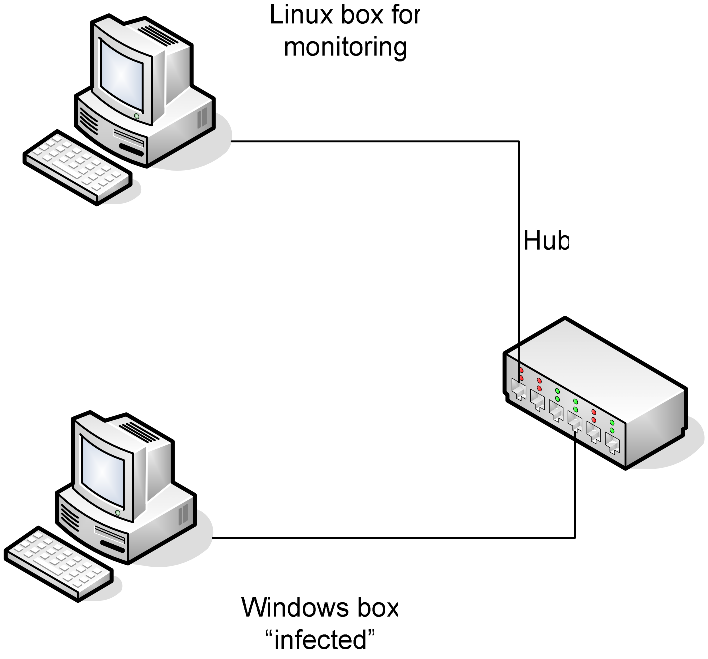
- When is the outbreak happening
- How to protect our assets against infection
- If infected how to respond
- If infected did I acquire a sample

How long do we have to wait ?

HH:MM	Vendor
06:51	Kaspersky
08:21	BitDefender
09:08	F-Secure
09:16	F-Prot
12:22	Sophos
13:06	TrendMicro
17:16	Esafe
26:11	McAfee
27:10	Symantec

Simple test lab setup

- EMC’s Vmware
- Symantec’s Norton Ghost
- Ethereal
- Nmap
- SNORT



- Behavioral analysis
- Code analysis

.. *you are only as good as your tools*

pointsec

Behavioral Analysis

- Packers
- Embedded text
- File system changes
- Registry changes
- Network ports
- Network shares

Packers

- Tools :
- PeID, UPX Unpacker

- Common Packers :
- UPX, TeLock, AsPack, PeSheild

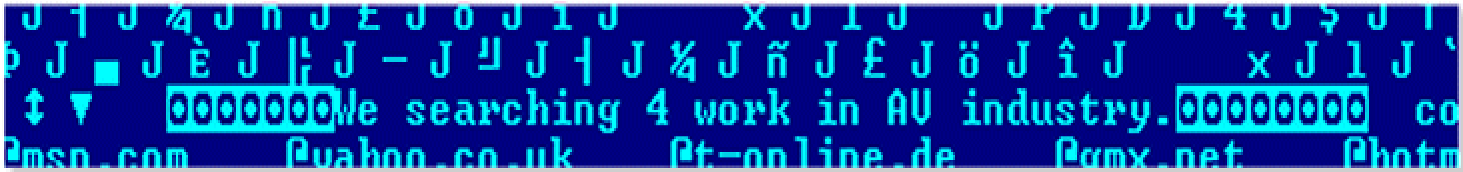
Embedded Text

- Packer information
- Passwords
- IP addresses
- IRC servers
- Mutices
- “Hidden Messages”

- Tools :

  BinText, UltraEdit,

  Binary Text Scan



```
J ┤ J ¼ J ñ J £ J ö J î J    x J 1 J    J P J D J 4 J $ J ⊤
þ J ■ J È J ╠ J − J ╝ J ┤ J ¼ J ñ J £ J ö J î J    x J 1 J `
↕ ▼   ◘◘◘◘◘◘◘We searching 4 work in AV industry.◘◘◘◘◘◘◘◘  co
@msn.com    @yahoo.co.uk    @t-online.de    @gmx.net    @hotm
```

Image Copyright © F-Secure Corporation

File system changes

- Tools :
- InCtrl, Winalysis, Installrite

- New files created
- New directories
- Network Shares

Registry changes

- Tools :
- InCtrl, RegMon, Winalysis

- Auto start entries
- Disable/Activate services

Network Ports

- Tools :
- Netstat, fport, nmap

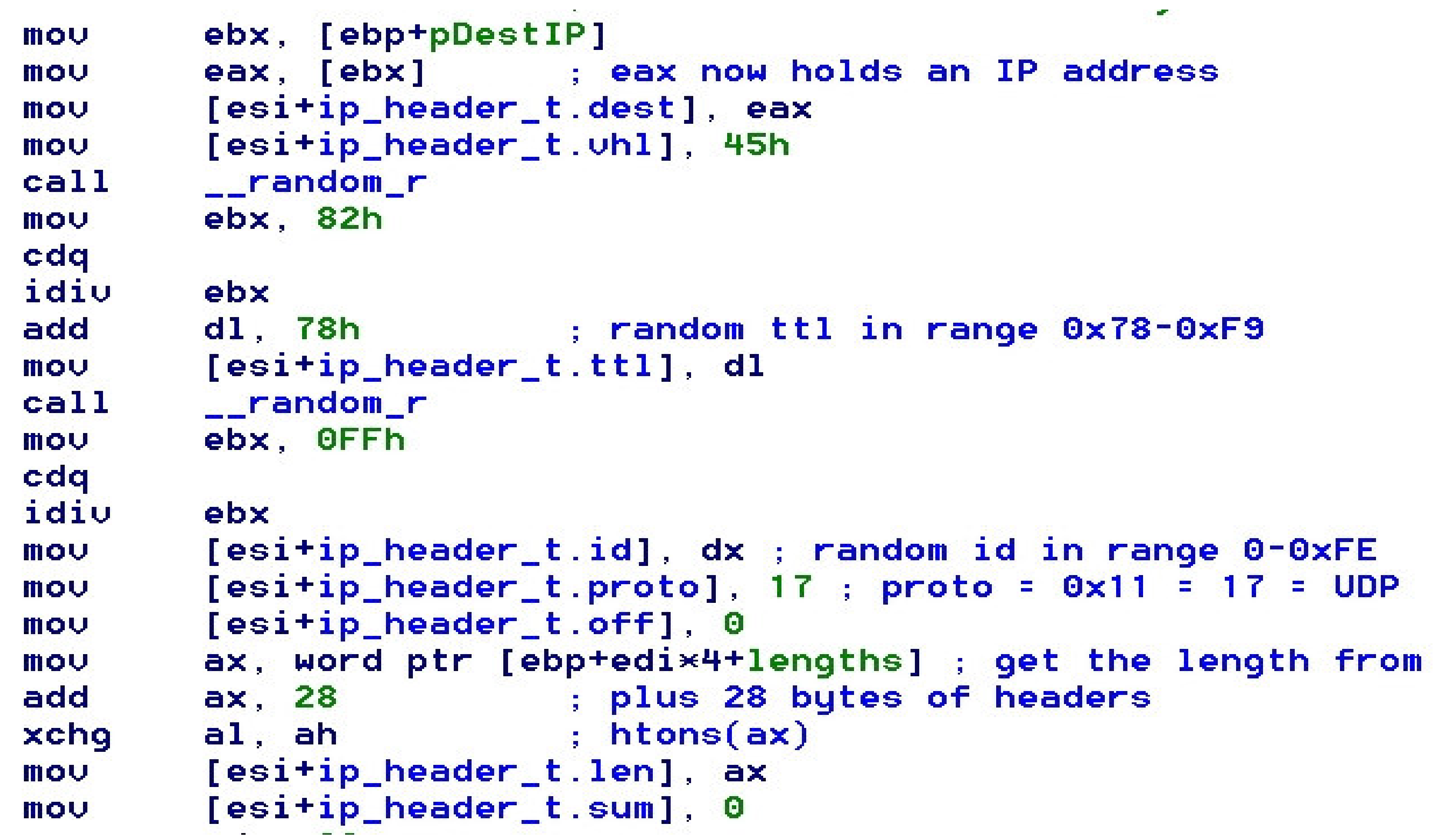
- Backdoor access
- Spreading mechanism
- Spam relay
- Mail server

Binary Code Analysis

- Tools :
- IDAPro, Ollydbg, SoftICE

- Step through assembly code
- Map functionality
- More in-depth understanding of code

Binary Code Analysis - IDAPro



```
mov     ebx, [ebp+pDestIP]
mov     eax, [ebx]      ; eax now holds an IP address
mov     [esi+ip_header_t.dest], eax
mov     [esi+ip_header_t.vhl], 45h
call    __random_r
mov     ebx, 82h
cdq
idiv    ebx
add     dl, 78h         ; random ttl in range 0x78-0xF9
mov     [esi+ip_header_t.ttl], dl
call    __random_r
mov     ebx, 0FFh
cdq
idiv    ebx
mov     [esi+ip_header_t.id], dx ; random id in range 0-0xFE
mov     [esi+ip_header_t.proto], 17 ; proto = 0x11 = 17 = UDP
mov     [esi+ip_header_t.off], 0
mov     ax, word ptr [ebp+edi*4+lengths] ; get the length from
add     ax, 28          ; plus 28 bytes of headers
xchg    al, ah          ; htons(ax)
mov     [esi+ip_header_t.len], ax
mov     [esi+ip_header_t.sum], 0
```

Other useful tools

- Multiple Vendor Scanner
- Virus Encyclopedias
- Google
- AVIEN.org (and other mailing lists)

Conclusion

- Antivirus is not enough to protect network
- IT personnel need basic skills to analyze viruses safely
- Behavioral analysis is within reach of most power users
- Code analysis is more complex but can be attained with practice

questions