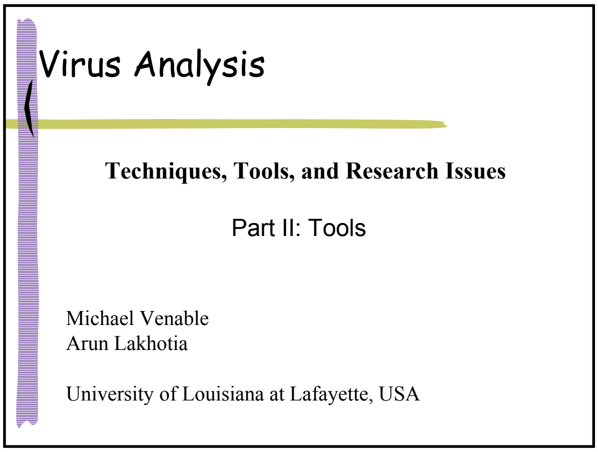


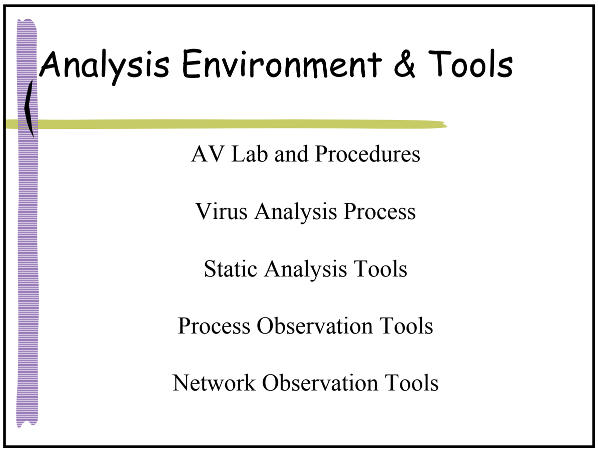
Virus Analysis

Techniques, Tools, and Research Issues

Part II: Tools

Michael Venable
Arun Lakhotia

University of Louisiana at Lafayette, USA



Analysis Environment & Tools

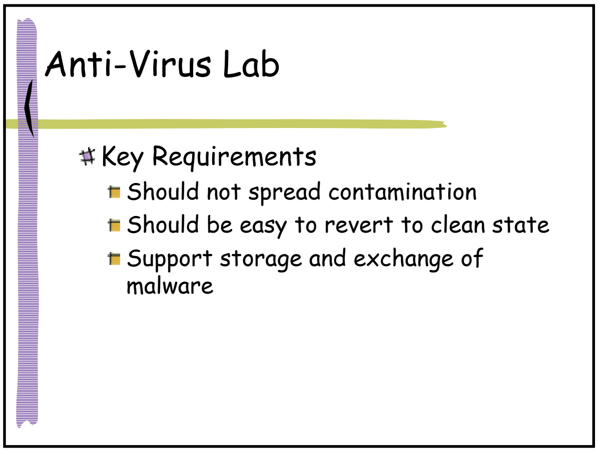
AV Lab and Procedures

Virus Analysis Process

Static Analysis Tools

Process Observation Tools

Network Observation Tools



Anti-Virus Lab

- Key Requirements
  - Should not spread contamination
  - Should be easy to revert to clean state
  - Support storage and exchange of malware

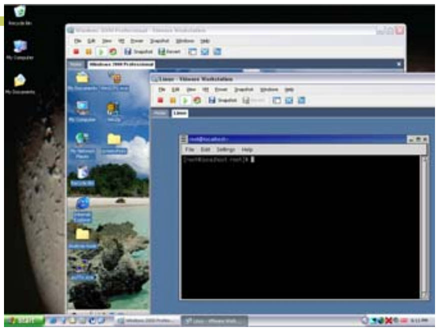
Procedures for handling malware

- Restrict access
- Save only disassembled files
- Rename file extensions
  - Protect against accidental double click
- Zip/compress and password protect
  - Protects against misappropriation
- Be cautious about exchanging malware
  - Preferably – Avoid sending malware
  - Send zip/password files, with notes of caution

Lab Alternatives

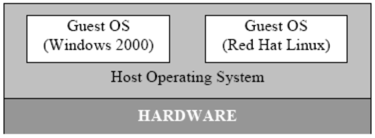
- Physically separate machines and network
  - Prevents accidental spread
  - Difficult to setup and tear down
  - Difficulty in accessing outside information during analysis
- Logically separate machines and network
  - Using virtualization technologies
  - Easy to setup and tear down
  - Must adhere to procedures to secure against accidental spread
  - Can create a sense of complacency

Example: Virtual Machines


Windows 2000 Professional - VMware Workstation
Linux - VMware Workstation
File Edit Settings Help
Start

VMWare

- Runs multiple operating systems simultaneously
- Creates network between host and guest systems


Guest OS (Windows 2000)
Guest OS (Red Hat Linux)
Host Operating System
HARDWARE

VMWare

- Snapshot
  - Can save copy of good state
- Self-contained files
  - Can transfer virtual machines to other PCs
  - .vmx – configuration file
  - .vmdk – image of hard disk

Virtualization Technologies

- Virtualizing a single host
  - VMWare (www.vmware.com)
    - USD 200/user
  - Virtual PC (Microsoft)
    - USD 129/user
  - Bochs (bochs.sourceforge.net)
    - Free. Emulates in software.
- Virtualizing a network
  - DETER/Emulab (www.isi.edu/deter)

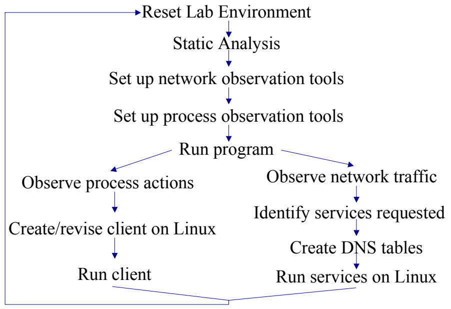
Attacking VMWare

- Detecting VMWare
  - Emulator remnants
    - Registry keys
    - Directories/files
  - Abnormalities
    - Predetermined hardware info
    - Possibly incorrectly emulated ports

Attacking VMWare

- Retaliation
  - Act benign
  - Communicate with VMWare
    - Enable/disable virtual devices
  - Spread to host (not yet seen)

Malware Analysis Process



Reset Lab Environment

Static Analysis

Set up network observation tools

Set up process observation tools

Run program

Observe process actions

Create/revise client on Linux

Run client

Observe network traffic

Identify services requested

Create DNS tables

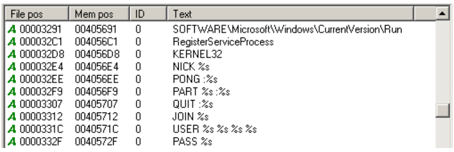
Run services on Linux

Static Analysis Tools

- BinText (www.foundstone.com)
  - Extracts strings from code
  - Free
- IDA Pro (www.DataRescue.Com)
  - Disassembler
  - USD 399/user
- UPX (upx.sourceforge.net)
  - UPX compression/decompression
  - Free
- MD5 Checksum

BinText

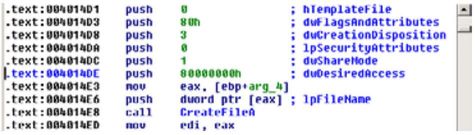
- Extracts strings from executables
- Reveals clues:
  - IRC Commands, SMTP commands, registry keys



File pos	Mem pos	ID	Text
A 00003291	00405691	0	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
A 000032C1	004056C1	0	RegisterServiceProcess
A 000032D8	004056D8	0	KERNEL32
A 000032E4	004056E4	0	NICK %s
A 000032EE	004056EE	0	PONG :%s
A 000032F9	004056F9	0	PART %s :%s
A 00003307	00405707	0	QUIT :%s
A 00003312	00405712	0	JOIN %s
A 0000331C	0040571C	0	USER %s %s %s %s
A 0000332F	0040572F	0	PASS %s

IDA Pro

- Disassembles executables into assembly instructions
- Easy-to-use interface
  - Separates subroutines, creates variable names, color-coded



```
.text:004014D1     push    0                      ; hTemplateFile
.text:004014D3     push    80h                    ; dwFlagsAndAttributes
.text:004014D8     push    3                      ; dwCreationDisposition
.text:004014DA     push    0                      ; lpSecurityAttributes
.text:004014DC     push    1                      ; dwShareMode
.text:004014DE     push    80000000h              ; dwDesiredAccess
.text:004014E3     mov     eax, [ebp+arg_4]
.text:004014E6     push    dword ptr [eax] ; lpFileName
.text:004014E8     call    CreateFileA
.text:004014ED     mov     edi, eax
```

UPX Decompression

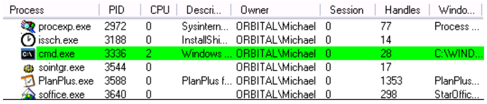
- Executable packer commonly used by virus writers
- Can compress wide range of files
  - Windows PE executables, DOS executables, DOS COM files, and many more
- To unpack:
  - `upx.exe -d -o dest.exe source.exe`

Process Observation Tools

- Process Explorer
  - Monitor processes
- FileMon
  - Monitor file operations
- RegMon
  - Monitor operations on registry
- Regshot
  - Take snapshot of registry and files
- ProcDump
  - Dump code from memory
- OllyDbg
  - Debugger

Process Explorer

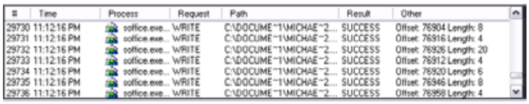
- Real-time monitoring
- Reports process name & id; Useful as filter with other tools
- Processes highlight in green when created
- Freely available from www.SysInternals.com



Process	PID	CPU	Descri...	Owner	Session	Handles	Windo...
procexp.exe	2972	0	Sysintern...	ORBITAL\Michael	0	77	Process ...
issch.exe	3188	0	InstallShi...	ORBITAL\Michael	0	14	
cmd.exe	3336	2	Windows ...	ORBITAL\Michael	0	28	C:\WIND...
sointgr.exe	3544	0		ORBITAL\Michael	0	17	
PlanPlus.exe	3588	0	PlanPlus f...	ORBITAL\Michael	0	1353	PlanPlus...
soffice.exe	3640	0		ORBITAL\Michael	0	298	StarOffic...

FileMon

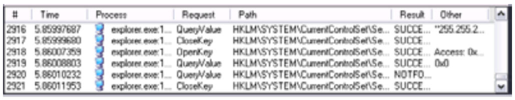
- Records all file accesses
- Freely available from www.SysInternals.com



#	Time	Process	Request	Path	Result	Other
29730	11:12:16 PM	soffice.exe...	WRITE	C:\DOCUME~1\MICHAE~2...	SUCCESS	Offset: 76904 Length: 8
29731	11:12:16 PM	soffice.exe...	WRITE	C:\DOCUME~1\MICHAE~2...	SUCCESS	Offset: 76916 Length: 4
29732	11:12:16 PM	soffice.exe...	WRITE	C:\DOCUME~1\MICHAE~2...	SUCCESS	Offset: 76926 Length: 20
29733	11:12:16 PM	soffice.exe...	WRITE	C:\DOCUME~1\MICHAE~2...	SUCCESS	Offset: 76912 Length: 4
29734	11:12:16 PM	soffice.exe...	WRITE	C:\DOCUME~1\MICHAE~2...	SUCCESS	Offset: 76920 Length: 6
29735	11:12:16 PM	soffice.exe...	WRITE	C:\DOCUME~1\MICHAE~2...	SUCCESS	Offset: 76946 Length: 8
29736	11:12:16 PM	soffice.exe...	WRITE	C:\DOCUME~1\MICHAE~2...	SUCCESS	Offset: 76958 Length: 4

RegMon

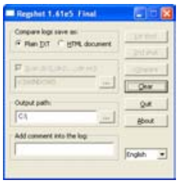
- Records all registry accesses
- Freely available from www.SysInternals.com



#	Time	Process	Request	Path	Result	Other
2916	5.85997687	explorer.exe:1...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	"255.255.2...
2917	5.85999680	explorer.exe:1...	CloseKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	
2918	5.86007359	explorer.exe:1...	OpenKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	Access: 0x...
2919	5.86008803	explorer.exe:1...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	0x0
2920	5.86010232	explorer.exe:1...	QueryValue	HKLM\SYSTEM\CurrentControlSet\Se...	NOTFO...	
2921	5.86011953	explorer.exe:1...	CloseKey	HKLM\SYSTEM\CurrentControlSet\Se...	SUCCE...	

RegShot

- Records modifications to registry and file system
- Does not detect read attempts
- Freely available from regshot.yeah.net

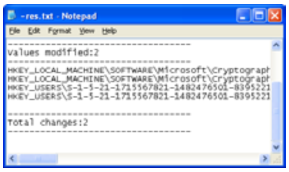


Compare logs save as: ● Plain TXT ○ HTML document

Output path: C:\

Add comment into the log:

English

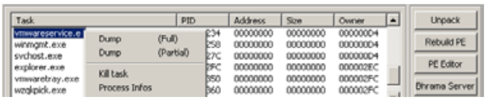


```
----------------------------------
Values modified:2
----------------------------------
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptograph
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptograph
HKEY_USERS\S-1-5-21-1715567821-1482476501-8395221
HKEY_USERS\S-1-5-21-1715567821-1482476501-8395221

----------------------------------
Total changes:2
----------------------------------
```

ProcDump

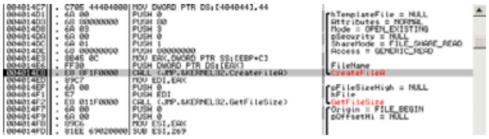
- Dumps process' code from memory
- Useful for polymorphic viruses



Task	PID	Address	Size	Owner
vmwareservice.e	234	00000000	00000000	000000D4
winmgmt.exe	258	00000000	00000000	000000D4
svchost.exe	27C	00000000	00000000	000000D4
explorer.exe	2FC	00000000	00000000	000002EC
vmwaretray.exe	350	00000000	00000000	000002FC
wzqkpick.exe	360	00000000	00000000	000002FC

OllyDbg

- Breakpoints
- Attach to process
- Can manipulate memory and registers
- Freely available at home.t-online.de/home/OllyDbg



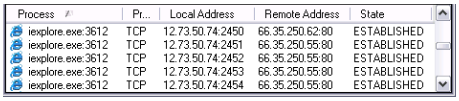
```
004014C7 . C705 44404000 MOV DWORD PTR DS:[404044],44
004014D1 . 6A 00         PUSH 0                                 ┌hTemplateFile = NULL
004014D3 . 68 80000000   PUSH 80                                │Attributes = NORMAL
004014D8 . 6A 03         PUSH 3                                 │Mode = OPEN_EXISTING
004014DA . 6A 00         PUSH 0                                 │pSecurity = NULL
004014DC . 6A 01         PUSH 1                                 │ShareMode = FILE_SHARE_READ
004014DE . 68 00000080   PUSH 80000000                          │Access = GENERIC_READ
004014E3 . 8B45 0C       MOV EAX,DWORD PTR SS:[EBP+C]           │
004014E6 . FF30          PUSH DWORD PTR DS:[EAX]                │FileName
004014E8 . E8 0F1F0000   CALL <JMP.&KERNEL32.CreateFileA>       └CreateFileA
004014ED . 89C7          MOV EDI,EAX
004014EF . 6A 00         PUSH 0                                 ┌pFileSizeHigh = NULL
004014F1 . 57            PUSH EDI                               │hFile
004014F2 . E8 011F0000   CALL <JMP.&KERNEL32.GetFileSize>       └GetFileSize
004014F7 . 6A 00         PUSH 0                                 ┌Origin = FILE_BEGIN
004014F9 . 6A 00         PUSH 0                                 │pOffsetHi = NULL
004014FB . 89C6          MOV ESI,EAX                            │
004014FD . 81EE 69020000 SUB ESI,269                            │
```

Network Observation Tools

- TCPView
  - Displays open network ports
- TDIMon
  - Monitors network activity
- Ethereal
  - Packet sniffer
- Snort
  - Packet sniffer

TCPView

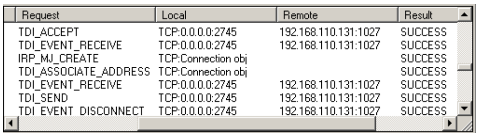
- Displays all open TCP and UDP endpoints
- Also displays process name
- Freely available from www.SysInternals.com



Process	Pr...	Local Address	Remote Address	State
iexplore.exe:3612	TCP	12.73.50.74:2450	66.35.250.62:80	ESTABLISHED
iexplore.exe:3612	TCP	12.73.50.74:2451	66.35.250.55:80	ESTABLISHED
iexplore.exe:3612	TCP	12.73.50.74:2452	66.35.250.55:80	ESTABLISHED
iexplore.exe:3612	TCP	12.73.50.74:2453	66.35.250.55:80	ESTABLISHED
iexplore.exe:3612	TCP	12.73.50.74:2454	66.35.250.55:80	ESTABLISHED

TDIMon

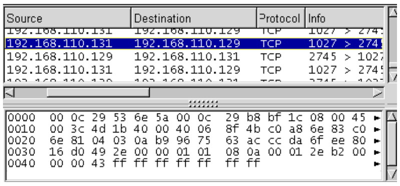
- Logs all network activity
- Does not log packet contents
- Freely available from www.SysInternals.com



Request	Local	Remote	Result
TDI_ACCEPT	TCP:0.0.0.0:2745	192.168.110.131:1027	SUCCESS
TDI_EVENT_RECEIVE	TCP:0.0.0.0:2745	192.168.110.131:1027	SUCCESS
IRP_MJ_CREATE	TCP:Connection obj		SUCCESS
TDI_ASSOCIATE_ADDRESS	TCP:Connection obj		SUCCESS
TDI_EVENT_RECEIVE	TCP:0.0.0.0:2745	192.168.110.131:1027	SUCCESS
TDI_SEND	TCP:0.0.0.0:2745	192.168.110.131:1027	SUCCESS
TDI_EVENT_DISCONNECT	TCP:0.0.0.0:2745	192.168.110.131:1027	SUCCESS

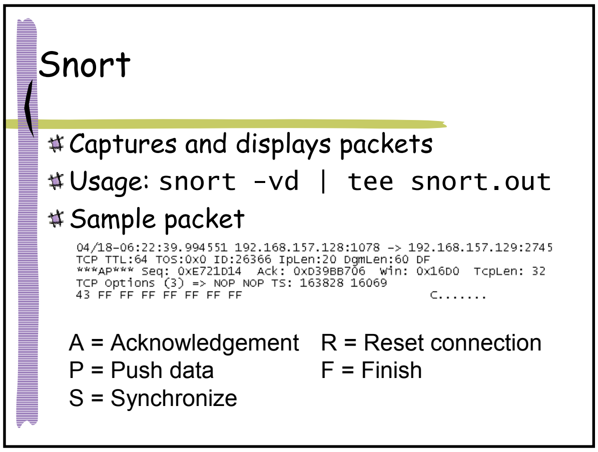
Ethereal

- Captures and displays packet contents
- Freely available from www.ethereal.com



Source	Destination	Protocol	Info
192.168.110.131	192.168.110.129	TCP	1027 > 274
192.168.110.131	192.168.110.129	TCP	1027 > 274
192.168.110.129	192.168.110.131	TCP	2745 > 102
192.168.110.131	192.168.110.129	TCP	1027 > 274

```
0000  00 0c 29 53 6e 5a 00 0c  29 b8 bf 1c 08 00 45
0010  00 3c 4d 1b 40 00 40 06  8f 4b c0 a8 6e 83 c0
0020  6e 81 04 03 0a b9 96 75  63 ac cc da 6f ee 80
0030  16 d0 49 2e 00 00 01 01  08 0a 00 01 2e b2 00
0040  00 00 43 ff ff ff ff ff  ff ff
```

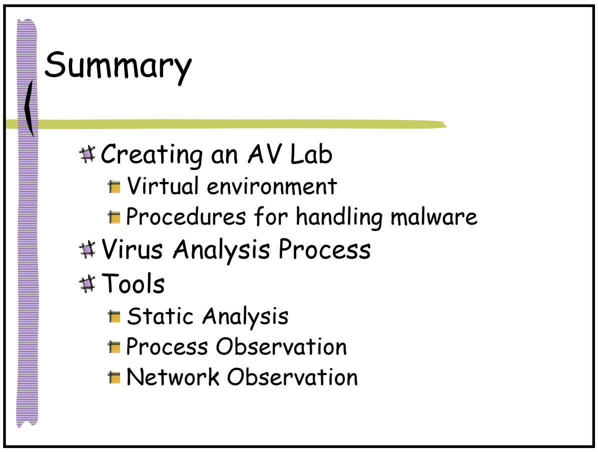


Snort

- Captures and displays packets
- Usage: `snort -vd | tee snort.out`
- Sample packet

```
04/18-06:22:39.994551 192.168.157.128:1078 -> 192.168.157.129:2745
TCP TTL:64 TOS:0x0 ID:26366 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0xE721D14  Ack: 0xD39BB706  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 163828 16069
43 FF FF FF FF FF FF FF                          C.......
```

A = Acknowledgement　R = Reset connection
P = Push data　F = Finish
S = Synchronize



Summary

- Creating an AV Lab
  - Virtual environment
  - Procedures for handling malware
- Virus Analysis Process
- Tools
  - Static Analysis
  - Process Observation
  - Network Observation