

# Virus Analysis

## Techniques, Tools, and Research Issues

### Part III: Malware Analysis Techniques - Basic

Michael Venable  
Arun Lakhotia

University of Louisiana at Lafayette, USA

---

---

---

---

---

---

---

---

# Malware Analysis Techniques - Basic

- # Demonstrate by Example
  - Analyze Beagle.J
- # Prepare the Lab
- # Malware Analysis Process
  - Static Analysis
  - Process Observation
  - Network observation

---

---

---

---

---

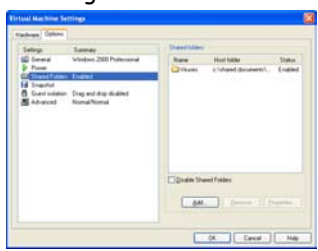
---

---

---

# Prepare the Lab

- # Create a shared folder for copying malware to guest OS



---

---

---

---

---

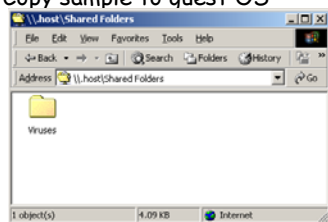
---

---

---

## Prepare the Lab

- # Navigate to \\host\ from within guest OS to find malware sample
- # Copy sample to quest OS



---

---

---

---

---

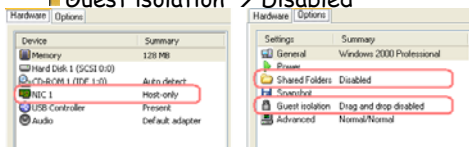
---

---

---

## Prepare the Lab

- # Secure the system
  - Network type → Host-only
  - Shared Folders → Disabled
  - Guest isolation → Disabled



---

---

---

---

---

---

---

---

## Prepare the Lab

- # Unzip malware sample
  - Password: "malware"
- # Take snapshot of virtual system

---

---

---

---

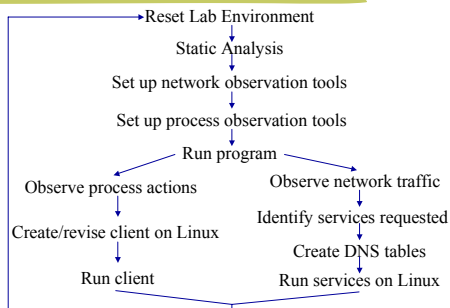
---

---

---

---

## Malware Analysis Process



---

---

---

---

---

---

---

---

## Beagle.J Capabilities

- # Registry/Run on startup
- # Copies into folders containing "shar"
- # Sends copies by email
- # Backdoor

---

---

---

---

---

---

---

---

## Static Analysis

- # Guessing program behavior from its strings
  - Using BinText
- # Detect UPX compression
  - Using Disassembler
- # UPX Decompression

---

---

---

---

---

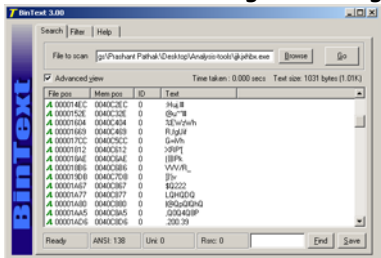
---

---

---

## String Extraction

# BinText reveals illegible strings



---

---

---

---

---

---

---

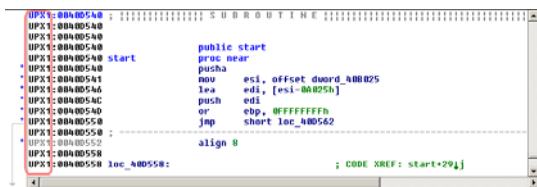
---

---

---

## Dissassembly

# IDA Pro shows file is UPX compressed



---

---

---

---

---

---

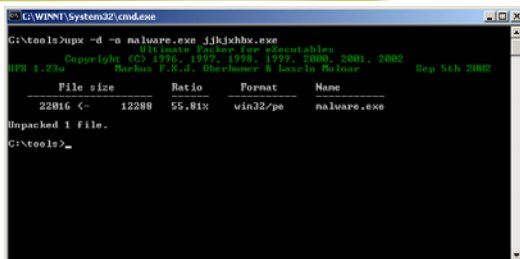
---

---

---

---

## UPX Decompression



---

---

---

---

---

---

---

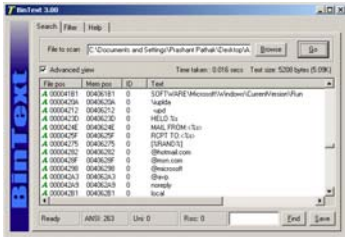
---

---

---

## String Analysis

- ✦ Analysis of the decompressed file reveals much more



---

---

---

---

---

---

---

---

## String Analysis Results

- ✦ "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
  - Registers itself to run on startup
- ✦ Suspicious EXE filenames (ex: "acdsee 9.exe")
  - Possibly for propagation
- ✦ "MAIL FROM:<%'s>", "RCPT TO:<%'s>"
  - Contains SMTP engine
- ✦ EXE filenames used by AV programs (ex: "update.exe")
  - Possibly kills processes belonging to AV programs

---

---

---

---

---

---

---

---

## Dynamic Analysis: Host Side

- ✦ Prepare process observation tools
  - Processes spawned by malware
  - Registry changes
  - File system changes
- ✦ Prepare network observation tools
  - Open ports
  - Network traffic

---

---

---

---

---

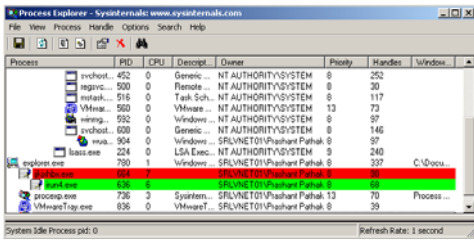
---

---

---

## Observe: Processes spawned

# jkxhbx.exe spawns irun4.exe



---

---

---

---

---

---

---

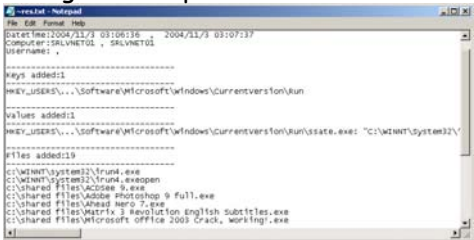
---

---

---

## Observe: System Changes

# RegShot output



---

---

---

---

---

---

---

---

---

---

## Observe: System Changes

# RegShot output

- File created called c:\winnt\system32\irun4.exe
- File created called c:\winnt\system32\irun4.exeopen
- c:\winnt\system32\irun4.exe configured to run on startup
- Several files added to c:\shared files

---

---

---

---

---

---

---

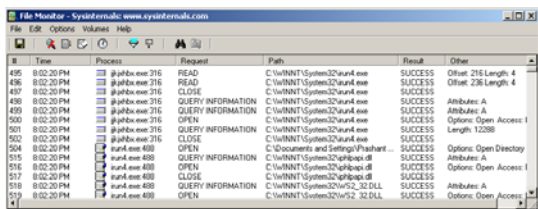
---

---

---

## Observe: File System changes

# jjkjxhbx.exe creates irun4.exe




---

---

---

---

---

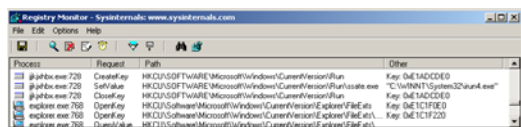
---

---

---

## Observe: Registry Changes

# jjkjxhbx.exe adds  
c:\winnt\system32\irun4.exe to  
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\  
Run\ssate.exe




---

---

---

---

---

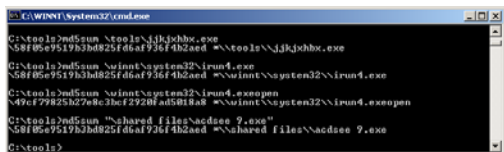
---

---

---

## Observe: Compare Copies

- # c:\winnt\system32\irun4.exe and files placed in c:\shared files are identical copies of jjkjxhbx.exe
- # c:\winnt\system32\irun4.exeopen is not a copy of jjkjxhbx.exe




---

---

---

---

---

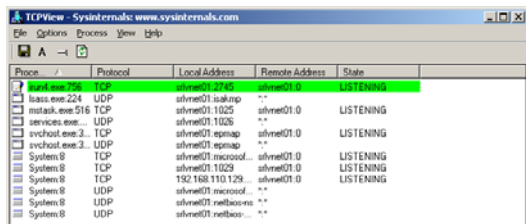
---

---

---

## Observe: Opening Backdoor

# irun4.exe listens for a connection on TCP port 2745



Process	Protocol	Local Address	Remote Address	State
irun4.exe.274	TCP	silver01.2745	silver01.0	LISTENING
lsass.exe.224	UDP	silver01.1sasknp	**	
mltask.exe.516	TCP	silver01.1025	silver01.0	LISTENING
services.exe...	UDP	silver01.1026	**	
svchost.exe.2...	TCP	silver01.epmap	silver01.0	LISTENING
svchost.exe.2...	UDP	silver01.epmap	**	
System 8	TCP	silver01.microsof...	silver01.0	LISTENING
System 8	TCP	silver01.1029	silver01.0	LISTENING
System 8	TCP	192.168.110.129...	silver01.0	LISTENING
System 8	UDP	silver01.microsof...	**	
System 8	UDP	silver01.netbiosns	**	
System 8	UDP	silver01.netbios...	**	

---

---

---

---

---

---

---

---

---

---

## Dynamic Analysis: Network

# Detect email propagation

---

---

---

---

---

---

---

---

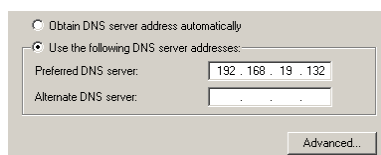
---

---

## Observe: Email Propagation

# Set RedHat Linux system as DNS server in Windows

# Run malware while observing with Snort



Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 192.168.19.132

Alternate DNS server: . . .

Advanced...

---

---

---

---

---

---

---

---

---

---



## Observe: Email Propagation

### ✦ Communication over port 53

■ Port 53 is used for DNS lookup

✦ Performs DNS lookup on sysinternals.com, winternals.com, and others. (Why?)

```
11/05/20:10:56.127296 102.168.19.130:11116 -> 102.168.19.130:53
TCP TTL:128 TOS:0x0 ID:353 SeqLen:20 OptLen:74 DF
***R*** Seq: 0x05082312 Len: 0x4F3083 Win: 0x4470 TcpLen: 20
02 02 01 00 00 01 00 00 00 00 00 00 0C 73 78 73 .....RPS
69 6E 74 65 72 6E 61 6C 73 03 63 6F 6D 00 00 0F .....nternals.com...
00 01 ..

11/05/20:11:04.160217 102.168.19.130:11118 -> 102.168.19.130:53
TCP TTL:128 TOS:0x0 ID:353 SeqLen:20 OptLen:72 DF
***R*** Seq: 0x0673311E Len: 0x4F6E05 Win: 0x4470 TcpLen: 20
02 02 01 00 00 01 00 00 00 00 0A 77 69 6E .....win
74 65 72 6E 61 6C 73 03 63 6F 6D 00 00 0F 00 01 .....ternals.com.....
```

---

---

---

---

---

---

---

---

---

---

## Observe: Email Propagation

✦ FileMon shows irun4.exe scans disk contents

✦ Perhaps the domain names were picked up from the hard disk

#	Time	Process	Request	Path
669	2:08:02 PM	irun4.exe 764	DIRECTORY	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\FLEM...
670	2:08:02 PM	irun4.exe 764	CLOSE	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\FLEM...
671	2:08:02 PM	irun4.exe 764	OPEN	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\LORD...
672	2:08:02 PM	irun4.exe 764	DIRECTORY	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\LORD...
673	2:08:02 PM	irun4.exe 764	DIRECTORY	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\LORD...
674	2:08:02 PM	irun4.exe 764	OPEN	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\LORD...
675	2:08:02 PM	irun4.exe 764	DIRECTORY	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\LORD...
676	2:08:02 PM	irun4.exe 764	DIRECTORY	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\LORD...
677	2:08:02 PM	irun4.exe 764	OPEN	C:\Documents and Settings\Pashant Pathak\Desktop\Analysis-tool\LORD...

---

---

---

---

---

---

---

---

---

---

## Observe: Email Propagation

✦ A search through the files confirms our suspicions

or modified form, or wish to use filemon source code in a product, please send e-mail to [licensing@sysinternals.com](mailto:licensing@sysinternals.com) with details.

#### Reporting Problems

If you encounter problems, please visit <http://www.sysinternals.com> and download the latest version to see if the issue has been resolved. If not, please send a bug report to:

[mark@sysinternals.com](mailto:mark@sysinternals.com) and [cogswell@winternals.com](mailto:cogswell@winternals.com)

---

---

---

---

---

---

---

---

---

---

## Summary

### ⌘ Lab Setup

- Virtual environments
- Security procedures

### ⌘ Analysis Process

- Guess behavior from strings
- Host side observations
  - files and registry changes, processes spawned, backdoors
- Network side observations
  - Services requested

---

---

---

---

---

---

---

---