Norman SandBox Solutions
15 January 2007
Righard J. Zwienenberg
Source: AV-Test, Andreas Marx, 2004
Agenda

• Introduction

• The Norman SandBox

• Demonstration

• Q&A
Introduction: Richard J. Zwienenenberg

- 1976: First experience computers (9 years old)
- 1977: Actively working with computers
- 1982: Teaching my first classes (15 years old)
- 1988-1991: Freelance consultant, VirScan.Dat (TBScan/HTScan)
- 1991: Member of CARO
- 1990-1996: The Hague High School, Sector Informatics
- 1998-now: Norman
- 2000: Co-founded AVED, Board Member on AVED
- 2003: Technical Overview Board Member of the WildList Organization
- 2005: Technical Board Member of CME (Common Malware Enumeration)
- 2005: Vice-President AVAR, European Operations
- 2005: Chief Research Officer at Norman
Introduction: Righard Zwienenberg in Norman

- Virus Research
- Scanner Engine Development
- Security Research
- Liaison for Norman to Virus Bulletin, EICAR, ICSA Labs, AVAR, Certification Organizations (e.g., Checkmark), Microsoft, Testers, Reviewers, etc.
- Presentations, Seminars, Workshops, Conferences
- Talking to journalists
- Flying over the world for Norman
Introduction: Righard Zwienenberg privately

- Married for 9.5 years
- 1 boy (almost 18 months) Matthew
- Drummer
- Magician
- Modelling
- Stand-up Comedy
Commodore Pet-2001

- 4KB Memory
- Video memory: 1KB
- Starts up with Basic

The next code made the Pet 2001 went up in fire!!!

10 motor 1
20 motor 0
30 goto 10
Sandbox: a quick introduction

• Why was it created?

• Why do we make the technology publicly available?

• How do we make it available?
Norman SandBox Solutions Overview

• Norman SandBox Reporter
  – Malware information sent by email
  – Subscription based

• Norman SandBox Analyzer
  – Application to perform fast and efficient analysis of suspicious files

• Norman SandBox Analyzer Pro
  – Application to perform in-depth analysis of malware
Norman SandBox Reporter

- Information gathered by Norman SandBox Information Center (http://sandbox.norman.com) in the past 24 hours

- SandBox summary

- List of URL’s with possible malicious content

- List of IRC servers including login details found in the analyzed files

- Provided as .txt and .xml file
SandBox Reporter Sample of SandBox Summary

- **Detection Info**
  - Display SandBox classification like, W32/Downloader
  - If the scanned file are known to Norman, the name of the malicious file will be displayed here like Bagle, Sober etc.

- **General Information**
  - Gives you file length and MD5 hash information

- **Changes to Filesystem, Registry etc.**
  - Here you will find information about files created and deleted as well as new registry keys and deleted registry keys.

- **Network services**
  - Will show information about network services the file are using like, downloading/uploading files from/to a specific location. IRC networks it will connect to with login details, SMTP server details etc.

- **Security issues**
  - We will describe why this would be a possible security issue

- **Signature Scanning**
  - In this case we will scan the created files and if they are know the name will be shown here.

- **More information are available depending of kind of malicious file.**
SandBox Reporter - URL List

- Contains exact paths to where files are connecting to download files, as these URL’s are found in malware they most likely to be malicious even if we report “no virus” as long as the file content is PE_I386 and there is a value in the length column.
- Signature means name of malware as reported Norman Virus Control
- SandBox means SandBox classification of malware in the URL
- The example below have 2 lines in blue and are found in the SandBox summary on the previous slide (show the link between the 2 reports).
SandBox Reporter - Summary

[ DetectionInfo ]
* Sandbox name: W32/Backdoor
* Signature name: NO_VIRUS

[ General information ]
* "IMPORTANT: PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMAN.NO - REMEMBER TO ENCRYPT IT (E.G. ZIP WITH PASSWORD)".
* Creating several executable files on hard-drive.
* File length: 48640 bytes
* MD5 hash: 68f1966e98c21a0643e9e7cd07966100

[ Changes to filesystem ]
* Creates directory C:\WIN\32dc.
* Creates file C:\WIN\32dc\DA0C + fix.exe.
* Creates file C:\WIN\32dc\Sims 2 + cheat.exe.
* Creates file C:\WIN\32dc\BattleField 1942 + serial.exe.

[ Network services ]
* Connects to "us.undernet.org" on port 6667 (IP).
* Connects to IRC server.
* IRC: Uses username xmasterwodkcfilnrulameftfi.
* IRC: Uses nickname MVDOMxOQKCFIlnrULAMeFtFRi.
* IRC: Joins channel #vdm with password fucK21.
* IRC: Sets the channel mode for channel #vdm to fucK21.

[ Signature Scanning ]
* C:\WIN32dc\DA0C + fix.exe (51841 bytes) : no signature detection.
* C:\WIN32dc\Sims 2 + cheat.exe (48769 bytes) : no signature detection.
* C:\WIN32dc\BattleField 1942 + serial.exe (50817 bytes) : no signature detection.
SandBox Reporter - IRC List

- Contains information about IRC servers found in the analyzed malware
- Information provided includes
  - Server name, port connects on, password used, IP address, active or not
  - Nickname, username, channel password, user mode
  - Etc.
- These IRC networks are likely to be Botnets as they are found in malware
SandBox Reporter: where to use...

- In (Personal) Firewalls...
- In Filters...
- Etc…
Norman SandBox Analyzer

- An applications for analyzing files, deeper, faster and more efficient than previously seen

- Analyze files one by one or in batch jobs to increase efficiency

- Ability to set number of emulation cycles to increase detection rate

- Get SandBox summary of files analyzed for fast evaluation of file action like type of malware, changes to filesystem, registry, network services used, signature name if existing and more

- Get the complete API log of the analyzed file actions

- Analyze further dropper files from analyzed files.
Norman SandBox Analyzer

- Designed for organizations dealing with suspicious files
  - Security organizations
  - Malware researchers
  - Network security application and appliance vendors etc.
  - ISP’s
  - Large corporate
  - Helpdesks
SandBox Relations Between API Log & Summary

- **API Log**

  ```
  KERNEL32CopyFileA ("C:\WINDOWS\SYSTEM32\KERN32.EXE","C:\WINDOWS\SYSTEM32\kern32.exe",0x00000000)
  KERNEL32GetFileAttributesA ("C:\WINDOWS\SYSTEM32\kern32.exe")
  KERNEL32CreateFileA ("C:\WINDOWS\SYSTEM32\KERN32.EXE",0x00000000,0x00000000,0x00000000,0x00000000,0x00000000,0x00000000,0x00000000,0x00000000)
  KERNEL32SetFileAttributesA ("C:\WINDOWS\SYSTEM32\kern32.exe",0x00000000)
  ADVAPI32RegCreateKeyExA (0x00000002, "Software\Microsoft\Windows\CurrentVersion\RunOnce",0x00000000, NULL, 0x00000000,0x00000000,0x00000000)
  ADVAPI32RegSetValueExA (0x720021E8, "kernel32", 0x00000000,0x00000000,0x00000000,0x74110F00,0x00000000)
  KERNEL32CreateMutexA (0x00000000,0x00000000,0x00000000,0x00000000)
  KERNEL32CreateThread (0x74110F00,0x00000000,0x00000000,0x00000000,0x00000000,0x00000000)
  ```

- **SandBox Summary**

  **General information**
  - **IMPORTANT:** PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMAN.NO – REMEMBER TO ENCRYPT IT (E.G. ZIP WITH PASSWORD)**.
  - File length: 58368 bytes.
  - MD5 hash: 60a8d2e41147f4b364e1eb3729ac53fb.

  **Changes to filesystem**
  - Deletes file C:\WINDOWS\SYSTEM32\kern32.exe.
  - Creates file C:\WINDOWS\SYSTEM32\kern32.exe.

  **Changes to registry**
  - Creates key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce".
  - Sets value "kernel32"="C:\WINDOWS\SYSTEM32\kern32.exe -sys" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce".

  **Changes to system settings**
  - Creates WindowsHook monitoring keyboard activity.

  **Network services**
  - Connects to "200.223.3.130" on port 6667 (TCP).
  - Connects to IRC server.
  - IRC: Uses nickname CurrentUser[FRK][19].
  - IRC: Uses username SERVERNO.
  - IRC: Joins channel #SMcK_r00T.
**SandBox Analyzer Pro**

- **Norman SandBox Analyzer Pro**
  - Target market, security organizations, security companies needing to do deep analysis of file behavior
  - Since deep analysis is not time critical you can set it to run a higher number of emulation cycles
  - By the use of a large set of parameters you are able to monitor various sections of the code as it runs and after it have been running
    - See the changes to the OS as the file is running
    - Set breakpoint’s and insert additional code to see the reaction
    - Watch library being loaded
    - See Threads running
    - See Sockets created
  - All in all you will get the full picture of the actions done by the file that is being analyzed
SandBox Analyzer Pro

• **Register view**
  – Shows the emulator “CPU” status.
    • The normal registers, including some debug registers and “CPU” flags.
    • ThreadScheduler
    • PageFault
    • Breakpoints
    • Emulation cycles
    • Status Line
SandBox Analyzer Pro

**Disassembler view**
- This view will disassemble the instruction at CS:EIP, or any given memory address.
- Arrow keys can be used to move up and down.
- The view will update, together with the “Register View” to show the state of the emulator.
- The disassembler will try to resolve addresses against imported functions
SandBox Analyzer Pro

• Memory dump view
  – This view can dump any memory area.

```
0033:0042FBD6 E9 25 E4 FF FF 00 00 00 54 46 46 A5 1E FC 02 00 .......TFF......
0033:0042FBD6 25E9 FFE4 00FF 0000 4654 A546 FC1E 0002 .......TFF......
0033:0042FBD6 FFE425E9 000000FF A5464654 0002FC1E .......TFF......
```

```
0033:0042FC4B kernel32.dll
0033:0042FC56 user32.dll
0033:0042FC69 GetModuleHandleA
0033:0042FC77 MessageBoxA
0033:0042FC77 N/A
0033:FFFFFFFF N/A
0033:FFFFFFFF N/A
```
SandBox Analyzer Pro

• API Log view
  – As the program being emulated interacts with the sandbox operating system, the details of supported APIs are showed in this window.
  – This memory buffer is predefined to be 64MB.
  – API log can be saved to disk

```c
#000695 KERNEL32!FlsGetValue (0x00000001)
#000696 KERNEL32!FlsSetValue (0x00000001, 0x73002447)
#000697 WS2_32!gethostname (0x4FF922C4, 0x000000FF)
#000698 WS2_32!gethostbyname ("FAKE")
#000699 WS2_32!socket (0x00000002, 0x00000001, 0x00000000)
#000700 KERNEL32!HeapAlloc (0x00000000, 0x00000000, 0x000000464)
#000701 WS2_32!gethostbyname ("irc.quakenet.org")
#000702 WS2_32!htons (0x00001A08)
#000703 WS2_32!connect (0x00000002, 0x4FF91B60, 0x00000010)
#000704 -connect port 06667, ["IP"] IP "irc.quakenet.org"
#000705 USER32!wprintfA (0x4FF91A8C, "Connects to "\%s" on port \%5d \(\%s\)
#000706 "0x72005BB1...")
#000707 USER32!wprintfA (0x73356F8D, "\%s \%s \%s :\%s"
#000708 "0x73356E2...")
#000709 USER32!wprintfA (0x73356FCB, "\%s \%s \%s :\%s"
#000710 "0x73356E2...")
#000711 WS2_32!fcntlsocket (0x00000002, 0x8004667E, 0x4FF91B5C)
#000712 WS2_32!send (0x00000002, 0x4FF91BA4, 0x00000033, 0x00000000)
#000713 4FF91BA4 55 53 45 52 20 49 72 65 63 4D 33 67 65 72 20 31 32 USER IrcMsger 12
```
SandBox Analyzer Pro

**Command input view**
- This view will receive information from the sandbox regarding detection, emulation cycles done etc
- You are able to give specific command to the SandBox
- Currently 30 commands are available, including:
  - Set a breakpoint on a given interrupt
  - Set a breakpoint on a memory write on the given selector:offset
  - Will display stack trace
  - Show the MMX registers
  - Show page table.
  - +25 more
SandBox Analyzer Pro

• Thread view
  – Shows information on all created threads
    • thread ID
    • thread status
    • Information regarding active threads
  – Possibility to navigate the different threads
SandBox Analyzer Pro

**SandBox Summary View**
- A view summarizing the findings of the emulation
- Grouping them into different categories like
  - Changes to file system
  - Changes to registry
  - Changes to system settings
  - Network services used by the analyzed file
  - Process/Window information created

```plaintext
Deletion: C:\2.exe
Create file: C:\WINDOWS\SYSTEM32\132x.exe
Create file: C:\WINDOWS\STARTUP\dllxw.exe
Create file: C:\WINDOWS\SYSTEM32\vxd32v.exe
Create file: system.ini

[Changes to registry]
Create value "load32"="C:\WINDOWS\SYSTEM32\132x.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"

[Changes to system settings]
Modify profile key "shell"="explorer.exe C:\WINDOWS\SYSTEM32\vxd32v.exe" in section [boot]
Create WindowsHook monitoring journal record activity.

[Network services]
Looks for an Internet connection,
Connects to "pop.btw.egold-hosting.com" on port 25 (IP),
**Connects SMTP server.

[Process/Window information]
Will automatically restart after boot (I'll be back...).
```
Connecting to the real internet

- Why would you want to connect to the real internet?
Connecting to the real internet

You have enabled the sandbox to use a real Internet connection.

The application C:\WINDOWS\SYSTEM32\wininit32.exe wants to connect to

<table>
<thead>
<tr>
<th>Address</th>
<th>ityoill1g0to.YGIO.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>6667</td>
</tr>
<tr>
<td>Type</td>
<td>IP</td>
</tr>
<tr>
<td>Max delay</td>
<td>2</td>
</tr>
</tbody>
</table>

[X] I want to verify each packet going to/from this source
[X] Copy this network activity to log
(*) Log as text (ASCII)
(>) Log as hex

[X] Notify when the connection is closed
[X] Remember the answer on this connection

If you let the application connect the remote server your personal firewall should react.

Do you approve of this external connection?

Press NO to treat it internally
Internal and/or external

[ Network services ]
Connects to "ityoilligoto.YGTO.com" on port 6667 (IP).
Connects to IRC server.
Connects to "ityoilligoto.YGTO.com" on port 6667 (TCP).
Connects to IRC server.
IRC: Uses nickname rpawu^pwq.
IRC: Uses username 1234BLA.
IRC: Sets the usermode for user rpawu^pwq to -x+i.
IRC: Joins channel #ot!macaton with password *P.^3h!+f9&6.(*&jjj).S.
IRC: Sets the channel mode for channel #ot!macaton to .

[ Network services ]
Connects to "ityoilligoto.YGTO.com" on port 6667 (IP).
Connects to "host1lliili.mooo.com" on port 6667 (IP).
Connects to "1lli1lllli11.afraid.org" on port 6667 (IP).
Connects to "til1lli11.afraid.org" on port 6667 (IP).
Connects to "thisislliili.b3ta.org" on port 6667 (IP).
Connects to "imiillil1not.afraid.org" on port 6667 (IP).
Connects to "user1ll11.a-p-e.m-a-f-i-a.com" on port 6667 (IP).
Connects to "1.love.you.oily.afraid.org" on port 6667 (IP).
Connects to "ill1.d0.l.hear.all.mooo.com" on port 6667 (IP).
Connects to "hlph0pf1ipf10p.afraid.org" on port 6667 (IP).
Connects to "1121I.0n.my.ignorelist.com" on port 6667 (IP).
Connects to "ftp.binary0101001I.YGTO.com" on port 6667 (IP).
Connects to "lli1llI1I.y2003zuxx.xxuz.com" on port 6667 (IP).
Connects to "ityoilligoto.YGTO.com" on port 6667 (IP).
What can Norman Sandbox do for you?

• Save time
  – The average response time to a new threat is 6 – 24 hours.
  – Start with knowledge of what the sample is trying to do.

• Save money
  – Growing number of viruses to analyze, growing number of analyst needed to respond to these threats.

• Save the day
  – You’ve been in the situation where something needed to be analyzed yesterday and now you have access to the tools to make it happen.
Demo-time...
Questions and Answers

Righard J. Zwienenberg
Chief Research Officer
Righard.Zwienenberg@norman.no
http://www.norman.com/fr

Norman France
8 Rue de Berri
75008 Paris
Tel: +33-1-42 99 94 14
E-mail: info@norman.fr

Cortina
14 avenue J-B Clement
92100 Boulogne-Billancourt
Tel : +33 (0)1 41 10 26 10
Email : info@cortina.fr