Mass Malware Analysis

A Do-It-Yourself Kit
Christian Wojner
- CERT.at
- Malware analysis
- Reverse-Engineering
- wojner@cert.at
Mass malware analysis needs automation!

Automated Malware Analysis Station
Talk's Outline

- What?
  - Characteristics

- How?
  - General concept
  - CERT.at's implementation
  - Screenshots

- What-For?
  - Example evaluations
What?
Characteristics

- Cheap (mostly free software)
- Autonomic
- Runs on a standard desktop
- Target-OS freely chooseable
- Easy to set up
- Ready for use within a day
- Fully customizable
- Easily evaluateable
- Runtime-unpacked/-decrypted samples must not be a hurdle
- Data/Analysis/Samples/… kept confidential
How?
Manual steps to behavioral analysis one sample:

1. Preconfigure proband
2. Throw in sample
3. Start monitoring tools
4. Execute sample
5. Get out logs
6. Interpret logs
Manual steps to behavioral analyze more than one sample:

1. fetch (next) sample
2. throw in sample
3. start monitoring tools
4. execute sample
5. get out logs
6. disinfect proband

(A) preconfigure proband

(B) interpret logs

STOP
Two scopes
- Researcher
- Proband

Virtual machines come in handy
- Researcher (= native machine)
- Proband (= virtual machine)
Identifying Components

native machine (host)

researcher

virtual machine (guest)

proband
We need some controller processes:
Communications over FTP:
We need two collections:
Defining Communications

Big picture with communication flow:
Problems Of Automation

- Synchronization
  - Two processes, different machines
  - FTP again

- Timing
  - Deadlocks
  - Timeouts

- Timeouts
  - Best values? – It depends!
Theory => Practice
VirtualBox (VBox)

- Commandline tool VBoxManage ...
  - ... list vms
    - Find out your uuid
  - ... startvm uuid
    - Startup virtual machine
  - ... controlvm uuid poweroff
    - Pull out power cable
  - ... snapshot uuid discardcurrent -state
    - Restore to last saved state
CERT.at's Implementation
Hardware

- Dell OPTIPLEX 745
- Intel Core 2 Duo 6400
- 2 Gigs of RAM
Researcher's software

- Ubuntu-Linux
- SUN’s VirtualBox
- Proftpd
- zip
- minibis-cpr (home-grown)
Proband's software

- Microsoft Windows XP SP3
- ProcessMonitor (from Sysinternals)
- minibis-cpp (home-grown)
Features

- Monitoring activities using ProcessMonitor (Procmon from Sysinternals)
- Making screenshot on exit
- .PML-files
- .CSV-files
- Compress (ZIP) the returned .PML-files and binaries
Big Picture For CERT.at's Implementation
Screenshots
The virtual machine (proband) is being started.
ProcessMonitor from Sysinternals has just been started.
Just an example of active malware.
The native ProcessMonitor saving format is being converted to CSV.
The virtual machine (proband) gets reverted.
Malware caused our proband to restart. That’s why we need the outer emergency break.
Viewing results after a few samples.
What-For?
Some example evaluations on the basis of 3902 .exe samples ...
„Size DOES matter“

- Biggest sample: 16,448,512 bytes
- Smallest sample: 812 bytes
- Average sample: 391.688 bytes
„Browser-History-Junkies“

- Historydata accessed: 1220 samples
  - Historydata written: 3 samples
“Cookie Monsters”

- Cookies accessed: 118 samples
  - Cookies read: 58 samples
  - Cookies written: 4 samples
  - Cookies created: 3 samples
“Security Center Kings“

- Service disabled: 2 samples
- Warnings disabled: 3 samples
- Firewall disabled: 9 samples
- Autoupdates disabled: 1 sample
Example Evaluations

■ „Internet Settings“

• Read: 1,480 samples
• Changed: 1,236 samples
Example Evaluations

- "DNS-Kiddies"
  - `\etc\Host` read: 9 samples
  - `\etc\Host` written: 14 samples
例の評価

- "Desktop Designers"
  - Screensaver changed: 44 samples
  - Wallpaper changed: 46 samples
“Reboot-Fetish”

- Pending renames scanned: 112 samples
- Pending renames added: 41 samples
- Pending renames deleted: 7 samples
„Miscellaneous“

- Taskmanager disabled: 446 samples
- Other processes forked: 1.486 samples
- Multiple threads used: 2.255 samples
- ADS used: 3 samples
<table>
<thead>
<tr>
<th>Favorite Autostart Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1161 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
</tr>
<tr>
<td>0887 HKLM\System\CurrentControlSet\Services</td>
</tr>
<tr>
<td>0113 HKCU\Software\Microsoft\Windows\CurrentVersion\Run</td>
</tr>
<tr>
<td>0101 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit</td>
</tr>
<tr>
<td>0085 HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects</td>
</tr>
<tr>
<td>0063 HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components</td>
</tr>
<tr>
<td>0061 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell</td>
</tr>
<tr>
<td>0050 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify</td>
</tr>
<tr>
<td>0030 \Programs\Startup \</td>
</tr>
<tr>
<td>0008 HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved</td>
</tr>
<tr>
<td>0007 HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks</td>
</tr>
<tr>
<td>0004 HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers</td>
</tr>
<tr>
<td>0002 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32</td>
</tr>
<tr>
<td>0001 HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls</td>
</tr>
</tbody>
</table>
The underlying paper provides you with
  • more details
  • a step-by-step guide for building CERT.at's implementation
  • and links for downloading our binaries

So, please take a look at it!
Feedback is always appreciated.
Topical Background

Paper from October 14th, 2009

Thanks!

Christian Wojner
wojner@cert.at