Forensic Memory Analysis: Files mapped in memory

Ruud van Baar
Wouter Alink
Alex van Ballegooij
Netherlands Forensic Institute

August 12, 2008
DFRWS 2008 Baltimore
Introduction

• Why analyse memory dumps?
• Files mapped in memory
• Implementation
• Results
• Demonstration
Why analyse memory?

- Interesting data [Walters 2007]
  - Processes
  - Network information
  - Passwords
  - Cryptography keys
  - …
- Can provide information about recent activities on a system
- Mapped files…
Files mapped in memory

- Link files to a user or process
- Point out recently used data
- Identify data in a memory dump to reduce search space for other information, e.g. passwords
Fragmentation

Problem:
High degree of fragmentation of files in memory
Approach

- Recognize pool structures used by the Windows Memory manager
  - Process structures [Schuster 2006]
  - File structures [Dolan-Gavitt 2007]
- Link these structures if possible
- Carve for unidentified structures
Different methods of identification

- Find process structures
- Identify private and shared files
- Carve for specific file-mapping structures
  - Control areas (MmCa)
  - Page tables (MmSt)
File information

• Original path in file system
• Not always available; Backup:
  • Use known mapping to eliminate fragmentation
  • Header/footer information
Implementation

- Proof of concept
- Currently only Windows XP SP2
- File size not always known
- Needs more testing
  - Different configurations (PAE, 64 bit)
  - Larger memory dumps
Results by extension

<table>
<thead>
<tr>
<th>Extension</th>
<th>DFRWS 2005 -1</th>
<th>DFRWS 2005 -2</th>
<th>Windows XP</th>
</tr>
</thead>
<tbody>
<tr>
<td>.dll</td>
<td>202</td>
<td>.dll</td>
<td>211</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.dll</td>
</tr>
<tr>
<td>.pnf</td>
<td>82</td>
<td>.exe</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.gif</td>
</tr>
<tr>
<td>.exe</td>
<td>29</td>
<td>.mmf</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.ttf</td>
</tr>
<tr>
<td>.mmf</td>
<td>11</td>
<td>.ttf</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.ini</td>
</tr>
<tr>
<td>.png</td>
<td>11</td>
<td>.log</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.jpg</td>
</tr>
</tbody>
</table>
Results by method

- Number of identified blocks
- Method: vadwalk, objecttables, mmca/mmci, mmst
Conclusion

• Possible to identify 25% of pages as part of mapped files
• 40% of these pages can be linked to the relating process or processes
• Less informative methods result in more pages identified
Demonstration

• Test memory dump of a VMWare system running Windows XP SP2 with 256MB of RAM.

• VirtualBLOB [XIRAF 2006]
Demonstration
Contact

Ruud van Baar      ruud@holmes.nl
Wouter Alink
Alex van Ballegooij
Netherlands Forensic Institute