Challenge forensics DC3

Christophe GRENIER - grenier@cgsecurity.org
Challenge forensics DC3

- Challenge réalisé par le « Defense Cyber Crime Center » (DC3) plus particulièrement « Defense Computer Forensics Laboratory » (DCFL)
- « DC3 Challenge is a call to the digital forensics community to pioneer new investigative tools, techniques and methodologies. »
Challenge forensics DC3

- The DC3 Challenge requires that all of its winning team participants hold **U.S. citizenship** and reside within (and travel from) the Continental US (CONUS); therefore the winning team must be comprised of all CONUS, U.S. citizens in order to claim the prize trip to the Conference.

- The DC3 Digital Forensics Challenge welcomes **non-US citizens** to participate for score and **bragging rights only**.
Challenge forensics DC3

- Objectif réel: « United States Cyber Challenge - a talent search and development program for finding and nurturing the next generation of cyber experts »
Challenge forensics DC3

• Conduct a forensic exam of the submitted media for evidence of violation(s) of:

  • 26 USC Sec. 5812 (possession of automatic weapons),
  • 10 USC Chapter 161 - Property Records And Report Of Theft Or Loss Of Certain Property (Weapons)
  • 42 U.S.C. 3713 Computer Crime Enforcement Act
  • 40 USC Sec. 5104 Sec. 5104. Unlawful activities
  • 10 USC Sec. 881 Sec. 881. Art. 81. Conspiracy
Logiciels suspects
Browsing Virtual Filesystem

Tree View

- msdownd.tmp
- NVIDIA
- Program Files
  - Accessories
  - CHAT
  - Common Files
  - DIRECTX
  - DriveWiper Pro 1.10
  - EvidenceEliminator5.0
  - Internet Explorer
  - Messenger
  - MSN
  - MSN Messenger
  - NetMeeting
  - Online Services
  - Outlook Express
  - PLUS!
  - PowerQuest
  - Skype
  - Steg Creator Plus
  - STEG_IT_v7
  - SuperVault_Encryption_Service_2.4

Table View

<table>
<thead>
<tr>
<th>Inode</th>
<th>Filename</th>
<th>Del</th>
<th>File Size</th>
<th>Last Modified</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>desktop.ini</td>
<td>☑</td>
<td>129</td>
<td>2009-02-26 11:14:20</td>
<td>r/r</td>
</tr>
</tbody>
</table>
Stéganographie
Extrait du rapport du Special Agent H. Edward Cicop:
« She stated that he would have pictures of Crystal Clocks up on the computer for hours and said he was ‘working on them’ like they were broken or he was fixing them somehow. »
<table>
<thead>
<tr>
<th>Thumbnail</th>
<th>Filename</th>
<th>Type</th>
<th>Size</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Clock" /></td>
<td><code>/c/IntelPRO/APPS/TOOLS/CC1.MDB</code></td>
<td>JPEG image data, JFIF standard 1.01</td>
<td>47780</td>
<td>2008-12-26 23:16:46</td>
</tr>
<tr>
<td><img src="image2.png" alt="Clock" /></td>
<td><code>/c/System Volume Information/ restore{2906B87C-A85F-43CD-91FA-1C1B08CE54E2}/RP31/log.ini</code></td>
<td>JPEG image data, JFIF standard 1.01</td>
<td>47191</td>
<td>2008-12-26 23:37:26</td>
</tr>
</tbody>
</table>
Système de fichier chiffré ?
Browsing Virtual Filesystem

Tree View

Filesystem Structure:
- /c
  - $RECYCLE.BIN
  - Documents and Settings
  - Downloads
  - ETHERNET
  - i386
  - IntelPRO
  - msdownload.tmp
  - NVIDIA
  - Program Files
  - Recycled
  - System Volume Information
  - WINDOWS
  - Windows.old
  - _deleted_
  - _unallocated_

Table View

<table>
<thead>
<tr>
<th>Inode</th>
<th>Filename</th>
<th>Del</th>
<th>File Size</th>
<th>Last Modified</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>K209688-0-0</td>
<td></td>
<td>4194304</td>
<td>2008-03-11 13:08:36</td>
<td>r/r</td>
</tr>
<tr>
<td>Id</td>
<td>K209793-0-0</td>
<td></td>
<td>4096</td>
<td>2008-04-01 08:52:50</td>
<td>d/-</td>
</tr>
<tr>
<td>Id</td>
<td>K209791-0-0</td>
<td></td>
<td>4096</td>
<td>2008-04-01 08:50:44</td>
<td>d/-</td>
</tr>
<tr>
<td>Id</td>
<td>K209789-0-0</td>
<td></td>
<td>4096</td>
<td>2008-04-01 08:50:18</td>
<td>d/-</td>
</tr>
<tr>
<td>Id</td>
<td>K209787-0-0</td>
<td></td>
<td>4096</td>
<td>2008-04-01 08:49:22</td>
<td>d/-</td>
</tr>
<tr>
<td>Id</td>
<td>K209785-0-0</td>
<td></td>
<td>4096</td>
<td>2008-04-01 08:42:30</td>
<td>d/-</td>
</tr>
<tr>
<td>Id</td>
<td>K209783-0-0</td>
<td></td>
<td>4096</td>
<td>2008-04-01 08:31:26</td>
<td>d/-</td>
</tr>
<tr>
<td>Id</td>
<td>K209781-0-0</td>
<td></td>
<td>4096</td>
<td>2008-04-01 08:37:18</td>
<td>d/-</td>
</tr>
</tbody>
</table>
Des Armes automatiques!
Viewing file in inode **K42784656-0-0**

Classified as XML document text by magic

```xml
<over><Text></Text></Message><Message Date="4/3/2008" Time="12:28:48 PM"
DateTime="2008-04-03T19:28:48.953Z" SessionID="3"><From><User FriendlyName="blane"/></From><To><User FriendlyName="bob"/></To><Text Style="font-family:MS Shell Dlg; color:#000000; ">I don't rat, ut maybe we better not. Least not now.</Text></Message><Message Date="4/3/2008"
Time="12:30:15 PM" DateTime="2008-04-03T19:30:15.968Z"
SessionID="3"><From><User FriendlyName="bob"/></From><To><User FriendlyName="blane"/></To><Text Style="font-family:MS Shell Dlg; color:#000000; ">It goes as planned and youre gonna be there too. I didn't spend all this time and effort for you to chicken out at the last minute. If youre too yellow to work this with me ill get somebody else to pull it with. **You just give me the guns and gear u got**</Text></Message><Message Date="4/3/2008" Time="12:30:55 PM"
DateTime="2008-04-03T19:30:55.125Z" SessionID="3"><From><User FriendlyName="blane"/></From><To><User FriendlyName="bob"/></To><Text Style="font-family:MS Shell Dlg; color:#000000; ">I aint no mor yellow than you. You think your so bad, just remember I can wip your tail anyday, did a year ago</Text></Message><Message Date="4/3/2008"
Time="12:31:25 PM" DateTime="2008-04-03T19:31:25.671Z"

```
Un casse!
B,  

You just watch your self man, you are walking on thin ice. You know the time is coming soon and we can’t afford any more mistakes. If we don’t hit this place by Friday we’re gonna miss our chance and you know I cant afford that. If you’re planning on chickening out don’t even think about it, I got ways of making sure you don’t back out. And don’t think about telling anyone, you know I know how to shut people up if I need to.
Un problème ?