Honeynet Scan of the Month 26

February 2003

Brian Carrier (carrier @ cerias.purdue.edu)

Tools

To complete this challenge, the following tools were used:

- `TASK 1.60` (http://sleuthkit.sourceforge.net)
- `Autopsy 1.70` (http://autopsy.sourceforge.net)
- `foremost 0.64` (http://foremost.sourceforge.net)
- `stegdetect` (http://www.outguess.org)
- `Invisible Secrets` (http://www.neobytesolutions.com/invsecr)

Setup

The `scan26.zip` file was downloaded from the Honeynet website and the MD5 value was verified. The zip file was then unzipped and the `scan26` image was extracted and the MD5 sum verified.

Autopsy 1.70 was started and a new case was created. The case name was `jimmyjungle`, the description was `Supplier for Joe Jacobs`, and the investigator was `carrier` (screen shot).

Inside the `jimmyjungle` case, a host was created called `floppy`, the description was `Floppy disk found at residence`, and the timezone was set for `EST5EDT`. Since this was not from a specific system, the clock skew can not be supplied and we do not have any hash databases for this case. (screen shot)

Inside the `floppy` host, the image was added by selecting "Add Image" and moving the `scan26` file to the `jimmyjungle/floppy/images` directory. The file system type was `fat12`, the mounting point was `A:\`, and we can add the known MD5 value of `e9c7d0c87ab0ecce09bf90362b830a74`. Check the "Verify Before Adding Image" box to verify the image integrity again (screen shot).

Quick Hits

The first step in our analysis was to get the quick and obvious pieces of evidence. A more comprehensive analysis was later performed to fill in the holes.

File Analysis

The first and most obvious step was to examine the file contents of the image. This was done with the 'File Analysis' mode in Autopsy. As shown in the screen shot , there were no files in the root directory. So much for the obvious quick hits.

Image Details

Based on the previous step, we had either a blank floppy, or a floppy with only hidden information. The 'Image Details' mode in Autopsy gave us more insight about what we were dealing with (screen shot). This view showed the following data that may be important later.

- Sectors 1-9 and 10-18 were for the Primary and Secondary FAT
- Sectors 19-32 were for the Root Directory
- Sectors 33-2878 were for the Data Area
- Nothing was being shown in the 'FAT CONTENTS' section

The Primary and Secondary FAT were examined to verify what was being seen. The 'Data Unit' mode was used to show the contents of sectors 1-9 (Starting Sector #1 and length of 9). Using the Hex view we were able to see data in the first 24-bits (which were reserved) and the remainder was all 0's (screen shot). The Secondary FAT (Starting at #10 with a length of 9) was the same. Therefore, all sectors were set as unallocated.

Next, the Root Directory area was examined. The 'Data Unit' mode was used again and sectors 19-32 were viewed (starting #19 and length of 14). Using the hex view, it was obvious that this was also full of 0's.

So far, this looked like an empty floppy, so that Data Area Area (sector 33) was examined. Using the 'Data Unit' mode, it was observed that the 'File Type' of sector 33 was `JPEG image data` and the the `JFIF` header value was observed (screen shot).

Unallocated Directory Entries

Although the root directory was wiped, subdirectory structures could still exist in the Data Area. The `ils` tool in TASK was used to check this:

```
% ils -f fat12 -e scan26
class|host|device|start_time
ils|host|scan26|1045803902
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_mode|st_nlink|st_size|st_block0|st_block1
2|a|0|0|0|0|0|40000|1|7168|1|0
```

This output showed that no other directories exist in the image except for the root directory, which was empty.

Analysis

Our quick hits analysis did not turn up many results. The root directory and FAT were wiped. Therefore, the traditional quick hits such as file activity timelines and file content analysis did not work.

Data Extraction

The previous section showed a JPEG image starting in sector 33. To analyze the Data Area, the unallocated space was extracted from the image. In this specific case, this step could probably be skipped because most of the file system image is unallocated Data Area space. The unallocated data was extracted from the 'Keyword Search' mode of Autopsy using the 'Extract Unallocated' button.

Data File #1	
File:	output/scan26.dls
MD5:	1FA19002023D3B1D1CF172F5CEE1635C
Source:	images/scan26
Sectors:	Unallocated

The strings were also extracted from the unallocated space. This was done with the 'Extract Strings' button.

Data File #2	
File:	output/scan26.dls.str
MD5:	D21B442595D3FBFA84BF18C5E66DF02
Source:	output/scan26.dls
Sectors:	Strings File

Doing a quick examination of this file from the command line showed uninteresting ASCII strings until the end of the image.

```
% less output/scan26.dls.str
...
31777 " ""
31782 " ""
31787 " ""
31862 h%ad
31945 H:qV
32006 kcpkt
32032 {:'�
32183 kA$4
```

```
    1210704 pw=help
    1385824 John Smith's Address: 1212 Main Street, Jones, FL 00001
```

At byte offset 1210704 of the `scan26.dls` image the string **pw=help** was found. This translated to sector 2364 of the unallocated space image. To identify the sector in the original image and to view the entire sector, Autopsy was used in Data Unit mode. Autopsy translated sector 2364 of the unallocated image to 2397 of the full image. The sector was filled with 0xf6 besides the identified string.

Finding #1	
String:	pw=help
File:	output/scan.26.dls
Byte Offset:	1210704
Sector:	2364
Original Sector:	2397

At byte offset 1385824 of the `scan26.dls` image the string **John Smith's Address: 1212 Main Street, Jones, FL 00001** was found. This translated to sector 2706, (1385824 / 512), of the unallocated space image. When viewed in Autopsy, the contents of sector 2739 in the original image were shown. As with the other sector, it was filled with 0xf6 in all bytes not used by the address.

Finding #2	
String:	John Smith's Address: 1212 Main Street, Jones, FL 00001
File:	output/scan.26.dls
Byte Offset:	1385824
Sector:	2706
Original Sector:	2739

Data Carving

The 'foremost' tool was used to analyze the unallocated space file. 'foremost' looks for header and footer values to identify known file types. The following was run from the `output` directory in the host:

```
    % mkdir foremost
    % foremost -o foremost scan26.dls
```

'foremost' found one 32602-byte data file that began at the start of the `scan26.dls` file. It can be found here. The 32602-byte picture was calculated to occupy 64 sectors (((32602 + 511) / 512) = 64 sectors).

Data File #3	

File:	output/foremost/00000000.jpg
MD5:	aee13c3e61441da124125fc1f9e9b869
Source:	output/scan26.dls
Sectors:	0-63

The picture showed a map with an **X** at **Danny's Pier 12 Boat Lunch** on Shore Line Drive.

Finding #3	
Location:	Danny's Pier 12
File:	output/foremost/00000000.jpg

Autopsy was used to view the next sector of the disk to see if the file type was known. In the 'Data Unit' mode, 64 was entered and the 'Unallocated' type is selected. This showed sector 97 of the original file system image with a file type of `PC bitmap data, Windows 3.x format, 720 x 540 x 24` (screen shot). If this was indeed a bitmap image, we were unsure of the total size of it. ('foremost' does not come with the configuration settings to identify bitmap pictures).

To find the end of the bitmap, additional file types were searched for. A quick Perl script was written that ran the 'file' command on each sector. This allowed us see if there was a new file type in the image. The output showed no other interesting file types.

As a first guess for the ending of the bitmap, the sector where the 'pw=help' string was found was used, sector 2706. Recall that the contents of this sector were all 0xf6, except for the string. The 'hexdump' tool was used to find out where 0xf6 started.

```
% hexdump scan26 | tail -15
0128e50 ffff fefe fefe ffff feff feff ffff fefe
0128e60 fffe feff feff ffff fffe ffff feff fffe
0128e70 fffe fefe fffe f6f6 f6f6 f6f6 f6f6 f6f6
0128e80 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6
*
012bb50 7077 3d68 656c 70f6 f6f6 f6f6 f6f6 f6f6
012bb60 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6
*
0156760 4a6f 686e 2053 6d69 7468 2773 2041 6464
0156770 7265 7373 3a20 3132 3132 204d 6169 6e20
0156780 5374 7265 6574 2c20 4a6f 6e65 732c 2046
0156790 4c20 3030 3030 31f6 f6f6 f6f6 f6f6 f6f6
01567a0 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6 f6f6
*
0168000
```

The 0xf6 started at offset 0x0128e76 (1216118 in decimal), or sector 2376. The `7077` values at 0x012bb50 corresponded to the 'pw' letters. The data was extracted with 'dd':

```
dd if=input/scan26 skip=97 count=2279 of=output/sector97.bmp
```

Data File #4	
File:	output/sector97.bmp
MD5:	a068d11a4c676903c655c8e9707569a4
Source:	output/scan26
Sectors:	97-2375

The picture shows a map that is similar to the previous JPEG image, except that it also contains an **X** at 22 Jones Avenue that says Hideout.

Finding #4	
Location:	22 Jones Ave - Hideout
File:	output/sector97.bmp

Putting it Together

So far, we have recovered two maps that show a hideout (Finding #4) and Pier 12 (Finding #3). We also found a string for 'pw=help' (Finding #1) and the address of John Smith (Finding #2). The remainder of the disk was 0xf6.

The only suspicious result was the password, which has not been used yet. Since we only have pictures, there could be additional data hidden in the pictures using steganography. 'stegdetect' was used to analyze the JPEG image.

```
stegdetect -n output/foremost/00000000.jpg
output/foremost/00000000.jpg : invisible[7771](***)
```

The 'invisible' shows that the 'Invisible Secrets' tool was used to hide data in the JPEG photo. The picture was imported into the Invisible Secrets tool and the 'help' password was used, the program said that it was an incorrect password.

To identify other password options, the police report was consulted for clues. The floppy disk had 'dfrws.org' written on it and the Joe Jacobs police report had a document that said that the 'goodtimes' password was the same as the "previous file". Both of those passwords were tried and were unsuccessful.

After receiving an "anonymous" tip, the actual dfrws.org website was examined. The site appeared normal, but two passwords were found upon viewing the HTML source. They were 'lefty' and 'right'.

Finding #5	
String:	PW=lefty
File:	www.dfrws.org/dfrws-overview.html

Byte Offset:	1856
Finding #6	
String:	PW=right
File:	www.dfrws.org/dfrws-overview.html
Byte Offset:	2453

The 'lefty' password was used with the Twofish decryption algorithm and the `John.doc` file was extracted.

Data File #5	
File:	John.doc
MD5:	85dba2fec1af9153a25e62a70c37d7b3
Source:	00000000.jpg

When opening this in Microsoft Word a password was required. The 'help' password was used and opened the document. Its contents can be found here. The document showed the following:

Finding #7	
Relationship:	Joe Jacobs was indeed a dealer for Jimmy Jungle
Source:	John.doc
Finding #8	
Relationship:	John Smith was the supplier for Jimmy Jungle
Source:	John.doc
Finding #9	
Relationship:	Danny's Pier was used for pickups
Source:	John.doc
Finding #10	
Location:	Jimmy Jungle is hiding out
Source:	John.doc

Finding #11	
Location:	John Smith had a condo in Aruba
Source:	John.doc

We still have one more password left though, 'right'. The bitmap photo could not be tested with stegdetect, but Invisible Secrets supports bitmaps. It was imported and the 'right' password was used. The result was `Jimmy.wav`, which can be found here.

Data File #6	
File:	Jimmy.wav
MD5:	27de3209e3b68414a7429e4104c22185
Source:	Sector97.bmp

The wav file contains Jimmy Jungle speaking instructions for a meeting tomorrow at the pier.

Finding #12	
Event:	Meeting at the pier tomorrow with Jimmy Jungle
Source:	Jimmy.wav
Finding #13	
Location:	Jimmy drives a 1978 Blue Mustang with Ontario plates
Source:	Jimmy.wav

We have finally exhausted the available data from the floppy and handed the data to the police. Hopefully, they will be ready for the meeting at the pier.

Questions

Who is the probable supplier of drugs to Jimmy Jungle?: From the document extracted, John Smith was the probable supplier of drugs.

What is the mailing address of Jimmy Jungle's probable drug supplier?: From the unallocated space on the disk, the following address was found:

> 1212 Main Street
> Jones, FL 00001

What is the exact location in which Jimmy Jungle received the drugs?: According to the extracted document and maps, the drugs come in via boat to Danny's, which was on Pier 12.

Where is Jimmy Jungle currently hiding?: From the extracted document and recovered bitmap, Jimmy was at 22 Jones Ave.

What kind of car is Jimmy Jungle driving?: 1978 Blue Mustang with Ontario Plates.

Bonus Question: The root directory and FAT were wiped and the data area was not because the disk had been "Quick" formatted.

Acknowledgments

Thanks to Dan Kalil for a great challenge!