



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>

Camouflaged and Attacked?

By
Bertha Marasky
GCFA Practical Assignment v1.5
Part 1 & Part 2 Option 2
6 March 2005

© SANS Institute 2005, Author retains full rights.

TABLE OF CONTENTS

<u>Synopsis</u>	5
<u>Part 1 – Camouflaged - Theft from Ballard Industries</u>	6
<u>Background</u>	6
<u>Chronology</u>	6
<u>Preliminary Examination Detail</u>	9
<u>Evidence Handling</u>	9
<u>Initial Investigative Steps</u>	10
<u>Investigation Environment</u>	10
<u>Case Management</u>	11
<u>Image Details</u>	13
<u>Timeline Creation</u>	14
<u>The Dirty Word List</u>	15
<u>Image Content Analysis</u>	16
<u>Deleted HTML File Analysis</u>	19
<u>Deleted DLL File Analysis</u>	21
<u>File Size Analysis</u>	22
<u>Program Identification</u>	23
<u>Steganography Tool Installation</u>	23
<u>Uncovering of Hidden Data</u>	23
<u>Steganography Tool Confirmation</u>	25
<u>Forensic Details</u>	27
<u>Steganography Tool Analysis</u>	27
<u>Action Duplication</u>	29
<u>Sequence of Events</u>	31
<u>Tool Removal Analysis</u>	33
<u>Legal Implications</u>	33
<u>Follow Up Recommendations</u>	35
<u>Part 2 – Attacked? - Tools of the Trade</u>	37
<u>Scope</u>	37
<u>Tool Description</u>	38
<u>Forensic Benefit</u>	38
<u>Selected Tool</u>	40
<u>Malware Signatures</u>	41
<u>Creating An Evidentiary Sound Tool</u>	41
<u>Test Apparatus</u>	43
<u>Environmental Conditions</u>	43
<u>Procedure Description</u>	43
<u>Approval Criteria</u>	45
<u>Data, Results and Analysis</u>	45
<u>Precursor Testing Of Tool Impact on System</u>	45
<u>Controlled Test 1 – Keystroke Logger</u>	48

<u>Controlled Test 2 - Packer</u>	51
<u>Controlled Test 3 - Backdoor</u>	52
<u>Uncontrolled Test 1 – Unknown System</u>	53
<u>Presentation</u>	54
<u>Conclusion</u>	55
<u>Exhibit A – Recovered Policy Documents</u>	57
<u>Acceptable Encryption Policy</u>	57
<u>Information Sensitivity Policy</u>	58
<u>Internal Lab Security Policy</u>	63
<u>Internal Lab Security Policy1</u>	66
<u>Password Policy</u>	69
<u>Remote Access Policy</u>	72
<u>Exhibit B – MAC TimeLine – Leszczynski Floppy</u>	75
<u>Exhibit C – MAC TimeLine – Test Floppy Image</u>	76
<u>Exhibit D – Deleted HTML File</u>	77
<u>Exhibit E – Recovered Letter of Intent to Commit Crime</u>	78
<u>Exhibit F – Recovered Client Authorized Table Database</u>	79
<u>Exhibit G – Recovered Design Schematics</u>	80
<u>Appendix A – Camouflage System Modifications</u>	83
<u>Appendix B – Summary of File Info to Aid in Determining Sequence of Events</u>	90
<u>Appendix C – Registry Entries After Tool Removal</u>	91
<u>Appendix D – Relevant Statutes</u>	95
<u>Appendix E – PestPatrol Evaluation License</u>	97
<u>Appendix F – Listing of Pest Detection Tools CD-ROM</u>	99
<u>Appendix G – PestPatrol System Modifications</u>	100
<u>Appendix H – PestPatrol IKS Output Log</u>	103
<u>Appendix I – Unknown System PestPatrol Output</u>	105
<u>References</u>	138
<u>Summary of Informational References</u>	140
<u>Summary of Download Site References</u>	141

TABLE OF FIGURES

<u>Figure 1 – Autopsy Case Details</u>	11
<u>Figure 2 – Autopsy Host Details</u>	12
<u>Figure 3 - Autopsy Host Manager Image Details</u>	13
<u>Figure 4 – Autopsy - Host Selected - Image Details</u>	16
<u>Figure 5 - Autopsy File Analysis</u>	17
<u>Figure 6 - Autopsy Meta Data</u>	18
<u>Figure 7 - Autopsy Data Unit</u>	19
<u>Figure 8 - Successful Un-Camouflage</u>	24
<u>Figure 9 - ReCamo Test File Listing</u>	28
<u>Figure 10 - Test Camouflage File Analysis</u>	30
<u>Figure 11 - Files Before Camo, NTFS</u>	31
<u>Figure 12 - Files After Camo</u>	32
<u>Figure 13 - PestPatrol Configuration Options</u>	42
<u>Figure 14 – Create Winalysis Snapshot</u>	45
<u>Figure 15 - PestPatrol Scan</u>	46
<u>Figure 16 - PestPatrol Changes Via Winalysis</u>	47
<u>Figure 17 - Invisible Keylogger Install</u>	49
<u>Figure 18 - Pest Found in Memory</u>	49
<u>Figure 19 - PestPatrol After Keylogger Install</u>	50
<u>Figure 20 - Pest Patrol "What to Search For Option"</u>	51
<u>Figure 21 - Back Orifice Installation</u>	52
<u>Figure 22 - PestPatrol Running Processes</u>	53

© SANS Institute Author retains full rights.

Synopsis

A major fuel cell battery company finds loyal customers are not reordering a particular design. Queries reveal that they are now ordering from a competitor. Forensic investigation of a floppy disk confiscated from an engineer leaving company premises reveals theft of trade secrets. There is evidence that a Steganography¹ tool was used to conceal information that is integral to the success of the company on the floppy. A hidden letter was uncovered from the floppy that was “signed” by the engineer. It included clues used to reveal more hidden information and admission that his intent was to provide company protected information to a source for profit. The protected company information included a database of customer information and schematic documents that had not yet been released. Federal statute 18 U.S.C. 1832, Theft of Trade Secrets is applicable. Section 31.05 of the Texas Penal Code, Theft of Trade Secrets is applicable. Additionally, company policies which prohibit the distribution of this classification of data were violated and it is spelled out that prosecution may be a result. Part I of this document provides step-by-step investigation details, findings, violations information and further investigation suggestions.

Part II considers the forensic application of a tool used for computer “pest” management. The intent is to show that when forensics is being performed on a copy of an image in a revertible environment, this tool could be used to quickly verify an incident has occurred, possibly give clues where to dig deeper and maybe even give an idea of the motive for attack. This document shows the tool can be run from forensically sound media, procedures used to understand modifications the tool introduces and provides real life examples.

Throughout Part I and Part II, forensics concepts and methodologies are presented.

¹ <http://www.webopedia.com/TERM/S/steganography.html> (ste-g&n-o'gr&-f•) (n.) The art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography literally means *covered writing*.

Part 1 – Camouflaged - Theft from Ballard Industries

Background

Ballard Industries is a company that designs specialized fuel cell batteries. The Vice President of the sales department, Bob Clements, had noticed that after years of successful relationships, many of Ballard's loyal clients had not been re-ordering from them -- particularly those that had been using a newer fuel cell battery design. Clements personally made follow-up calls to clients and discovered that they had been placing orders with one of Ballard's major competitors, Rift Inc. Since this design had been unique to Ballard for quite some time, an investigation ensued. It was believed that proprietary information had been provided to Rift. It was also feared that somehow the customer database of all Ballard's clients had been released along with the proprietary information. The lead process control engineer for the project is Robert John Leszczynski, Jr. The security administrator is David Keen. The only potential physical evidence available was a floppy disk. Leszczynski had been leaving one of Ballard's Research and Development labs on April 26, 2004, around 4:45pm MST, and it was discovered in his briefcase. Taking removable media off premises is against company policy, so the security guard seized the disk and told Leszczynski he could recover it from Keen.

Chronology

The following lists forensics procedures and findings as presented in this paper. Examination detail follows this listing.

Preliminary Examination Detail

1. A copy of a seized floppy disk that contained potential evidence was obtained.
2. The md5 tool was used to verify the evidence tracking information matched the image received.
3. It was determined the image was of filesystem type FAT12.
4. The investigation environment is described.
5. Case management using the Autopsy tool is presented.

Image Details

6. A listing of the intact allocated files was obtained after mounting the image on a local loopback device using the Unix mount and ls commands. Copies of these Ballard policy documents which were in Microsoft Word format are included as an Exhibit.
7. A MAC timeline was created using Autopsy create timeline feature in combination with the mactime tool. This timeline showed the six intact files in addition to two deleted files. Timeline included as an Exhibit.
8. An initial dirty word list was created using the Unix vi text editor and

- applied to the image using the Unix strings and grep commands. Nothing in addition to what had been seen was apparent at this point.
9. Using Autopsy File, Meta Data and Data Unit Analysis functions, it was discovered that three of the six Word documents had what appeared to be unexplained binary data following the Unicode. Additionally, an anomaly was noted that both deleted files pointed to the same image sector.
 10. The foremost utility was used to extract a deleted HTML file, included as an Exhibit. Analysis revealed the webpage used Macromedia Shockwave Flashplayer to display a .swf file. A hex editor was used to identify the .swf file identification pattern. The foremost utility was used to attempt extraction of a hidden or deleted .swf file. This was not found.
 11. A Google search for the deleted filename CamShell.dll did not find any matches. The string "shell" was added to the dirty word list. Searching for this string revealed a reference to CamouflageShell. A Google search for this string led to a SANS posted article on a Steganography tool called Camouflage.
 12. File size analysis reveals files with discrepancies between layer views.

Program Identification

13. The significance of the "extra" binary data was realized in that it was possible the Camouflage tool was used on these files.
14. An executable version of the Camouflage v1.2.1 tool is downloaded and installed. The Readme file is reviewed and familiarity with the tool was gained.
15. The Camouflage tool was used to reveal a hidden letter of intent to commit crime that was not password protected. Letter is attached as an Exhibit.
16. This letter held clues that lead to the passwords protecting the other two altered Word documents. The recovered company protected information, which included the customer database and design schematics, are attached as Exhibits.
17. To confirm the use of the Camouflage tool (in addition to the ability to unlock the hidden files) the md5 tool was used to compare the installed CamShell.dll file and the partial one extracted from the image. The DLL file was extracted from the image using the Unix dd command. The HTML code analyzed previously actually occupied the first portion of the extracted DLL file, so a hex editor was used to remove an appropriate amount of data from the beginning of both files before the md5 sum was validated.
18. An md5 listing of all unCamouflaged files compared to an md5 listing of the intact files, listed when the image was locally mounted, showed another fact that seemed to reinforce the use of the tool. The md5 sum of one of the files that had not been tampered with matched the sum of a similarly named extracted file.
19. An unsuccessful attempt was made to replicate the md5 sum of a

Camouflaged file using the extracted files. It appeared the tool uses a volatile seed when calculating the hash.

Forensic Detail

20. A system modification audit tool named Winalysis was used to identify file and registry changes that occur when the Camouflage tool is used. The DOS format utility was used to erase a floppy disk for testing purposes.
21. The Camouflage utility was used to create a floppy disk that included a Camouflaged file directly to the disk, one created on a different disk and copied to the floppy, and a standard text file. A MAC timeline of this new floppy was created. This information along with directory listings of the files allowed an understanding of the behavior of the tool under different circumstances. It was determined that the Camouflaged files were created on a different disk and copied to the floppy.
22. The timeline from the original floppy along with the knowledge of the tools behavior allowed a sequence of events relative to the floppy's creation to be proposed.
23. Removal of the Camouflage tool was analyzed by using the Windows Remove Programs option and the regedit tool. These modifications would be helpful only if one had access to the Ballard systems on which the Camouflage action took place.

Legal Implications

24. The examination revealed the seized floppy disk contained company proprietary information. The suspect was in the process of leaving the building with said floppy. Theft of trade secrets appears ascertained.
25. Applicable statutes include Federal 18 U.S.C. 1832, Theft of Trade Secrets and Section 31.05 of the Texas Penal Code, Theft of Trade Secrets.
26. It is described that the company Information Sensitivity Policy was violated and prosecution is a potential consequence.

Follow Up Recommendations

27. Suggestions are given that provide specific information that a systems administrator or company forensic investigator could pursue to strengthen the case.
28. Additional violation was cited as potential based on future findings.

Preliminary Examination Detail

Evidence Handling

I was engaged to do computer forensics investigation. The floppy was provided to me accompanied by a chain of custody form containing the following information:

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

Keeping track of evidence is absolutely necessary. If an investigator ends up testifying in court, he needs to be able to explain exactly how the evidence was handled, otherwise, the credibility of his conclusions may be in doubt. I verified the tag number on the form matched the number on the disk.

I also verified the image I obtained was a bit-for-bit copy of the original. Forensics investigation should always take place on a copy of the original evidence if at all possible. There are circumstances that may warrant an investigation taking place on an operational or “live” system, but that was definitely not the case here since we are dealing with removable storage media that was not in the process of being updated when it was obtained. As forensics procedures are performed, the state of the evidence will change. Minimally, all modification must be understood, explainable, and documented, ready for court if necessary.

One tool used to aid in maintaining evidence integrity is the md5 checksum. One reference describes the tool as follows:

The MD5 program generates a unique, 128-bit cryptographic message digest value derived from the contents of a file. This value is considered to be a highly reliable fingerprint that can be used to verify the integrity of the file's contents. If as little as a single bit value in the file is modified, the MD5 checksum for the file changes. Forgery of a file in a way that causes MD5 to generate the same result as that for the original file is considered to be extremely difficult.²

Think of it kind of like a human fingerprint. No two are alike and when comparing, if any reference points don't match, you have to question whether or not they came from the same person. For anyone that wants to delve into the nuts and bolts of the program, see [RFC 1321 - The MD5 Message-Digest Algorithm](#).³ This mechanism can be used for evidence tracking and during

² <http://www.cert.org/security-improvement/implementations/i002.01.html>

forensics investigation to monitor changes. After you receive the data and make it accessible on the system where you will do the examination, you can use an md5 tool to verify that the file you have has that same hash value as the one listed on the evidence tracking form. If you have a match, you are good to go. As you are digging through the haystack, looking for the needle, you can use md5 sums to verify you have returned back to the original image if you find the need, verify results are repeatable, or use it to compare any two files to ensure they are exact.

Initial Investigative Steps

Of course, the first thing I did, once I got the file unzipped, was verify that the md5 sum matched the one given on the evidence tracking form. I was a bit concerned because the filename listed on the evidence form did not match the name of the file made available to me. Running the md5 command against the file returned the same value though, so I was sure the image was indeed an exact copy of the one referenced on the form.

```
# md5 v1_5
d7641eb4da871d980adbe4d371eda2ad v1_5 (it's a match!)
```

Next, I wanted to have an idea what type of image I would be working with, so I used the Unix "file" command.

```
# file v1_5
v1_5: 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)
```

FAT12, that tells me something. FAT stands for File Allocation Table. FAT is the filesystem supported by MS-DOS that was originally developed for floppy drives. Knowing the filesystem structure is very important when trying to extract files or partial files from media. A helpful tutorial like presentation on the FAT filesystem can be found at <http://faculty.cs.byu.edu/~seamons/cs345/FatTutorial-Seamons.pdf>.

Investigation Environment

I took the floppy disk back to my lab and copied the disk image to one of my forensics machines. The one I used is an HP Pavilion ze4500 that has an AMD Athlon™ XP2500 chip. It has 1GB of memory and a 40GB hard drive. While the system has both Ethernet and wireless capabilities, all network interfaces are disabled, so it is in essence a standalone system. Currently, I have Red Hat

³ <http://www.fags.org/rfcs/rfc1321.html>

Fedora Core 1 loaded along with VMWare version 4.5.1 build-7568. No operating system patches are loaded.

VMWare allows multiple virtual machines, even with different operating systems, to function simultaneously on one system. I like to use a number of forensics tools that run in a Unix world but, chances are pretty likely this disk was created in the Windows world. I had just recently installed a Windows 2000 virtual machine under VMWare, so I knew I had a clean install readily available. This set up allows me to easily transfer files between the environments, so on this one portable system I can use tools in my Unix world yet still have ready access to Windows software, like Microsoft Word. VMWare also allows me to operate on files, that have unknown origin and are potentially malicious, in an encapsulated space. VMWare also has a revert function that allows you to return to a known state without system rebuild...very handy!

Case Management

For this investigation, I chose to use Autopsy Forensic Browser for image analysis and case management. It provides a visual interface for commands you find in the suite of forensics analysis tools known as The Sleuth Kit. Autopsy helps keep all the case details in order and jumping from one piece of evidence info to another is very simple. These awesome open source tools are from Brian Carrier and are available for download at <http://www.sleuthkit.org/proj.php>.

I have Autopsy version 1.70 loaded. I start the tool using the autopsy_start script and click on New Case. I enter gcfa_v1_5 as the case name, certification practical as the description and I use the initials bem for investigator. I get a created message and click ok. That takes me back to the case screen and I select gcfa_v1_5. I see:

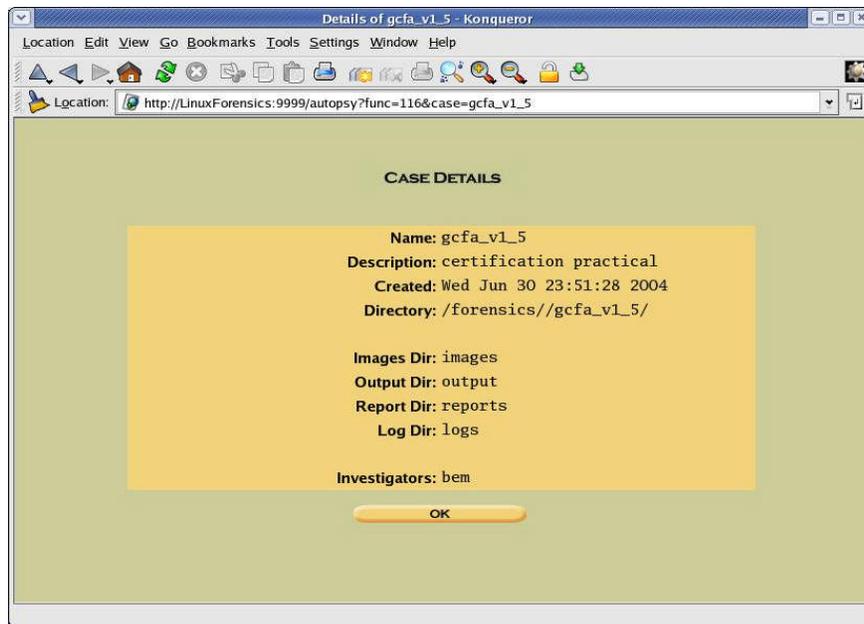


Figure 1 – Autopsy Case Details

Once I select the case from the main menu, I click on add host. After adding the relevant information for a new host called gcfa, I can click on details and see the following:

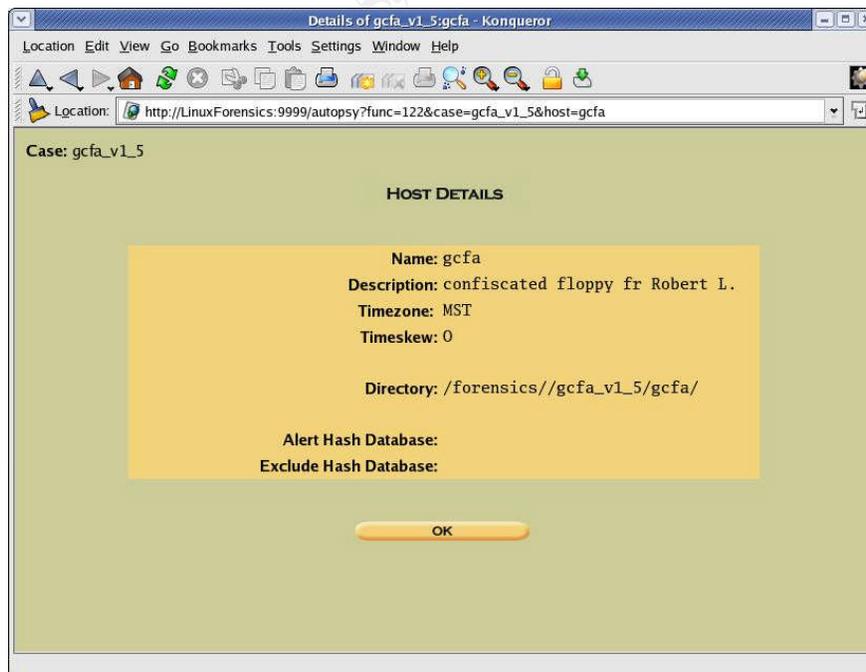


Figure 2 – Autopsy Host Details

Note I selected Mountain Time when I added this host. Time stamps are critical

during investigation as they correlate events. You can imagine it would be hard to follow the chain of events if times are not accurately understood. Skew can be compensated for, but it makes the investigator's job more tedious and increases the chance for incorrect interpretation. Mountain time is my best guess as this was the time zone in which the floppy disk was confiscated from Leszczynski.

The next step is to associate the image file itself (the one Keen gave me) to the case. I select the add image button and enter the requested information. I use the copy to evidence locker option and select FAT12 file system type. I choose to validate the md5 sum (notice the number still matches the one on the evidence form).

When I return to the Host Manager and view the details for this image I see:

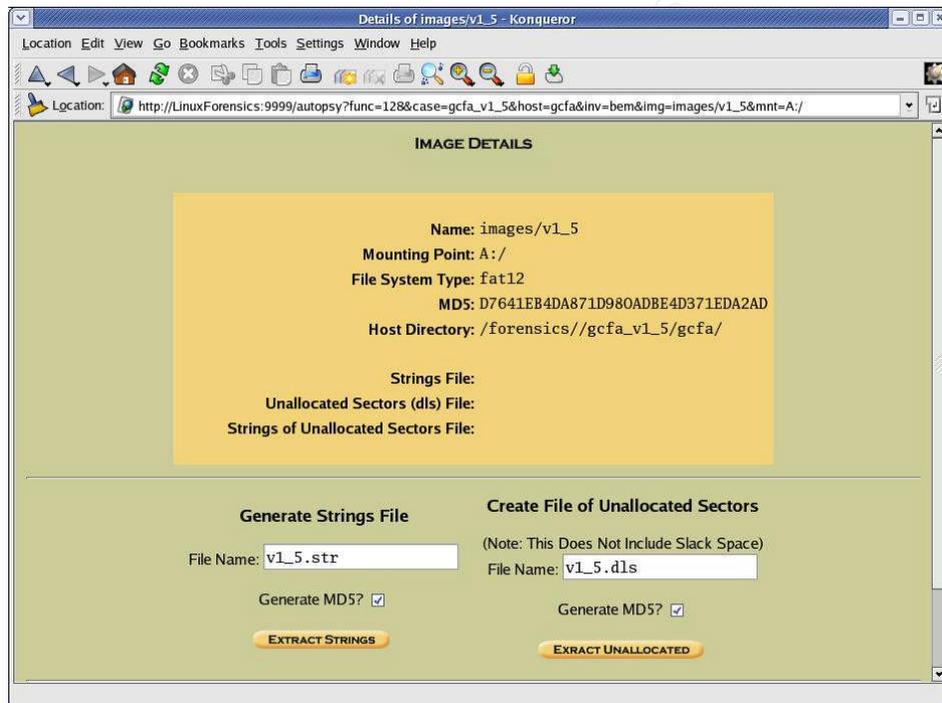


Figure 3 - Autopsy Host Manager Image Details

Regardless of the tools you use to manage an investigation, it is imperative that you keep four principles in mind⁴:

- Minimize data loss.
- Record everything.
- Analyze all data collected.
- Report your findings effectively.

⁴ Lee, Rob. Forensic and Investigative Essentials. Pg 22.

Image Details

Beginning the actual data analysis, I was first curious to see what files would appear intact, so I locally mounted the image read-only using what's called the loop device.

```
# mkdir ./view                (create a local mount point)
# mount -o loop,ro ./v1_5 ./view (mount the disk)
# ls -l ./v1_5                (show a listing of files in the image)
total 640
-rwxr-xr-x 1 root root 22528 Apr 23 14:10 Acceptable_Encryption_Policy.doc
-rwxr-xr-x 1 root root 42496 Apr 23 14:11 Information_Sensitivity_Policy.doc
-rwxr-xr-x 1 root root 32256 Apr 22 16:31 Internal_Lab_Security_Policy1.doc
-rwxr-xr-x 1 root root 33423 Apr 22 16:31 Internal_Lab_Security_Policy.doc
-rwxr-xr-x 1 root root 307935 Apr 23 11:55 Password_Policy.doc
-rwxr-xr-x 1 root root 215895 Apr 23 11:54 Remote_Access_Policy.doc
```

See [Exhibit A – Recovered Policy Documents](#) for printed versions of these recovered documents.

Timeline Creation

Creating a timeline is a prudent step in computer forensics. In an investigation on a system that cannot be taken out of operation, it is critical to gather this information very early because commands issued against the system will alter what are known as MAC times. MAC is an acronym for Modify, Access and Change. There is some slight variation in what these time stamps represent between file system types. In the FAT12 file system, these times show the last time a file was written to, accessed, or created respectively. Notice I said the last time, it is NOT a history. This timestamp data is stored in structures called meta data. Most Unix flavors refer to these structures as inodes. When dealing with NTFS filesystems they are known as master file table (MFT) entries. In this investigation, since we are dealing with a FAT filesystem, they will be referred to as directory entries. Note, it is fairly easy for a hacker to muck with these timestamps, but they can still help give clues as to what might have taken place, tie clues together, and help support determinations.

One limitation of Autopsy is timeline viewing because of the date range selection requirement. I find it easier to view and search outside of the tool. So I use the create timeline feature in Autopsy to create the body file. If I wanted to create the body file on the command line I would use the following:

```
# fls -f fat12 -m / -r v1_5 > cl_v15.fl5 (create a file of existing filename data)
# ils -f fat12 -m v1_5 > cl_v15.ils      (create a file of deleted directory entries)
# cat cl_v15.?ls > /forensics/gcfa_v1_5/gcfa/output/body (put those two together)
```

Whether I create the body file through the Autopsy interface or on the command line, I then go to the /forensics/gcfa_v1_5/gcfa/output directory and enter:

```
#mactime -b body > timeline.txt
```

The mactime command actually creates the text output from the body file (which for other cases may include multiple images). I use the Unix view command (read only version of the vi editor) to look through the file:

```
# view timeline.txt
```

See [Exhibit B – MAC TimeLine – Leszczynski Floppy](#) for a copy of the timeline.txt file. Note, when I created the body file I instructed Autopsy to include allocated files, unallocated files and unallocated meta data structures. This means I want to look at the whole disk, anything it knows is on there now or anything that may have been on there before. Looking at the timeline we see dead, deleted and regular allocated filenames. Dead means MAC time info is likely good, but the filename may be questionable. Deleted means the directory entry information is unallocated and the data pointed to may or may not be valid. Those dead and deleted references to CamShell.dll and _ndex.htm look interesting and I store that information for later recall. I also make a note that the create date appears to be the latest stamp on all the files. In this FAT12 instance, that could mean that new versions of the files were created at a different file location. Then I notice the time stamps are consistently 3 hours different than those on the File Analysis screen in Autopsy, so I may have some time skew that I will need to keep in mind.

The Dirty Word List

I review the notes I had made during my conversation with Keen and begin to make a list of words that may give me a lead to pursue if any of them are found somewhere in the image. This is known as a dirty word list. You can always add to the list so it makes sense to get started early in the investigation. So far I have the following in a file called dirty_words.txt:

```
Ballard  
Robert  
John  
Leszczynski  
fuel  
cell  
battery  
Rift  
customer  
confidential  
proprietary
```

I tried running the command

```
# strings v1_5 | grep -if dirty_words.txt
```

to see if something might jump out at me, but generally speaking, it just displayed a good chunk of the Word documents you will see shortly. What the command did was pull everything out of the whole floppy image that it considered regular text and then it searched that output for any word in my dirty word list. I also instructed it to disregard upper and lower case. There were a couple tidbits that I made note of -- I saw what appeared to be an HTML header and references to DLL files. HTML is the language many web pages on the internet are written in and DLL files are libraries used by running programs. Program libraries are kind of like real libraries. They contain information that everyone shares. I classified the HTML as worth looking into and the DLL files may certainly prove to be important.

Image Content Analysis

At this point I chose to get back into Autopsy. I pulled up the Image Details screen as shown below:

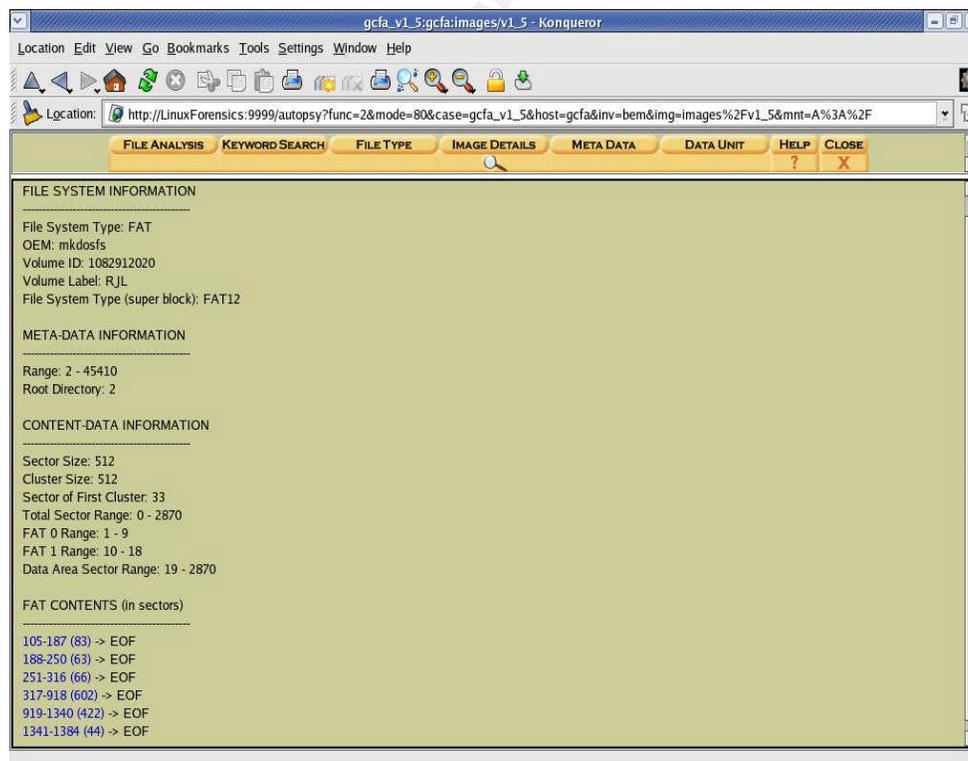


Figure 4 – Autopsy - Host Selected - Image Details

This screen allows me to see details about the image I obtained from Keen. I see confirmation that it is indeed a FAT12 filesystem. I note the sector/cluster size is 512. When analyzing an image this is a vital piece of information for understanding how data was written to the disk. This display also shows the sector numbers allocated to the known (non-deleted) files. These sector numbers represent the location on the disk where the file data is actually stored. In Autopsy, you can click on those sector numbers and jump right to viewing the data at that location. If I wanted to use the command line utilities to see information similar to the Image Details I would type:

```
# fsstat -f fat12 v1_5 (the output would appear the same as above,
however, you would need to use additional tools to view the sector content)
```

What I want to do now is get more detail about the information represented by those sectors. I know there appears to be six Word documents, but what else might be there? Does anything else look out of the ordinary?

Clicking on the file analysis tab there are those six Word documents and the deleted file references I saw on the timeline.

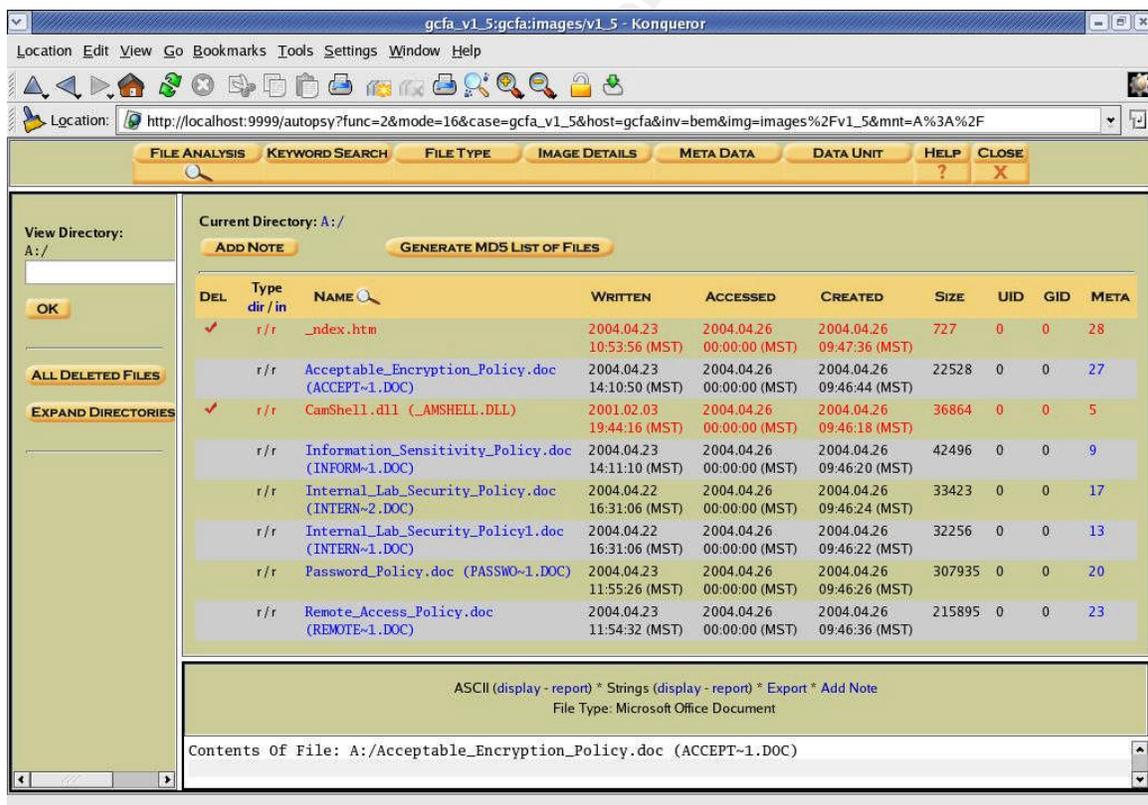


Figure 5 - Autopsy File Analysis

You can think of files and directories like a filing cabinet. A directory is a separate drawer and files are the things you put inside. This floppy image only

has one drawer. There are six intact items and two that may be damaged.

I begin browsing the data and click on `Acceptable_Encryption_Policy.doc`. If you look at the bottom pane of the display it will show an ASCII representation of the file. ASCII is basically a text version of the data. With Word documents it is a bit illegible because Word uses Unicode and ASCII representation does not interpret the Unicode. Unicode is a standard way of efficiently encoding characters so that no matter what spoken language you need to view the file in, it will display correctly. Unicode is presented as readable text if you use the Strings report function. So, I click on the Strings report function and it looks pretty typical. Details about the file like the title, the Word template used, version of Word, that sort of information is down at the bottom. I do the same for `Internal_Lab_Security_Policy.doc` and there is definitely some extra data at the end of the file beyond the Unicode. I do this for each of the six doc files and I make a note that three of them look like they have this extra non readable text. I am not sure of the significance at this point, but I highlight this information for later reference.

Now, let me look a little closer look at those deleted entries. To the far right of the filename `_ndex.htm`, there is a 28 under the Meta column. I click on that 28 and it takes me to the Meta Data analysis screen for this particular file. Remember the metadata, also known as a directory entry when dealing with a FAT filesystem, is information about the file, like MAC times and pointers to where the data actually resides on the disk.

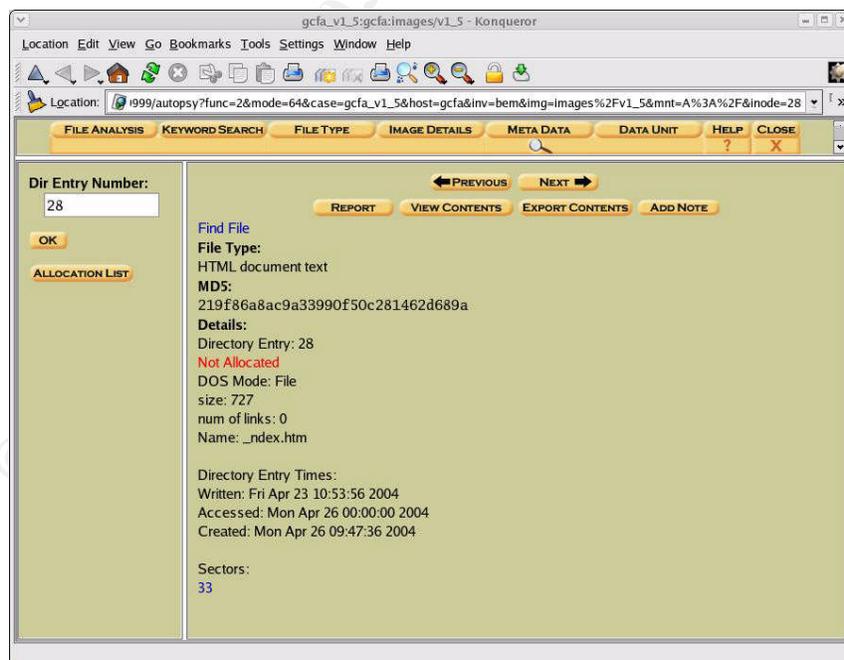


Figure 6 - Autopsy Meta Data

To get this same information using a command line tool I would type:

istat -f fat12 v1_5 28 (to see directory entry 28 in image v1_5)

In Autopsy I can click on a sector number (which points to the actual location on disk) and it will take me to the Data Unit analysis screen for sector 33. There I will see the actual contents of that sector.

The command line equivalent would be:

icat -f fat12 v1_5 28 (to see the contents of the sector pointed to by directory entry 28)

Think of it this way, the Image Detail (v1_5 of type FAT12) is the card catalog at the library. The File Analysis is the drawer containing the information about the desired book (named _ndex.html). The Metadata (directory entry 28) is the card containing the location information for the book. The Data Unit (sector 33) is the shelf location where the book is stored. Proceed to that location and begin to read.

Jumping to sector 33, it looks like that HTML file I saw when I ran the strings command earlier.

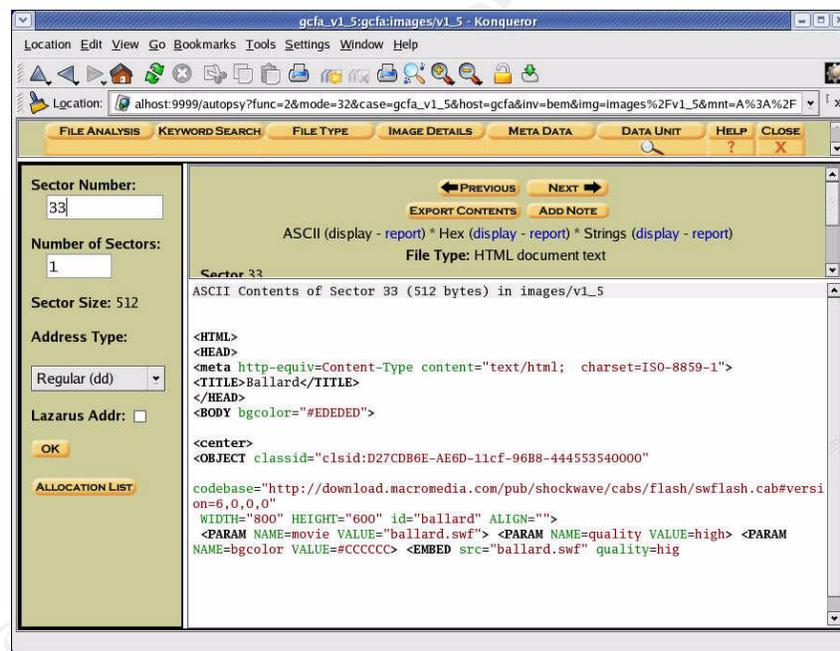


Figure 7 - Autopsy Data Unit

I went back to the File Analysis screen and clicked on the metadata number for the deleted .dll file, which was 5. I noted an anomaly. Both directory entry 5 and directory entry 28 show sector 33 as the only location for data. Additionally, looking back at the file analysis for directory entry 28, I saw it was supposed to be 727 bytes big. It won't fit in just one sector because, if you remember from the Image Analysis screen, on this FAT12 disk, a sector is 512 bytes -- 727

bytes won't fit in just one sector. At this point I knew the metadata for these two files was not reliable.

Deleted HTML File Analysis

I decided to investigate the HTML file a bit to see if it held a clue. Although the HTML file could have been extracted a number of ways, I used a utility called Foremost. It is a program used to recover files based on their headers and footers. It is available from <http://foremost.sourceforge.net/>. You define what the headers and footers are supposed to look like in a configuration file. I intend to use it to extract from a file that will contain only the unallocated space in the image, which includes deleted files. This file does not include the space that is occupied by the six Word documents (which is considered allocated space).

```
# dls -f fat12 v1_5 unalloc_v1_5.dls (create image of unallocated space only)
```

I verified the configuration file was set to minimally attempt to identify .gif, .jpg, .png, .htm, .pdf, .wav, .zip, .exe and .tar files and then typed:

```
# foremost -v -o /gcfa -c /usr/local/src/foremost/foremost.conf /gcfa/unalloc_v1_5.dls  
(use the configuration file named after -c, put the output in /gcfa)
```

After the command completed, in the output directory I typed:

```
# ls -l  
total 8  
-rw-r--r-- 1 root root 725 Jun 30 2004 00000000.htm  
-rw-r--r-- 1 root root 526 Jun 30 2004 audit.txt
```

See [Exhibit D – Deleted HTML File](#) for the content of 00000000.htm. The audit.txt file is just a summary of what foremost found.

I chose to attempt viewing the HTML file in my encapsulated Windows environment in VMWare just in case it might be malicious. I copied the file to the mount point shared between my Unix workstation and the VMWare environment. I fired up VMWare and did a revert on the saved Windows environment. I called up the Internet Explorer browser and attempted to open the 00000000.htm file. It began loading, but then appeared to hang. Viewing the source code I see it is looking for MacroMedia Shockwave FlashPlayer. I do not allow this VMWare partition to access the internet, so I manually downloaded FlashPlayer, moved it to the shared mount point and installed it. The HTML page still appeared to hang on load.

Next up was trying to interpret the HTML. I did a Google search for clsid:D27CDB6E-AE6D-11cf-96B8-444553540000 (which is the text that followed the OBJECT classid= element). Google is a service available on the internet that essentially scours millions of files looking for references to the string you type in. I ended up at <http://toolittletime.com/free/f01.html>. It is a

website for free flash introductions. I now understand this webpage uses Shockwave Flash Player to load a file called ballard.swf. I didn't have a file called ballard.swf, so I downloaded the file TLTClock.swf from toolittletime and renamed it ballard.swf in my forensics environment. Now when I browse to that file, I see an actual running clock that says TooLittleTime.com and some flashing text in the bottom half of the clock. The HTML file seems intact. To see the webpage as originally written I just need the .swf Shockwave Flash file called ballard.swf that is referenced in the HTML.

I opened a number of .swf files in a hex editor to see if I could identify a common header and footer. I did come up with pattern 46 57 53 for a header and a footer of 40 00 00 00. I added a swf definition to the foremost configuration file and tried rerunning the tool. No .swf files were identified in the image file based on the definition I used.

Deleted DLL File Analysis

I decided it was time to do a Google search for CAMSHELL.DLL, which is the name of the other deleted file, but didn't get a hit. I added shell to my dirty word list (so the list would be complete), but then did a manual search for just shell:

```
# strings v1_5 | grep -i shell
AMSHELLDLL
ll\SheCamouflageShell
ShellExt
CamShell
BitmapShellMenu
CamouflageShell
CamouflageShell
Shell_Declares
Shell_Functions
ShellExt
modShellRegistry
shell32.dll
IShellExtInit_Initialize
FIShellExtInit
C:\My Documents\VB Programs\Camouflage\Shell\IctxMenu.tlb
IShellExtInit
CamShell.dll
lCamouflageShellW
_ShellExtWWWd
_ShellExt
```

This time I did a Google search using CamouflageShell and did get a hit. The reference was to an article in the SANS reading room. The article was titled "Steganography: The Ease of Camouflage"⁵. It turned out to have some very

⁵ <http://www.sans.org/rr/papers/20/762.pdf> Later referenced in this document as the SANS Steganography paper

interesting information indeed. It described how a tool called Camouflage could be used to embed a file into any other type of file while allowing that other file to still function as originally intended. For example, a .jpg, a picture format, file could be “inserted” into a Word document. The Word document could be viewed and copied without it being obvious it contained any other information. The Camouflage tool is required to embed and remove the hidden file. One key piece of information was that Camouflage uses a Steganography technique that appends the extra file, encrypted, to the original file. That means two things: 1) the resulting camouflaged file will have a different size than the original document and 2) viewing the contents of the camouflage file in a tool not normally used to access that file type will likely show something out of the ordinary. Recall the extra non-readable data I saw at the end of three of the Word documents when I was doing the [Image Content Analysis](#) previously.

File Size Analysis

A disk has 5 different layers which could be considered views or perspectives⁶:

- Physical Layer – the drive itself.
- Data Layer – where the data is stored. Units of reference are sectors or clusters. They are either allocated or not.
- Metadata Layer – structures that store information about a file such as MACtimes, owner, size. For this FAT12 disk we reference these structures by a directory entry number.
- File System Layer – contains information relative to mounting the disk in the operating system environment.
- File Name Layer – makes the correlation between a name (which is much easier to remember) and a metadata structure number. With a FAT filesystem this structure is actually the same as the metadata structure.

The Image Details view in Autopsy or the fsstat command shows file allocation information from the data layer perspective. From the image detail I recalled the FAT Contents (sector allocation) information:

105-187 (83) -> EOF	x 512 = 42496
188-250 (63) -> EOF	x 512 = 32256
251-316 (66) -> EOF	x 512 = 33792
317-918 (602) -> EOF	x 512 = 308224
919-1340 (422) -> EOF	x 512 = 216064
1341-1384 (44) -> EOF	x 512 = 22528

I multiplied each number in parentheses (total sectors) by 512 (sector size in bytes). For those of you not familiar with the term, a byte is a unit of

⁶ Paraphrased from Lee, Rob. [Forensic and Investigative Essentials](#). Pgs 75-82.

measurement used in computing. A byte is 8 bits. Each bit can represent one alphanumeric character.

The File Analysis view in Autopsy or the `istat`, `ils`, and `fls` commands are using metadata and file name layers views. I used the `ils -af fat12 v1_5` command to list the allocated directory entry numbers. I used the `istat -f fat12 v1_5 dirent#` command for each directory entry number and compiled the following information which allows me to tie the filename to sectors.

Dir Ent #	Starting Sector	Filename	Size
9	105	Information_Sensitivity_Policy.doc	42496
13	188	Internal_Lab_Security_Policy.doc	32256
17	251	Internal_Lab_Security_Policy1.doc	33423
20	317	Password_Policy.doc	307935
23	919	Remote_Access_Policy.doc	215895
27	1341	Acceptable_Encryption_Policy.doc	22528

When space is allocated for a file it is done by sectors, even if the whole sector is not used. When viewing this allocated space from the data layer, you will see numbers that represent the total number of sectors, regardless of whether or not only a fraction of the sector is used. When the same file is viewed from the metadata layer, the size reflects only the actual size of the file. The following three files inconsistently report size when viewed from different layer perspectives and therefore have portions of sectors that should be accounted for:

Internal_Lab_Security_Policy.doc
Password_Policy.doc
Remote_Access_Policy.doc

Program Identification

Since the article referenced CamouflageShell and I had seen that in the deleted space on the image, I considered it a possibility that the Camouflage software had been used on this data.

Steganography Tool Installation

Unfortunately, I couldn't find the software referenced at the location listed in the article, so I had to search around a bit. I could not find the source code online. At <http://camouflage.unfiction.com> I did find and download an executable Camouflage version 1.2.1. I installed this in my VMWare Windows partition. It installed the following files:

1. Camouflage.exe
2. CamShell.dll

3. Readme
4. Uninst.isu

Note the CamShell.dll file. Remember there was a deleted file entry by that name and the text “CamShell.dll” was extracted during a strings search of the image.

I looked through the Readme file and experimented with the tool a bit so I would feel comfortable with how it works. I remounted the floppy image locally and copied the doc files to the shared workspace.

Uncovering of Hidden Data

I tried opening Internal_Lab_Security_Policy.doc using the Camouflage tool. Once the tool is installed, a right mouse click on the file listing displays the Uncamouflage option. The software FAQ indicated there was no way to recover a forgotten password, but the file could be created without a password. For this file, I hit return at the Password prompt (the equivalent of no password) and a listing of multiple files contained in this one file was displayed. Notice in **Figure 8** the camouflaged file contained two files called Opportunity.txt and Internal_Lab_Security_Policy.doc.

© SANS Institute 2005, Author retains full rights.

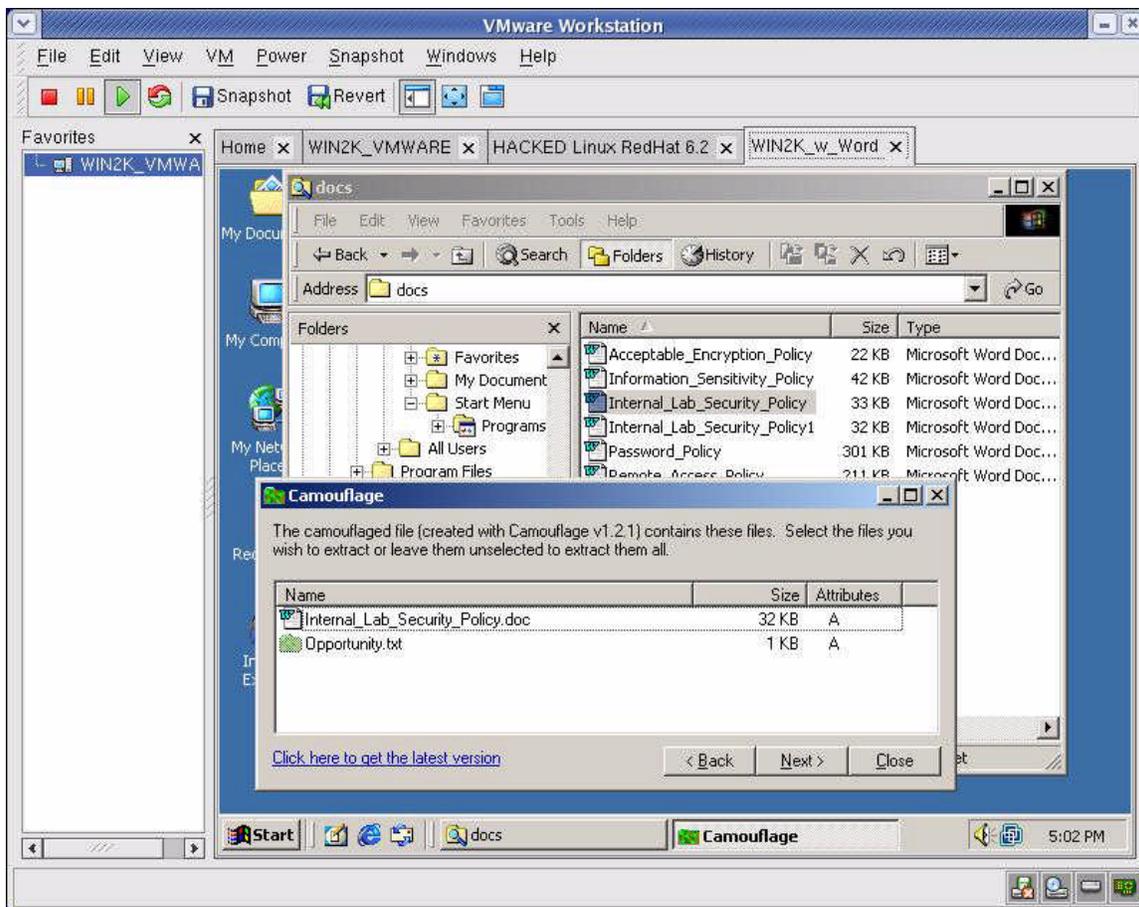


Figure 8 - Successful Un-Camouflage

I clicked Next and saved the file Opportunity.txt. When displayed it read:

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

A copy of this file is included as [Exhibit E – Recovered Letter of Intent to Commit Crime](#). I tried to do the same with the other two files with no luck. They were both either password protected or were not Camouflaged. I went back and added password, pass, pwd, and pw to my dirty words list and did another strings command in combination with a search. This resulted in a lot of output, but the only thing that looked promising was the string pwReserved. I tried using Reserved as the password on both files to no avail. I had a hardcopy of the only recovered file. I read it over and over. That last sentence “They are available as we discussed - "First Name”.” caught my attention. I read through my notes and the printed policy documents and made note of any person or company name. I tried Robert. I tried nicknames commonly associated with

Robert. I tried Rift, Ballard, and Bright. I tried different combinations of upper and lowercase since the password is case sensitive. I then thought to use the first word in the file's name and it worked. For Password_Policy.doc the password was Password and it contained:

```
Password_Policy.doc
PEM-fuel-cell-large.jpg
Hydrocarbon%20fuel%20cell%20page2.jpg
```

For Remote_Access_Policy.doc the password was Remote and it contained:

```
Remote_Access_Policy.doc
CAT.mdb
```

See [Exhibit F – Recovered Client Authorized Table Database](#) and [Exhibit G – Recovered Design Schematics](#).

I needed further evidence to validate the finding.

Steganography Tool Confirmation

I got a full listing of the Camouflage files I had installed in my VMWare partition, so I would know approximate size. Then, I used the md5 sum on the files.

```
# ls -l Cam*
-rw-r--r-- 1 root root 2718208 Jul 1 21:12 Camou121.exe
-rwxr--r-- 1 nobody nobody 217088 Mar 29 2001
Camouflage.exe
-rwxr--r-- 1 nobody nobody 36864 Feb 3 2001 CamShell.dll

# md5 Cam*
c62b050117c2cba3518e5a734fedef1f Camou121.exe (install file)
9f08258a80d578a0f1cc38fe4c2aebb5 Camouflage.exe (Camo binary)
4e986ab0909d2946bed868b5f896906f CamShell.dll (DLL file)
```

I concentrated on the dynamic link library (DLL) file since I had seen a reference to it in the image. Since it is 36864 bytes, it would occupy 72 sectors (36864/512). I know that the data sectors started at 33 (from the Image Details analysis) and the first .doc file started at sector 105. $105-33=72$ so that may be the location of the DLL file. I extracted this portion of the image using the dd command:

```
# dd if=v1_5 bs=512 skip=33 count=72 of=dd2.dll
72+0 records in
72+0 records out
```

The parameters are:

bs = blocksize (sector size)

skip = how many blocks to skip before beginning the extract

count = how many blocks to extract

if and of = input file and output file respectively

I then, using the md5 command, attempted to confirm the file extracted was exactly the same as the file installed when I loaded Camouflage:

```
# md5 dd2.dll
6462fb3acca0301e52fc4ffa4ea5eff8      dd2.dll
```

(And the downloaded and installed file again just for easy comparison.)

```
# md5 CamShell.dll
4e986ab0909d2946bed868b5f896906f      CamShell.dll
```

It wasn't a match. I remembered the HTML file was at sector 33. Looking back at the directory listing for the foremost recovered file it is 725 bytes. I pulled the dd2.dll file into a hex editor and removed everything above the 5th byte into row 02d0 (decimal 725 = hex 02d0). I did the same for CamShell.dll. I can see something isn't right though, the first two bytes of the files are not consistent. Looking back at the File Analysis screen, it lists _ndex.htm as being 727 bytes, not 725. I remove 2 more bytes from the beginning of both files and try again.

```
# md5 dd2-2.dll
ab16749d6fb4cc35b004319e7f4abb50      dd2-2.dll
```

```
#md5 CamShell-2.dll
ab16749d6fb4cc35b004319e7f4abb50      CamShell-2.dll
```

It is a match. The HTML file had been written on top of the DLL file on the floppy. I was a bit uncomfortable not having an exact match before trimming the files so I wanted another form of verification.

© SANS Institute Author retains full rights.

I did an md5 sum of all the files extracted with the Camouflage tool.

```
# md5 *
c3a869ff6b71c7be3eb06b6635c864b1 CAT.mdb
9da5d4c42fdf7a979ef5f09d33c0a444 Hydrocarbon%20fuel%20cell%20page2.jpg
e0c43ef38884662f5f27d93098e1c607 Internal_Lab_Security_Policy.doc
3ebd8382a19c88c1d276645035e97ce9 Opportunity.txt
e5066b0fb7b91add563a400f042766e4 Password_Policy.doc
864e397c2f38ccfb778f348817f98b91 pem_fuelcell.gif
5e39dcc44acccdca7bba0c15c6901c43 PEM-fuel-cell-large.jpg
2afb005271a93d44b6a8489dc4635c1c Remote_Access_Policy.doc
```

Now displaying the md5 sums from the policy files as they appeared when the image was mounted on the local loop device:

```
# md5 ./view/*
f785ba1d99888e68f45dabeddb0b4541 ./view/Acceptable_Encryption_Policy.doc
99c5dec518b142bd945e8d7d2fad2004 ./view/Information_Sensitivity_Policy.doc
e0c43ef38884662f5f27d93098e1c607 ./view/Internal_Lab_Security_Policy1.doc
b9387272b11aea86b60a487fbdc1b336 ./view/Internal_Lab_Security_Policy.doc
ac34c6177ebdcaf4adc41f0e181be1bc ./view/Password_Policy.doc
5b38dlac1f94285db2d2246d28fd07e8 ./view/Remote_Access_Policy.doc
```

I noticed the md5 sum for the unCamouflaged Internal_Lab_Security_Policy.doc is exactly the same as the md5 sum for the Internal_Lab_Security_Policy1.doc file when the image was mounted locally. I surmised the Internal_Lab_Security_Policy.doc is a Camouflage file containing the original Internal_Lab_Security_Policy1.doc and Opportunity.txt.

After multiple attempts to recreate Camouflaged files with the same md5 sums as those found on the local loop device, I concluded that the Camouflage tool uses volatile seed information when calculating the hash value. Therefore, it is not possible to recreate a Camouflaged file with the same md5 sum even if using the same hidden file and the same “wrapper” file (which is the one that someone would see if they open the document using the software native to that file such as Microsoft Word).

Forensic Details

Steganography Tool Analysis

Next, I wanted to understand how the system was affected by use of the Camouflage tool. I decided the best approach would be to use an audit type tool that uses a baseline to allow you to track changes. Winalysis is such a tool and can monitor registry, files, users, groups, services, security policies, the event log and more. At the time of this writing, a licensed version is available for \$55 USD. A full-featured free 14 day trial is also available. I downloaded the

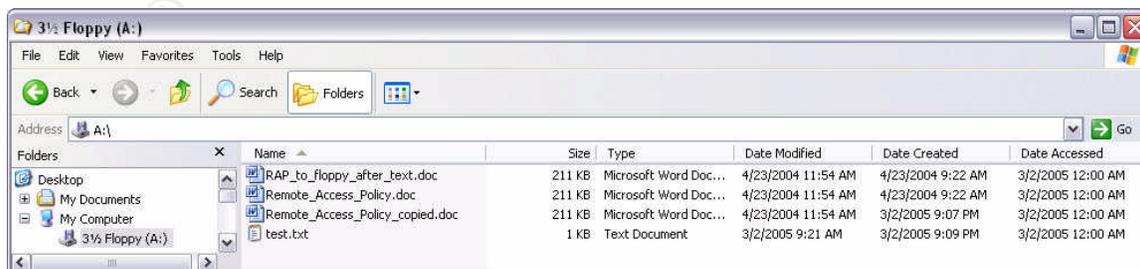
trial Winalysis version 3.0 from <http://www.winalysis.com/>. I enabled the private network on my forensics workstation just long enough to use sftp to copy the install file from my download environment to my test environment.

After default installation of Winalysis, I took a look through the Readme file. The installation notes indicated Winalysis will not modify any files outside of the user specified install folder. Note I am not going to include analysis of system changes from the installation of the tool as that is covered fairly well in the SANS Steganography document previously mentioned. This test focuses on changes identified when the tool is used.

I launched the Winalysis interface using the Windows Start menu. I clicked on the Snapshot button to create an initial baseline. I pressed Filters and specified C: and added A: including subdirectories. I also select entire registry. Once that is accepted I press the Start button on the Create Snapshot page. The default is to create the snapshot including all components. Once the snapshot is created, press Finish to return to the main window.

I chose to re-Camouflage the extracted Remote_Access_Policy.doc and CAT.mdb files onto a formatted floppy. I found that at least one file had to exist on the floppy before I could create the camouflaged file directly into A:. I Camouflaged the files on the local disk and did a copy to the floppy first. Then I did a Camouflage directly to the floppy. I copied a text file to the floppy. Finally, I did one more Camouflage to the floppy. I had taken a snapshot using Winalysis before the test floppy was created and after. I then tested for differences using the two saved snapshots and extracted the following. See [Appendix A – Camouflage System Modifications](#) for a complete listing.

It is noted there are files and registry keys modified on the system where the Camouflage is actually performed, but there is no trace of the DLL file nor registry key information on the floppy. Looking at a file listing of the newly created floppy disk, I see the created and modified dates for the files that were Camouflaged straight to the floppy, were from April and the access date was the current date. Yet, the files that were copied from the local disk to the floppy had create and accessed dates of the current date, while only the modified date had an April date.



Name	Size	Type	Date Modified	Date Created	Date Accessed
RAP_to_floppy_after_text.doc	211 KB	Microsoft Word Doc...	4/23/2004 11:54 AM	4/23/2004 9:22 AM	3/2/2005 12:00 AM
Remote_Access_Policy.doc	211 KB	Microsoft Word Doc...	4/23/2004 11:54 AM	4/23/2004 9:22 AM	3/2/2005 12:00 AM
Remote_Access_Policy_copied.doc	211 KB	Microsoft Word Doc...	4/23/2004 11:54 AM	3/2/2005 9:07 PM	3/2/2005 12:00 AM
test.txt	1 KB	Text Document	3/2/2005 9:21 AM	3/2/2005 9:09 PM	3/2/2005 12:00 AM

Figure 9 - ReCamo Test File Listing

Action Duplication

To see what activity was “taking place behind the scenes” I decided to try to duplicate the perpetrator’s actions. I first formatted a floppy disk so that any previous data was overwritten (not just marked available). At the Windows command prompt I typed:

```
C:> format/u a:
Insert new disk for drive A:
and press ENTER when ready...
The type of the file system is FAT.
Verifying 1.44M
Initializing the File Allocation Table (FAT)...
Volume label (11 characters, ENTER for none)?
Format complete.
  1,457,664 bytes total disk space.
  1,457,664 bytes available on disk.

      512 bytes in each allocation unit.
  2,847 allocation units available on disk.

      12 bits in each FAT entry.

Volume Serial Number is 3447-B161
Format another (Y/N)? n
```

As I was unsure whether the camouflaged files had been created directly on the floppy or on a local hard drive and subsequently copied, I chose to do both. (I also copied a test text file before any camouflage activity.) I made a bit-for-bit image copy of the newly created floppy disk to associate with the case using the dd command. Follows is fsstat output for this image called floppy5.img.

```
FILE SYSTEM INFORMATION
-----
File System Type: FAT
OEM: MSDOS5.0
Volume ID: 413832098
Volume Label: NO NAME
File System Type (super block): FAT12

META-DATA INFORMATION
-----
Range: 2 - 45538
Root Directory: 2

CONTENT-DATA INFORMATION
-----
Sector Size: 512
Cluster Size: 512
Sector of First Cluster: 33
```

Total Sector Range: 0 - 2878
 FAT 0 Range: 1 - 9
 FAT 1 Range: 10 - 18
 Data Area Sector Range: 19 - 2878

FAT CONTENTS (in sectors)

 33-454 (422) -> EOF x 512 = 216064
 455-876 (422) -> EOF x 512 = 216064
 877-877 (1) -> EOF x 512 = 512
 878-1299 (422) -> EOF x 422 = 216064

I multiplied the total block by 512 as I had done previously. I then associated the sectors to the filename.

Dir Ent #	Starting Sector	Filename	Size
6	33	Remote_Access_Policy_copied.doc	215895
12	455	Remote_Access_Policy.doc	215895
13	877	test.txt	14
21	878	RAP_to_floppy_after_text.doc	215895

I then imported the image into Autopsy and noted interesting residual files only when I Camouflaged directly to the floppy. Note the two deleted 0 length files in [Figure 10](#).

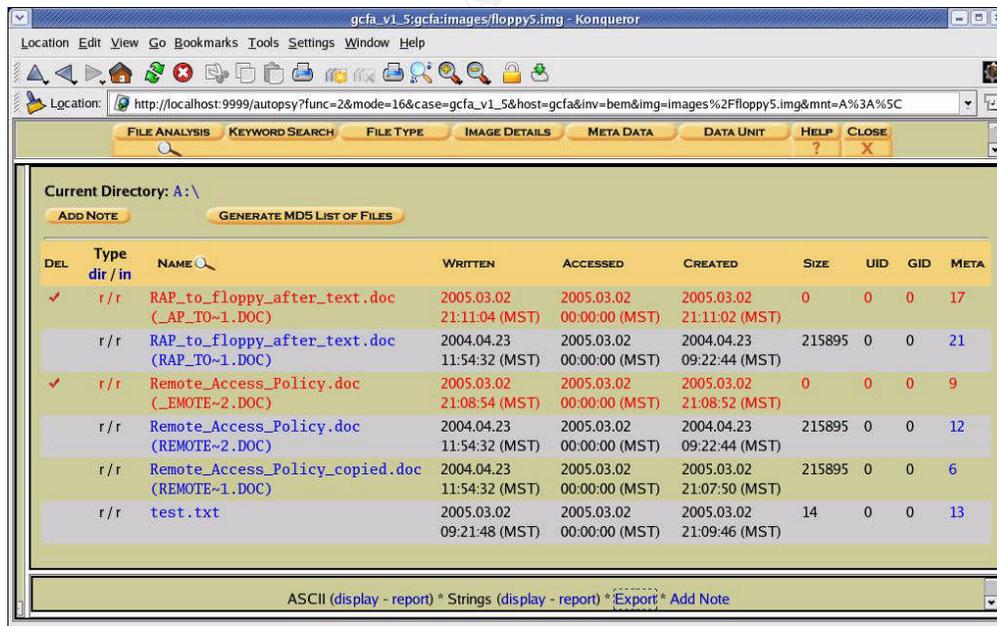


Figure 10 - Test Camouflage File Analysis

Recalling the File Analysis for the Ballard floppy, [Figure 5](#), I did not see any evidence of that kind of activity, so it was concluded that the files were Camouflaged on a different system and subsequently copied to the floppy. I

then created a timeline of this image to identify mac patterns based on how the Camouflage files end up on the floppy. See [Exhibit C – MAC TimeLine – Test Floppy Image](#). The sequence of mac was found on the Camouflaged file that had been copied to the floppy.

Sequence of Events

Next I summarized all the dates and files from the Ballard image to identify sequence of events. I have created a matrix of pertinent file information in a format that makes it easier for me to piece together. See [Appendix B – Summary of File Info to Aid in Determining Sequence of Events](#). I still couldn't quite follow the trail so I began to utilize the Camouflage tool in an effort to understand the MAC time changes that occur. I re-camouflaged CAT.MDB to masquerade a copy of Remote_Access_Policy.doc, used the same password and saved the file to a local disk, which is an NTFS partition. I compared the dates before and after.

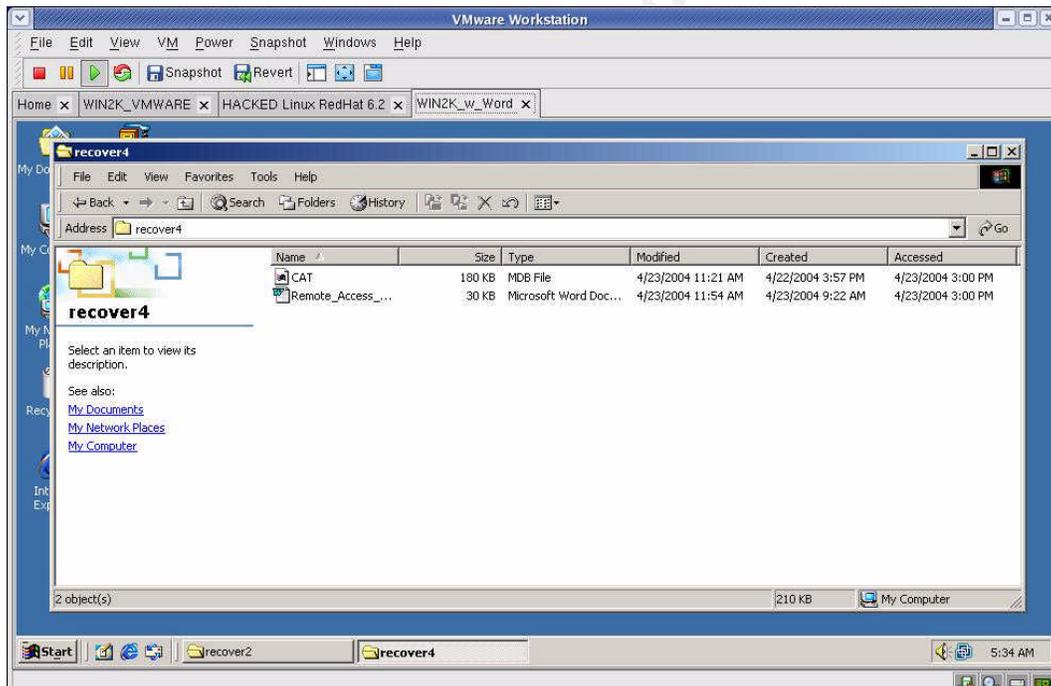


Figure 11 - Files Before Camo, NTFS

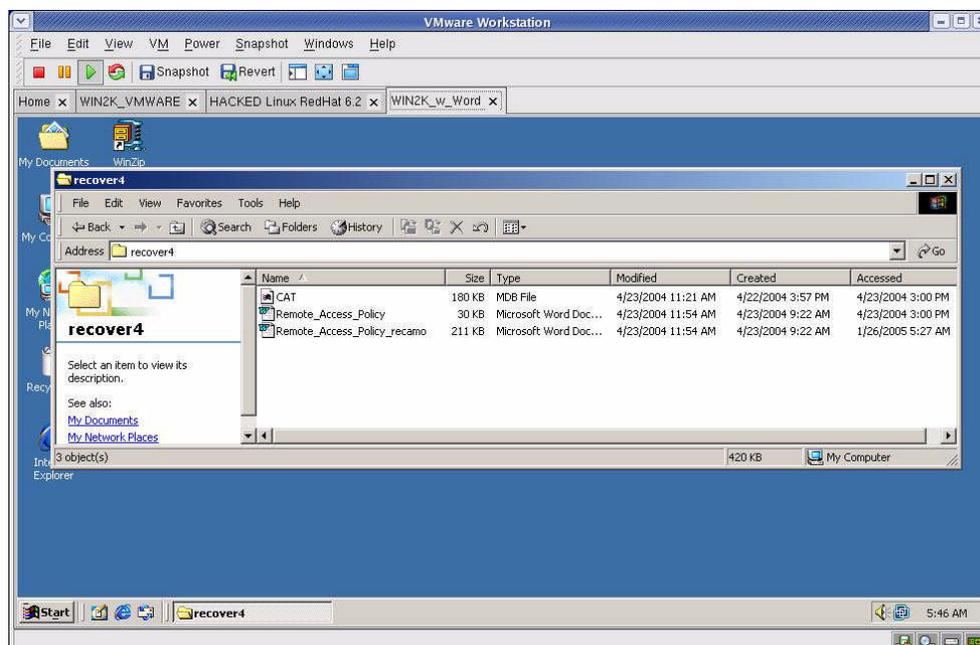


Figure 12 - Files After Camo

It appears that MAC times on the files that are included into the camouflaged file stay the same. The camouflaged file takes on the modified and created date of the “wrapper” file. The accessed date on the camouflaged file is the date and time the camouflage action took place. I look at my matrix of file information and I don’t see that type of trail.

I began to wonder if the dates do not seem to follow the sequence I just witnessed because it is a FAT12 filesystem. According to the help screens for File Analysis within the Autopsy tool, in the FAT12 filesystem specification the following guidelines apply:

- The modified or written date is the only required time field.
- The accessed timestamp is optional and is only accurate to the day. No hours or seconds.
- The created time is optional.

I copy the two files to a floppy and notice changes that may explain what I saw in the Ballard timeline. Here it appears that on the files included in the camouflaged file the modified time remains the same. The created time changes to the time of the copy to disk. The access date changes to the current date at midnight (remember this is the one that is only accurate to the day). The camouflaged file itself again retains the modified and created date of the wrapper file, but you have to keep in mind that the created date had changed on the wrapper. The accessed time is the current date at midnight.

Reviewing the matrix again, I first acknowledge that there is a three hour time skew because of the time zone selected when I created the timeline. Looking back at the timeline now it makes more sense, I believe the .doc files were placed on the floppy in the order shown at the bottom, looking only at the created entries (minus 3 hours). I believe all the .doc files were created using the Camouflage tool on a different machine at the times listed in that group at the top of modified times (again minus 3 hours). I believe it was on a different machine because there is no reference anywhere in the image of the files that are hidden in the camouflaged file and all listing for the three “tainted” files are the same size. If one of those was the pre-camouflaged version, it would be a different size. The accessed times really don’t give us any additional information since the date and time fields are not accurate.

I copied the CamShell.dll file from the local system onto the floppy and witnessed the modified time remained the same, which was the date it was actually originally created (wherever that was). The installation procedure maintains that original date. The created time went from the time I installed the tool on my machine to the time of the copy. The accessed time ends up today at midnight. I’m sure the _ndex.dat file would be similar. I would have to do further research to understand exactly how the HTML file ended up over the top of the CamShell.dll

Regardless, I am confident the data was hidden with the Camouflage tool. The files were loaded onto the floppy disk during the morning of the same day the disk was confiscated from Leszczynski.

Tool Removal Analysis

The SANS Steganography paper mentions there are registry keys that maintain a list of files that have been Camouflaged. The paper says after uninstall these keys are not removed. While my experience varied slightly from the author’s, the notion of residual registry keys is still valid and details are included in the [Follow Up](#) section of this document. See [Appendix C – Registry Entries After Tool Removal](#) for a complete listing of registry entries still existing after removal. This information is most relevant to someone that has access to the systems on which the files were originally Camouflaged. I also did not find the start menu option dangling after uninstall as was suggested in the paper.

Legal Implications

It is obvious to me Leszczynski had intended to sell company secret information to someone and it was not the first time. To start with, he named the communication file “Opportunity.txt” which seems incriminating in and of itself. He sets his price at \$5 million. He specifically states he is willing to provide MORE information, indicating he had done so in the past.

If the case were pursued in Texas, there are both federal and local statutes that may apply to this crime.

- Federal 18 U.S.C. 1832, Theft of Trade Secrets
- Section 31.05 of the Texas Penal Code, Theft of Trade Secrets

See [Appendix D – Relevant Statutes](#) for copies.

One of the ambiguities when dealing with trade secrets is the definition of a trade secret. Lawyer Mark Grossman states, “There’s no single precise legal definition of a trade secret. Each state has its own take on this area of law.”⁷

The following citation from a Texas law firm website provides some precedence in determining if this crime fits under theft of trade secrets in this jurisdiction.

In Schalk 823 S.W.2d 633 Court Crim. App. 1991, two defendants, former employees of Texas Instruments (TI), terminated their employment at TI and began working for a competitor in the same technical area. Soon afterwards, another former employee of TI working for this same competitor noticed what he believed to be proprietary information of TI stored in the memory of the computers of this competitor. This third party contacted TI with this information and agreed to collect information from the competitor's files. Meanwhile, an internal investigation at TI revealed that in the few hours before the two defendants left their employment at TI, they had downloaded and copied the entire content of their computer directories, including the programs which TI claimed to be trade secrets.

The two defendants were prosecuted under Section 31.05 of the Penal Code, theft of trade secrets, convicted and appealed. The convictions were upheld by the Texas Court of Criminal Appeals pointing out that the Texas Trade Secret Law had its origins in the civil law area, and the Restatement of Torts. In affirming the conviction, the Court relied heavily on the fact that the Defendants had signed non-disclosure agreements, that there was plant security, particularly in the area where these defendants worked, that the computer had software security, and that there were generally other security measures taken on these particular trade secrets. The Court of Criminal Appeals found that the computer software qualified as a trade secret under the penal code definition.⁸

Two crucial points to support company claims are that the company has taken steps to attempt security of the secret data and that the employee (or non-employee thief) has been notified that the information is not for public disclosure.

I did not want to assume the extracted policy documents were genuine, so I contacted Keen and had him compare the md5 sums of the copies I had against those of the published corporate documents. Once confirmed, I felt confident that I could use the documents I had to determine applicable violations. I also

⁷ <http://www.gigalaw.com/articles/2000-all/grossman-2000-05c-all.html>

⁸ <http://www.attorneyinparis.com/publwork.htm>

had him verify that Leszczynski had signed an acknowledgement letter indicating he had received and understood all related company policy documents.

In Opportunity.txt, Leszczynski indicates he has included schematics that are “not yet available” which lends credence to the fact it was indeed trade secret information. In section 3.3 of the company “Information Sensitivity Policy”, it states:

Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

... Once again, this type of Ballard Industries Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Ballard Industries employees and non-employees) designated with approved access and signed non-disclosure agreements.

...

Distribution outside of Ballard Industries internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within Bright Industries, but it is highly recommended that all information be strongly encrypted.

...

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

I had Clements (the Ballard Sales VP) verify that no one at Rift had a signed non-disclosure on file.

Leszczynski intended to distribute trade secrets and operational information that is integral to the success of the company against company policy. Electronic distribution was only allowed internally for this classification of data. The policy states that it doesn’t matter if the information is properly marked or not, it must be protected accordingly. It is spelled out that prosecution may be the penalty. Federal 18 U.S.C. 1832 more specifically lists the fines and jail time he could face. Section VIII. Theft of Commercial Trade Secrets, of the Department of Justice Computer Crime and Intellectual Property Section (CCIPS)⁹, discusses further implications if the transaction involves a foreign country. This document also sheds more light on prosecution requirements.

Follow Up Recommendations

To bolster the prosecution, it would be worthwhile to pursue some additional evidence on copies of the system(s) accessed by Leszczynski at Ballard.

- Look for evidence the Camouflage tool is installed.

⁹ <http://www.usdoj.gov/criminal/cybercrime/ipmanual/08ipma.htm>

- Right click on a file name displaying the Camouflage options.
 - Registry keys in HKEY_CURRENT_USER/Software/Camouflage.
- Look for evidence the Camouflage tool had been installed and is now deleted by looking for registry keys not removed during uninstall (as described in section [Tool Removal Analysis](#)).
- A systems administrator could inventory the value of registry keys of suspect systems at Ballard and show the filenames found on the floppy disk match those that have been Camouflaged and appear in the registry listing.

- Investigate both allocated and unallocated space in the image.
 - Make a list of clients that are no longer reordering from Ballard and use all of those names in a dirty word search looking for any evidence of communication between Leszczynski and a Rift employee.
 - Look for indications of email address syntax to potentially reveal the purchaser.

For any files found, ownership should be assessed. File ownership is the way computer systems keep track of whose files are whose. If tools, production data on a lab system or files with names that match the Camouflaged files are recovered and the local system shows the owner as an account Leszczynski had access to it would further reinforce the case against him.

Lastly, to increase the number of violations, it is possible that the Internal Lab Security Policy may also have been abused. It states that production data is not to be used in the lab. Somehow Keen had access to the real customer database. Section 33.02, Breach of Computer Security, of Texas Penal Code Chapter 33, Computer Crimes, may be applicable. Discovery of this data on one of the lab systems (intact or deleted) may prove beneficial to prosecuting this offense.

Part 2 – Attacked? - Tools of the Trade

Scope

Headline: “Lawsuit could amplify data protection laws¹⁰”

A Miami man blames Bank of America for more than \$90,000 stolen in an unauthorized wire transfer to Latvia. Joe Lopez filed a lawsuit on Feb. 7 claiming that Bank of America had not alerted him to malicious code that could -- and indeed had -- infected his computer. A forensic investigation by the U.S. Secret Service revealed that a Trojan called Coreflood, which acts as a keystroke logger, had compromised one of his PCs.

Some discussion of this pending lawsuit¹¹ includes the following thought:

When a customer has a direct loss because his information was used for fraud, is the customer responsible for the theft, or is the bank responsible for accepting fraudulent ID, in the same way they would for cashing a check with a fake driver's license?

No doubt this case will be precedent setting. Phishing scams, trojans downloaded when visiting a website, malware delivered via email, peer to peer programs and software downloads that harbor unwanted “extras”... The creativity of the bad guys continues while the dependence on the internet grows. These factors will lead to increase and severity of desktop and server compromise.

Desktop pest management tools on the market these days are becoming more popular and more sophisticated. While these tools and anti-virus tools are distinct, more of the anti-virus vendors are incorporating pest management into their tools or tool suites. Unfortunately, not all users take advantage of either of these preventive eradicators. When investigating potential compromise of a desktop system, I believe these pest management tools could be used to expedite the process of identifying whether or not there has been an incident, provide clues about where to dig deeper, and give an indication of an attacker's motive. Using a pest management tool for identifying compromise is even more attractive when the evaluation is done on a bit-for-bit image copy of the system in an environment where one can easily revert to a known state (such as VMWare).

The potential advantage of using these pest management tools is not just when investigating a victim machine. Another prospective use of the tool is to identify incriminating software on a suspected criminal's system.

For forensic purpose we are only interested in the scan and reporting function of

¹⁰ http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_qci1062438,00.html

¹¹ http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_qci1062440,00.html

this type of tool. Taking any corrective action to rid the system of pests would introduce extensive modification and possibly obfuscate key evidence.

Pest management tools are like virus scanners, you have to keep the scanning reference data current. With this in mind, this method of compromise identification will not be useful in detecting unknown malware whether it be undiscovered or if malware signature files are allowed to become outdated.

Lastly, these tools generally only run in a Microsoft Windows environment.

Tool Description

Pest management tools attempt to detect and remove software and configuration mechanisms that were put there very likely without the system owner's knowledge and that use the system for purposes other than those intended. The following five classes of offending pests¹² are included when referring to pest control:

1. Adware – “Advertising R Us” - In addition to showing you lots of ads you didn't want to see, this class is likely tracking your browsing habits and reporting it somewhere.
2. Browser Helper Object – “Browser Spy” - Integrates itself into a web browser. May replace page banners with other ads, monitor and report user actions, change your homepage, etc.
3. Hijacker – “Control Freak” – May reset browser homepage or search settings to point to different sites (like porn). They may prevent you from changing your browser's homepage or from visiting a particular site.
4. Spyware – “Free Loader” – Uses your internet connection without your knowledge. Will likely gather up information about your system and pass it along. Often times they are introduced on your system when you load some commercial product.
5. Trojan – “Unwanted Guest” – Software that runs on your machine, for some attacker's benefit, that you don't know about. Keystroke loggers, that record everything you type – such as bank account numbers and passwords, fit into this category.

Forensic Benefit

Based on the descriptions above, the most useful to a forensics investigator would be identification of a trojan. A trojan could very well indicate compromise of a system and imply an attacker may have gained control of the system. Likely, the next most useful would be finding spyware. That means that someone somewhere is interested in the victim's system and activities. If they

¹² Paraphrased from http://research.pestpatrol.com/Whitepapers/About_Spyware.asp.

see something they want, they may show up later to take it! Finding hijackers, browser helpers or adware likely indicates a website has been visited where someone is using every trick at their disposal to gather or disseminate information so the victim system owner will want to use their “product” or to force him/her to use their “product” regardless.

Some reasons a system is attacked include:

- To use it as an IRC server.
- To use it as a place to store “warez” or illicit material.
- To gather personal information from the victim with the intent of committing fraud or theft.
- To use it as a zombie in a distributed denial of service attack.
- To use it as a way to cover the attacker’s tracks by making it a hard trail to follow.
- To use it to download malware to other systems.

A way to easily detect signs indicating these activities may be taking place on a system could save a lot of time and reveal compromise that may have been overlooked if a manual forensics approach was used.

Pest management tools also identify many of the tools used by miscreants to commit a crime, not just the software that is the result of an attack. This software may reside on the compromised system or the attackers own system. Some other software categories that pest management tools may identify and that may provide clues to the forensics investigator are¹³:

- AV Killer – Attempts to disable anti-virus tools to evade detection.
- Binder – Combines files in an attempt to hide one of them.
- Cracking Tool – Software used to remove access restrictions from other software.
- Downloader – Automatically downloads and installs software.
- Firewall Killer – Attempts to disable firewall software to gain entry.
- IRC War – Any tool that uses Internet Relay Chat for malicious activity.
- Key Generator – Tool to break copy protection by extracting internal keys.
- Notifier – A tool designed to stealthily notify an attacker when an event occurs.
- Peer to Peer – Tool to swap files between machines.
- Packer – Utility to compress and encrypt, used to bundle trojans to avoid detection.
- Password Cracker – Tool used to decrypt passwords.
- PhreakingTool – An executable that assists in hacking a phone system.
- Port Scanner – Used to gather information about target machines such as programs waiting for a connection.

¹³ Definitions from the PestPatrol glossary at <http://www3.ca.com/securityadvisor/glossary.aspx>.

- ProbeTool – Tool to find vulnerabilities on another machine.
- Sniffer – Network eavesdropper that captures and replays packets.
- Spoofer – Used to forge identity.
- Trojan Creation Tool – Used to create those dreadful trojans.
- War Dialer – Program used to dial many numbers in a range looking for a modem that will answer.

Finding any of these types of malware on a system may indicate law has been or will be violated.

Pest management tools will detect a number of virus related entities that are not included here as we are distinguishing between viruses and pests.

Selected Tool

I chose to test the PestPatrol product, now from Computer Associates¹⁴, because they have a fairly extensive pest encyclopedia, with thousands of entries, freely available on the internet or from the scan report by just clicking on an identified pest. I have used this database many times¹⁵. It provides general information about pests and includes manual removal instructions even if the tool is able to effectively remove the pest. Many other tools are available such as Ad-Aware from LavaSoft. If you are interested in tool comparison, Eric Howes did some testing and posted quite a bit of information at <http://spywarewarrior.com/asw-test-guide.htm#descript>. He also provides a list of rogue and suspect products. Unfortunately, there are those out there that have created tools that purport to be spyware removal when in fact the tool itself is malicious.

As of this date, a licensed version of PestPatrol is available for \$29.95 USD from <http://www.pestpatrol.com>. The demo version is free, but time limited. The only difference between the demo and licensed versions is the licensed version includes the ability to delete or quarantine pests. To make certain creating a cdrom using the demo version would be acceptable, I called PestPatrol licensing support at 1-800-656-5443 and the representative confirmed legitimacy. See [Appendix E – PestPatrol Evaluation License](#). While I have a licensed copy of the software, there is wording in the purchased license agreement that prevents me from pursuing use for this testing unless I had written acknowledged permission. At the time of this writing the author does not have such permission, therefore the demo version is utilized.

The demo software can be downloaded from http://www.pestpatrol.com/Products/PestPatrolHE/Single_User_Evaluation.asp.

¹⁴ <http://www.pestpatrol.com/acquisition.asp>

¹⁵ <http://research.pestpatrol.com/Search/Search.aspx>

One last bit of information about the distribution is to note if you purchase the cdrom, installation is required (the tool can not be run from the installation cdrom).

Malware Signatures

There are three methods used by the vendor to verify PestPatrol's ability to accurately identify and remove pests. These include file content, object location and live pest detection tests. File content tests use a checksum concept, kind of like the md5 validation used during forensics in the Ballard case. This allows them to verify the product can detect a pest regardless of location or filename. Object location tests are just what they sound like...if registry entries, files or processes exist in this specific location and/or with a certain name, it is a quick and easy method of identification. Live pest detection testing is when the vendor actually installs the pest in a controlled environment. This type of testing is critical for the vendor to ensure the tool can successfully and completely eradicate the pest.

Creating An Evidentiary Sound Tool

When performing forensics, you can never assume there hasn't been compromise of the utilities and commands on the machine being investigated. Likewise, it is a good idea to create a copy of necessary tools on read only media and statically compile if at all possible. When statically compiled, applications will not try to use the default system libraries (on the potentially compromised machine) when it comes time to execute, the necessary library information has been included in the program. Also, it is possible that when media is attached or inserted in the compromised environment it may be attacked. So, my first order of business was to find out if PestPatrol could be run from read only media. I downloaded demo version 4.4.3.24 with data files (PPfile.dat, PPInfo.dat and Spyware.dat) from 10/6/2004. I did a default install on a download machine. I verified PestPatrol was not running on my download machine and subsequently burned the program directories to a cdrom. See [Appendix F – Listing of Pest Detection Tools CD-ROM](#) for a listing of the contents. I loaded the cdrom into the forensics workstation cdrom drive, pulled up Windows Explorer in my VMWare virtual server, drilled down to D:\ Program Files\PestPatrol\PestPatrol, and clicked on the filename to run the app. PestPatrol is fairly configurable, but I opted for a default scan.

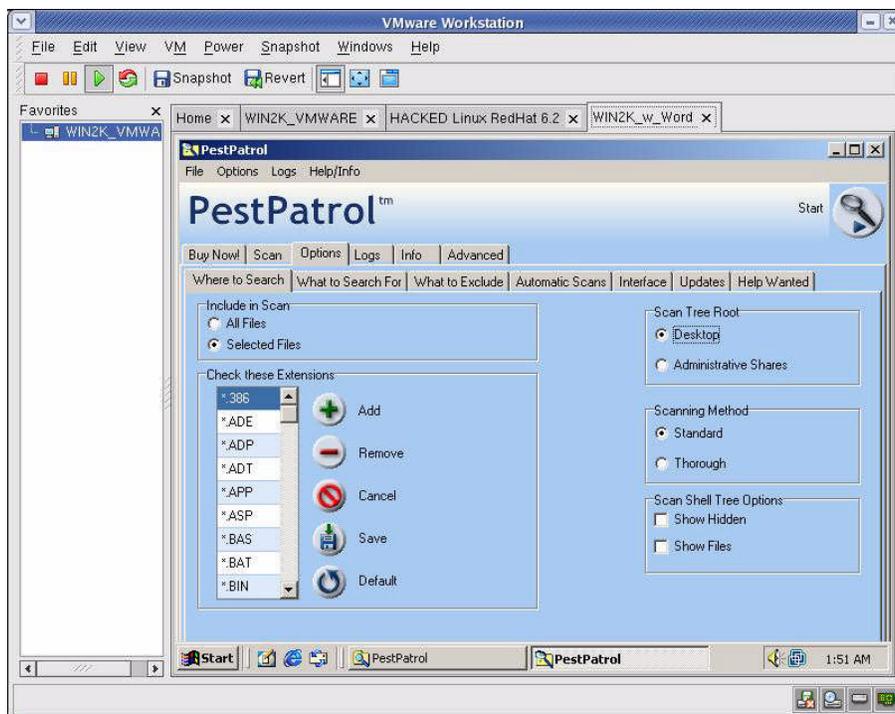


Figure 13 - PestPatrol Configuration Options

On the Scan tab you need to click on the name of the disk to scan and press the add button to move it into the Selected for Scanning box. I added C:, pressed the Start button and off it went. Once complete, the report can be saved to any location by selecting the Save Session Log option from the file menu. Of course, since the cdrom is read only we would have to have another removable device or save to our compromised system. There is also a print option. When exiting PestPatrol two errors were received:

PestPatrol is unable to save the Master Log.
Please ensure that you have full permissions for "D:\Program Files\PestPatrol"

and

PestPatrol is unable to save its configuration setting (.ini file)
Please ensure that you have full permissions for "D:\Program Files\PestPatrol"

I could not find a configuration file or parameter to control the location of the master log or the configuration file in the GUI version of the tool. The master log file is a .csv (comma separated values) file that contains information from all of the PestPatrol sessions, by all users, and reports information for all pests deleted or quarantined. If a pest has been ignored it will not be entered. Since during our use of the tool, pests will always be ignored, I concluded the tool could be successfully run from the created cdrom for this purpose. The Master Log and ini files were not necessary for proposed forensic use and the two errors could be safely ignored.

Test Apparatus

For my controlled test, I used the VMWare environment on my forensics workstation (described in the Ballard case). Additionally, I used a Leading River UD-11 256 MB thumb drive onto which I saved resultant log files.

The currently saved revert environment includes:

- Microsoft Windows 2000 unpatched
- Macromedia Shockwave Player
- Microsoft Word 97
- WinZip 8.0
- Camouflage 1.2.1
- Winalysis 3.0

Environmental Conditions

A controlled set of tests is done with network connectivity completely disabled except for short periods of time when malware installation files are copied from a download system on the local network. For these tests the image is intentionally compromised and the VMWare virtual system is reverted to a known state following each test. Default installations are accepted for all malicious code.

Another more real life, but limited test is run on an unknown system about which the owner had performance degradation complaints. Internet connectivity was disabled only during scanning. When the network is up and running on this system it sits behind a router/firewall that performs NAT and DHCP functions. An image copy is not made and full blown forensic analysis is not performed. The intent is only to show concept application in a more uncontrolled environment. It is understood, for this particular test, that system modifications incurred from executing the tool on a running system, as opposed to an image copy, are acceptable.

Procedure Description

Initial testing is done to determine impact on system of tool use. During the controlled testing, multiple snapshots of the environment are taken to capture state of the environment at different points during malware installation. This history is maintained as an aid in determining how the malware modifies the system in the event PestPatrol does not adequately identify the malicious code.

Follows are the steps taken in the controlled tests:

1. Obtain malware and make installation file(s) available in shared workspace on the forensics machine.
2. Revert the VMWare virtual environment to the known state.
3. Start Winalysis and select the snapshot option.
 - 3.1. Configure scan to include entire registry.
 - 3.2. Configure scan to include C: with all subdirectories.
 - 3.3. Remove System32 subdirectory since it is redundant now.
 - 3.4. Start the snapshot. Do not save previous snapshots.
4. Install the malware.
5. If a reboot is required.
 - 5.1. Create Winalysis snapshot before reboot. Do save previous snapshots.
 - 5.2. After reboot restart Winalysis.
6. Create a Winalysis snapshot. Do save previous snapshots.
7. Run PestPatrol and capture output.
 - 7.1. Insert cdrom (created previously).
 - 7.2. Use Windows Explorer and browse to the PestPatrol executable in the directory A:/Program Files/PestPatrol.
 - 7.3. Add disk C: to the selected drives.
 - 7.4. Upon completion, use the file menu to do a "Save As", select type text file. Do include all changes. Note you must have selected the system name at the top of the list to get all details included. I used a created subdirectory under C:/ in the virtual environment.
 - 7.5. Use the file menu to do a "Save Session", select type text file.
8. Determine if the malware was adequately detected.
 - 8.1. Compare Winalysis snapshots to understand the modifications made to the systems by installation.
 - 8.2. Review the PestPatrol report.
9. Review PestPatrol Advanced screen tabs "Startup Files" and "Running Processes" to see if any malware was started at boot time and any malware processes currently running respectively.
10. Consider potential implications of finding this malware.
11. Eject the cdrom.

In the uncontrolled test:

1. Disconnect the network connection.
2. Run PestPatrol and capture output to thumb drive.
 - 2.1. Insert cdrom (created previously).
 - 2.2. Use Windows Explorer and browse to the PestPatrol executable in the A:/Program Files/PestPatrol.
 - 2.3. Add disk C: to the selected drives.
 - 2.4. Use the file menu to do a "Save As", select type text file.
 - 2.5. Use the file menu to do a "Save Session", select type text file.
3. Evaluate PestPatrol findings to determine significance.
4. Review PestPatrol Advanced screen tabs "Startup Files" and "Running Processes" to see if any malware was started at boot time and any malware

- processes currently running respectively.
5. Consider potential implications of any significant malware found.

Approval Criteria

For each of the three controlled tests the installed malware will hopefully be adequately detected.

For the one uncontrolled test, information may be presented that would allow an investigator to determine whether or not malware found may indicate intrusion.

Data, Results and Analysis

Precursor Testing Of Tool Impact on System

I needed to understand how the system was affected by use of the PestPatrol tool. I used the Winalysis tool as described in the [Steganography Tool Analysis](#) section of the Ballard investigation in this document. As noted previously, it is expected that the Winalysis tool should not affect files outside of the Winalysis subdirectory.

Since I had been playing with the virtual system making sure PestPatrol would run, I hit the revert button in VMWare to take me back to a known state. I launched the Winalysis interface using the Windows Start menu. I clicked on the Snapshot button to create an initial baseline. I modified the filters to include all of the C:\ drive and the entire registry. Once that is accepted I press the Start button on the Create Snapshot page. At this point I do not save previous snapshots. The default is to create the snapshot including all components. Once the snapshot is created, press Finish to return to the main window.

© SANS Institute

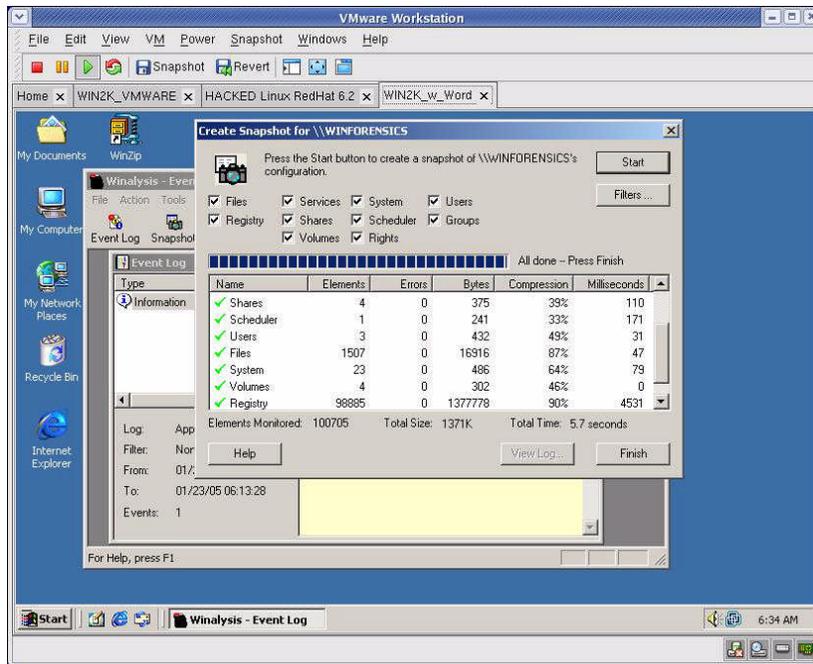


Figure 14 – Create Winalysis Snapshot

Since I now have a clean baseline, I launch PestPatrol from the cdrom, select the C: disk and Start the scan.

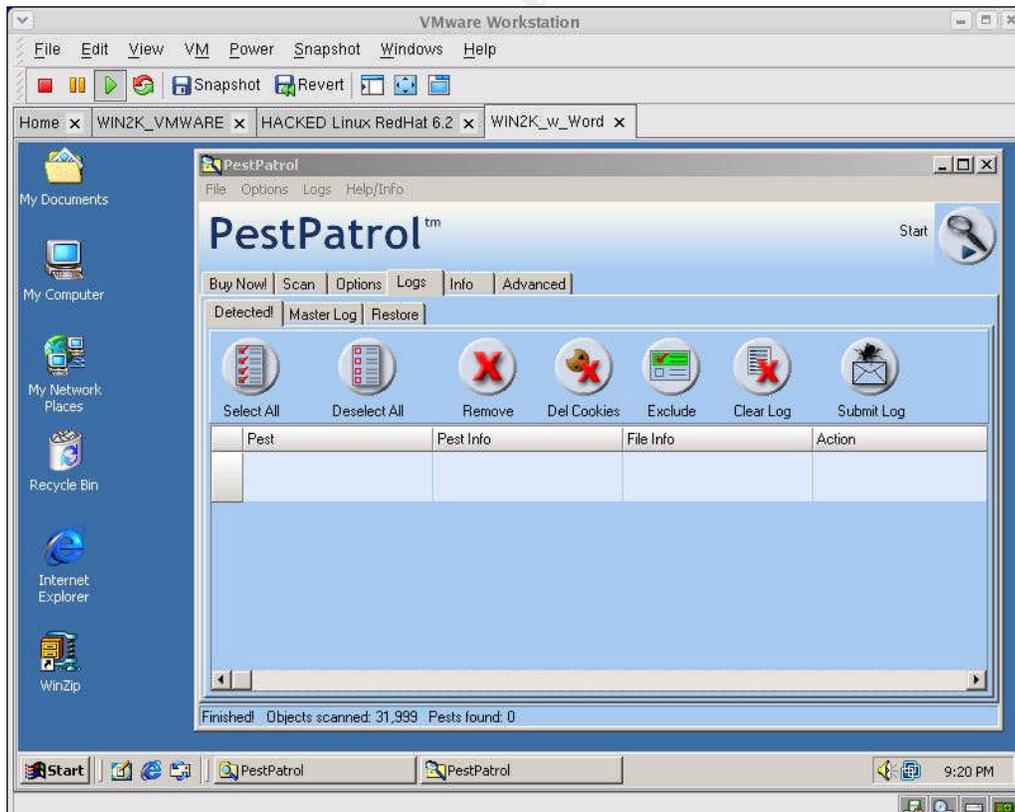


Figure 15 - PestPatrol Scan

I exit PestPatrol, again ignoring the two error messages and maximize my Winalysis window. I create another snapshot, I do save previous snapshots this time, and then use the test feature to identify changes between the first snapshot and this one (which should only include the running of the PestPatrol scan). With the Winalysis tool I can press the “Test” button at anytime to compare the current state of the system to the snapshot or even snapshot to snapshot.

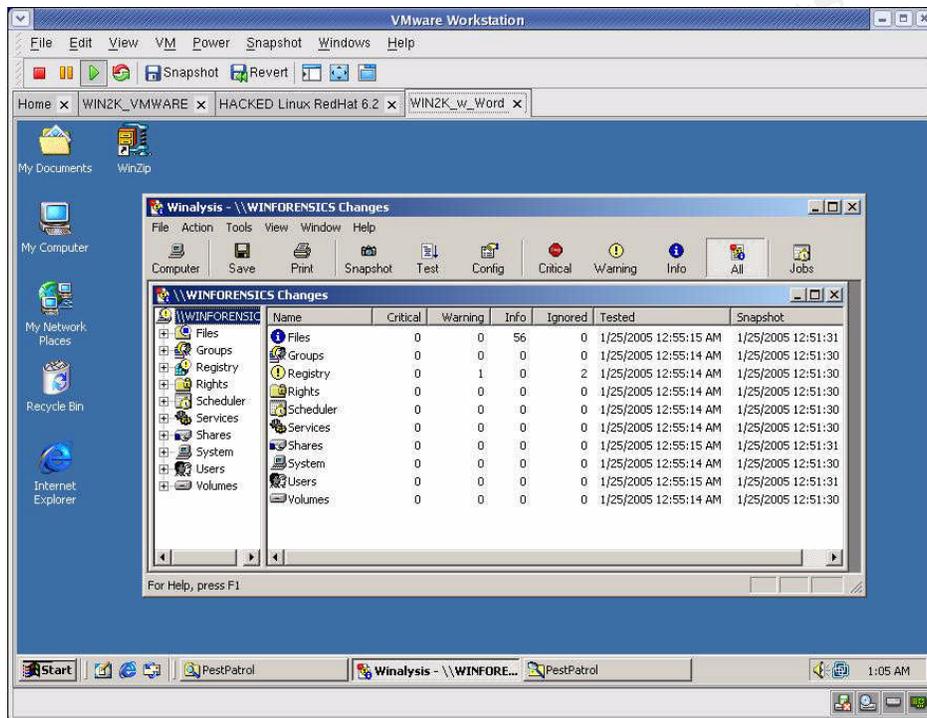


Figure 16 - PestPatrol Changes Via Winalysis

I can see from the summary screen that there are informational messages on the Files category and warnings under Registry. I know I can get back to a clean state so I select Save and put the report of all changes to a local file for review. See [Appendix G – PestPatrol System Modifications](#) for complete output. In that full report, the changes not in the Winalysis tree have been changed to a blue font for readability since I expected the Winalysis tree to change. That leaves the following changes that must be understood (again font change for clarity):

```

C:\WINNT\system32
    Folder Last Modified Date 1/25/2005 12:30:25 AM 1/25/2005 12:28:21 AM
C:\WINNT\system32\config\software
    File Last Modified Date 1/25/2005 12:31:12 AM 1/25/2005 12:17:04 AM
C:\WINNT\system32\config\software.LOG
    File Last Modified Date 1/25/2005 12:31:12 AM 1/25/2005 12:17:04 AM
C:\Documents and Settings\Administrator\NTUSER.DAT
    File Last Modified Date 1/25/2005 12:30:58 AM 1/25/2005 12:30:03 AM
C:\Documents and Settings\Administrator\ntuser.dat.LOG

```

```

File Last Modified Date      1/25/2005 12:30:58 AM 1/25/2005 12:30:03 AM
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
File Last Modified Date      1/25/2005 12:30:54 AM 1/25/2005 12:16:36 AM
C:\Documents and Settings\Administrator\Local
Settings\History\History.IE5\index.dat
File Last Modified Date      1/25/2005 12:30:54 AM 1/25/2005 12:16:36 AM
C:\Documents and Settings\Administrator\Cookies\index.dat
File Last Modified Date      1/25/2005 12:30:54 AM 1/25/2005 12:16:36 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Number of Values
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PPMemCheck
New Value
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PestPatrol Control
Center
New Value                      D:\PROGRA~8\PESTPA~5\ PControl.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CookiePatrol
New Value                      D:\PROGRA~8\PESTPA~5\ ookiePatrol.exe
HKLM\SOFTWARE\Microsoft\Cryptography\RNG
Key Last Modified Date
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
Value Changed
HKLM\SOFTWARE\Classes\.key
Key Last Modified Date

```

If PestPatrol was already up and running, there were no additional system modifications when a scan was run, however, the other 7 files listed above and the noted registry keys were changed when the PestPatrol program was first invoked.

Now that Winanalysis and PestPatrol modifications are understood, I can proceed with testing to verify the proposed forensic tool would serve the intended purpose which is to identify potential compromise.

Controlled Test 1 – Keystroke Logger

A keystroke logger is a program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack. For example, a key logger will reveal the contents of all e-mail composed by the user. Keylog programs are commonly included in rootkits and RATs (remote administration trojans).¹⁶

I downloaded a demo version (2.1) of a keystroke logger called Invisible Keylogger Stealth (IKS) from <http://www.invisiblekeylogger.com/>. I did a default install in the VMWare Windows partition.

¹⁶ <http://www3.ca.com/securityadvisor/pest/pest.aspx?id=2983>

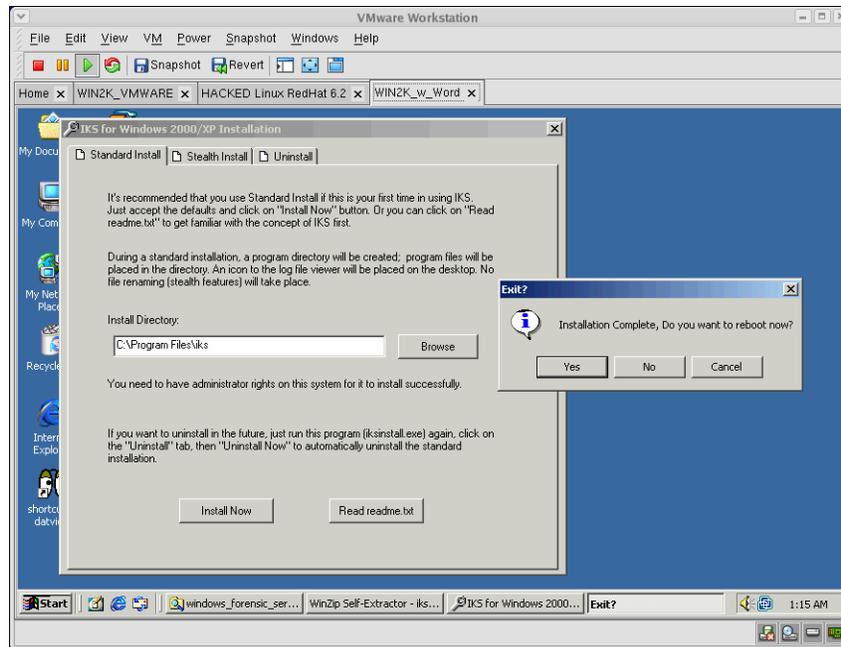


Figure 17 - Invisible Keylogger Install

You do need to reboot after installation of this software. So, in preparation, I shutdown PestPatrol and WinAlysis and clicked Yes. After the system came back up, I clicked on the IKS shortcut to datview icon on my desktop. All of a sudden I had an alert from PestPatrol.

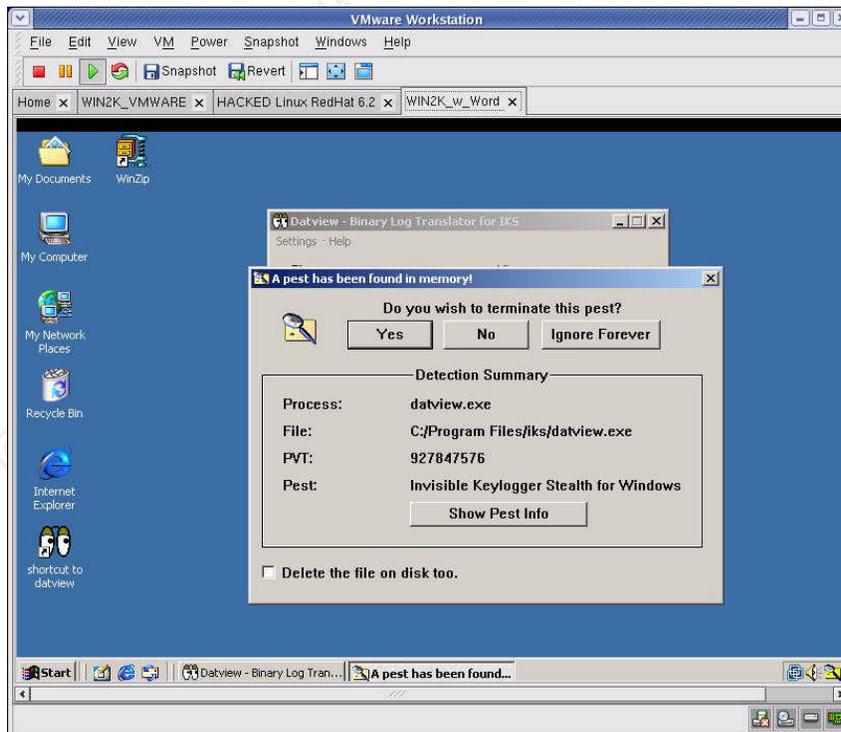


Figure 18 - Pest Found in Memory

As PestPatrol was not installed on this virtual machine and was not supposed to be running at this point, I investigated further. I pulled up Windows TaskManager, which shows you all the currently running processes and there I saw PPMemCheck.exe, PPControl.exe, and CookiePatrol.exe.

Tests showed that once PestPatrol is invoked in an environment for the first time, even from the cdrom, if the disk is inserted upon reboot, the PestPatrol executables will start up. Looking back at the modifications made by the initial invocation of PestPatrol this is explained by examining the registry modifications. To avoid duplication of this scenario, it is recommended that the cdrom be ejected whenever a reboot is to be performed.

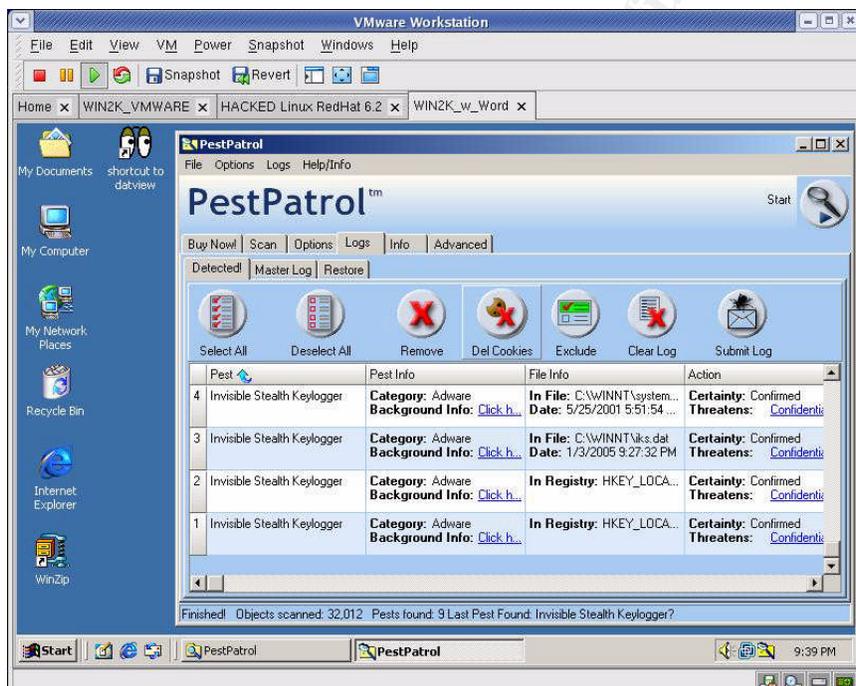


Figure 19 - PestPatrol After Keylogger Install

Scanning using the default configuration of PestPatrol found the Invisible Stealth Keylogger installation. See [Appendix H – PestPatrol IKS Output Log](#) for a complete listing of the PestPatrol output.

I had read the readme file that was installed and it indicated there are three primary files:

- iks.sys – is the main program file, the driver that records the keystrokes
- iks.dat – is the binary data log where the recorded information is stored
- Dataview.exe – viewer for the binary log data

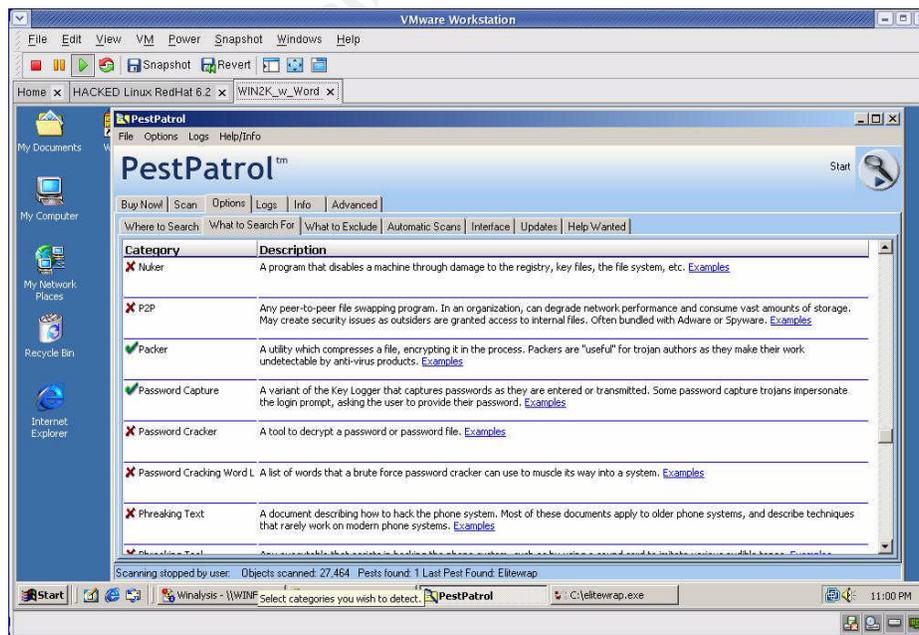
Reviewing the PestPatrol output, it definitely found those files. Finding a specific keylogger on the machine of someone that has been a victim of identity theft is a good indication that further investigation is warranted. The direction of the investigation could then turn to trying to identify how the keylogger was installed on the system. Which could provide clues that may eventually lead to when it was placed and by whom.

Controlled Test 2 - Packer

A packer is a utility which compresses a file, encrypting it in the process. It adds a header that automatically expands the file in memory, when it is executed, and then transfers control to that file. Some packers can unpack without starting the packed file. Packers are “useful” for trojan authors as they make their work undetectable by anti-virus products. Elitewrap is an EXE wrapper, used to pack files into an archive executable that can extract and execute them in specified ways when the packfile is run. Features: Programs in the packfile can be extracted without starting.¹⁷

Elitewrap was downloaded from <http://homepage.ntlworld.com/chawmp/elitewrap/elitewrap.zip>. The installation is accomplished by simply copying 3 files to the desired directory.

Initially, Elitewrap was not detected by the PestPatrol scan. A packer is not included in the default PestPatrol options. For EliteWrap to be successfully identified I had to select packer from the “Options - What to Search For” page.



¹⁷ <http://www3.ca.com/securityadvisor/pest/pest.aspx?id=1857>

Figure 20 - Pest Patrol "What to Search For Option"

Finding a packer on a suspected criminal's system would suggest further investigation looking for other detected malware on the machine is warranted. If none were revealed by the PestPatrol scan, it would still be worthwhile to perform a manual search for both pest classes of software and any virus code as either may be packaged up by this type of software tool.

Controlled Test 3 - Backdoor

A backdoor is a secret or undocumented means of getting into a computer system, or software that uses such a means to penetrate a system. Some software has a backdoor placed by the programmer to allow them to gain access to troubleshoot or change the program. Software that is classified as a "backdoor" is designed to exploit a vulnerability in a system, and open it to future access by an attacker.¹⁸

Back Orifice is such a tool and a copy was downloaded from <http://www.cultdeadcow.com/tools/bo.html>. On that webpage you will find, "Once running, BO does not show up in the task list or close-program list, and is rerun every time the computer is started." The Back Orifice installation uses the Windows installer.

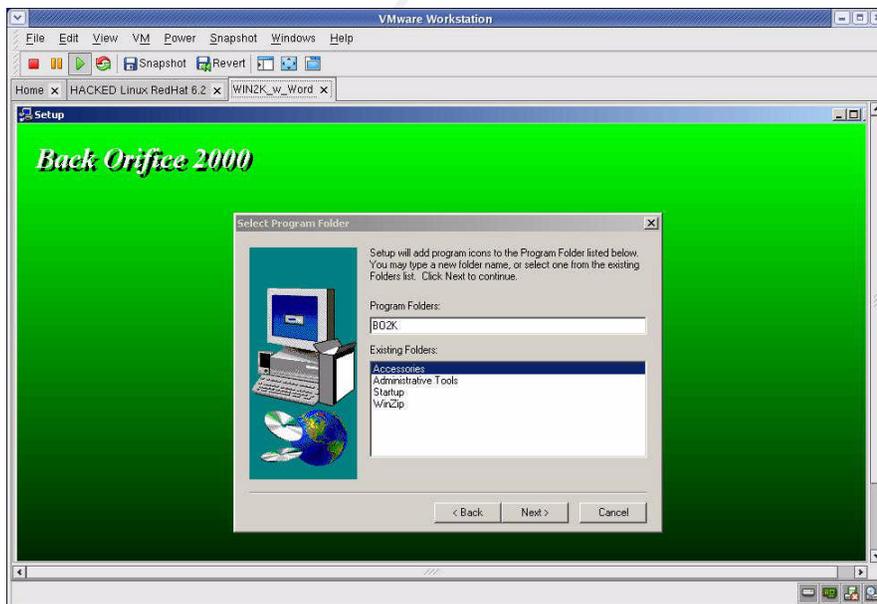


Figure 21 - Back Orifice Installation

Back Orifice was detected as long as the Commercial RAT category was

¹⁸ <http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453089849>

selected on the “What to Search For” page. Also note, viewing the “Running Processes” screen did identify any component of the tool if it was running. Note the md5 information included. This would prevent allowing the stealth naming capabilities of the malware to hide from the scan.

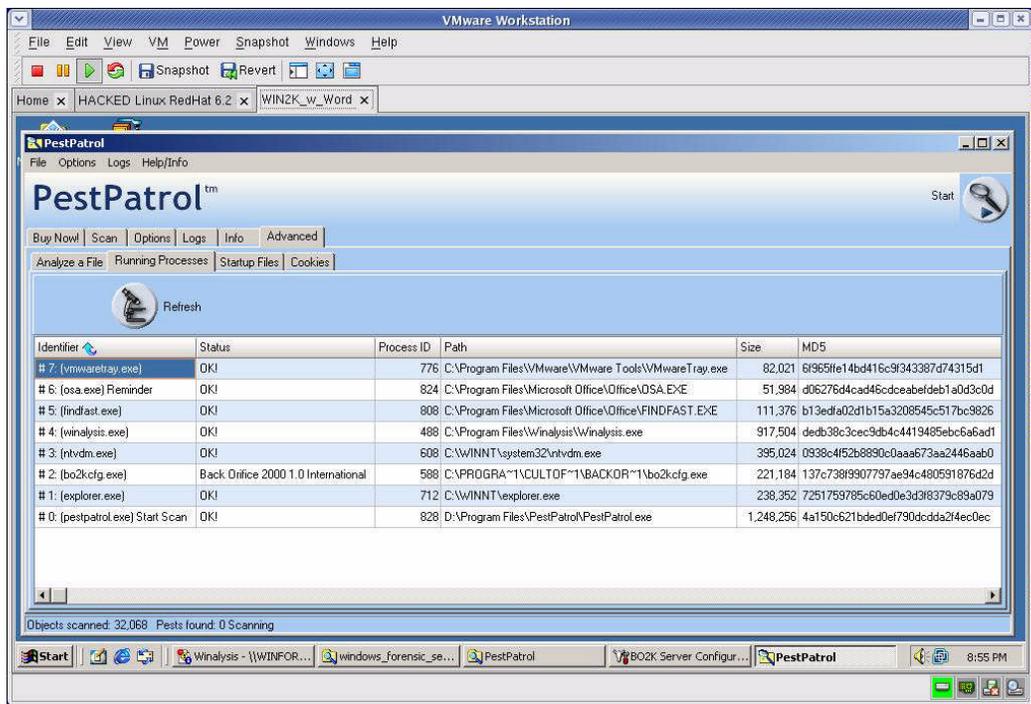


Figure 22 - PestPatrol Running Processes

Finding a remote access trojan client on a compromised system would indicate that the system is being used for purposes not intended by the owner. This could be a zombie involved in a distributed denial of service attack. It could be that the perpetrator is using the system to cover his tracks to make it harder to find and convict him. Finding a remote access trojan server on a suspected criminal’s machine may implicate him for using systems without authorization and as an orchestrator of the crime in which the victim machines were used.

Uncontrolled Test 1 – Unknown System

PestPatrol was run on this system, from the cdrom, after removing the network connection. See [Appendix I – Unknown System PestPatrol Output](#) for a complete listing (in consideration of length, many shared music files, multiple related browser hijackers, and cookies were deleted). Upon interviewing the owner of the system, it was learned that the system had not been rebuilt in six years. As mentioned in the summary, it had been exposed to the internet only behind a firewall/router using NAT and DHCP. The owner did admit that Morpheous and Kazaa had been in use on the system previously, so it was concluded that the system was not likely used to house an attacker’s warez or

illicit material. The unidentified trojan appears to be a utility included with some game distributions for copy protection purposes. This system is used for a multitude of on and off-line games. Again, this may not lead anywhere. Many browser hijackers and adware were noted which may explain some of the performance degradation, but likely not an indication of criminal compromise (more like visiting inhospitable websites).

One disconcerting detail noted was that many pests found were labeled as adware yet when the pest encyclopedia was consulted it was listed as something more ominous. For example, TrojanDropper.Win32.Siboco.a is a dropper class pest. The description for this pest category found on <http://www3.ca.com/securityadvisor/pest/pest.aspx?id=453088188> is, "In viruses and trojans, the dropper is the part of the program that installs the hostile code onto the system." To an investigator this information may lead to attempting to locate additional trojans or viruses. UCSearch is actually classified a downloader which is, "A program designed to retrieve and install additional files, when run. Most will be configured to retrieve from a designated web or FTP site." Upon further investigation, it appears this one is more benign than some other downloaders may be. Ares is a password cracker which according to the site is,

A tool to decrypt a password or password file. PestPatrol uses the term both for programs that take an algorithmic approach to cracking, as well as those that use brute force with a password cracking word list. Password crackers have legitimate uses by security administrators, who want to find weak passwords in order to change them and improve system security.

The system owner did not have the knowledge of password crackers, so this finding should definitely be pursued further. Possibly the dropper and this code are related in some way. Maybe victim machines are being used for cpu cycles to do password cracking and pass the data back to the source via some spyware.

Presentation

The output of PestPatrol can be presented in multiple formats. Text, HTML, comma separated values, etc. The text report as included in this document can be described as follows (red text):

Scan of 1/25/2005 1:39:39 AM	(date and time of scan)
Pests found: 9	(total pests found this scan)
Area scanned: C:\	(drives selected)
User Name: Administrator	(username under which scan ran)
MAC Address: XX-XX-XX-XX-XX-XX	(note: author masked for privacy)
Computer Name: WINFORENSICS	(hardware/software summary info)
Volume Name:	
File System Name: NTFS	

Volume Serial No: 2089221924
Windows Version: Windows 2000
Product Edition: Evaluation
PestPatrol version: 6/7/2004 4.4.3.24
PPServer.dll version: 1/26/2003
PPClean version: 10/6/2004 4.5.4.14
PPfile.dat version: 10/6/2004
PPInfo.dat version: 10/6/2004
Spyware.dat version: 10/6/2004
PPMemCheck version: 4/2/2004
PestPatrolCL version: 6/7/2004 4.4.3.19
PPUpdater version: 5/3/2004 4.4.3.36

Pest: (common name of pest)
Pest Info: Category: Adware Background Info: Click here
(pest category and quick link to description on website)
File Info: In File: C:\Program Files\iks\readme.txt Date: 1/23/2003 4:30:46 PM
(specific file name and location information, md5 sum may be available)
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
(information about the confidence of the finding along with threat level description and recommended action)
Action: Ignored (action taken again pest)

Conclusion

Most desktop and often Windows server attacks lead to installation of a trojan or some other unwanted software at some point. Use of a pest management tool, such as PestPatrol, should not be considered exhaustive investigation. The intent of this exercise was to show that using such a tool could accelerate the findings. It could be used as an easy method by which an investigator could quickly identify malicious code that very often indicates compromise on a victim desktop or server. Using this method as an initial step in investigating a suspected criminal's system could give indication of intent and provide direction in an investigation.

It is recognized that there is minimal system modification even when using the tool from a read only source. Additionally, there may be instances when the pest management tool does not identify the malware because it is yet to be discovered, evaluated or added to the comparison database. Unknown concealment methods may also render this tool inadequate. However, in a situation where the investigation is being done on an image copy, especially when it is in an environment where known state can be easily reinstated, there is no reason to not include this type of tool in the arsenal.

Dependence on the internet is increasing. Number of persons connected to the internet is increasing. The amount of malware continues to increase. Storage size and computing power continue to rapidly increase. Unfortunately security

awareness and practices among the general population is still severely lagging for many reasons. Any tools that could aid in the analysis of compromise are welcome and even necessary as the number of incidents will no doubt continue to increase.

The following must be kept in mind if PestPatrol is used for forensic purpose:

- Most pest management tools today, including PestPatrol, run in a Windows environment.
- When using PestPatrol to detect malicious software, be sure to visit the “Options – What to Search For” configuration page to ensure detection of all types of malware in scope with a given investigation.
- Be sure to eject the PestPatrol cdrom during system reboot.
- Be aware when evaluating the output, it is somewhat misleading in that the category of the pest is not always accurately reported, therefore, it would be wise to review the whole list. The search function of the pest encyclopedia becomes a very valuable tool for this task. Hopefully, the misreporting of category type will be corrected in later versions of PestPatrol. This would make the tool much more valuable for this forensic purpose as it would speed the time allocated to accurate malware identification.
- Lastly, some mechanism will need to be put into place to address the issues of malware signatures becoming outdated.

© SANS Institute 2005, All rights reserved.

Exhibit A – Recovered Policy Documents

The following six documents were recovered by simply mounting the floppy disk image read only and viewing via Microsoft Word.

Acceptable Encryption Policy

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope

This policy applies to all Ballard Industries employees and affiliates.

3.0 Policy

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Bright Industries's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Ballard Industries without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Ballard Industries Confidential information (e.g., Ballard Industries Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

2.0 Scope

All Ballard Industries information is categorized into two main classifications:

- Ballard Industries Public
- Ballard Industries Confidential

Ballard Industries Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Ballard Industries Systems, Inc.

Ballard Industries Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in Ballard Industries Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Ballard Industries Confidential information is "Ballard Industries Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Ballard Industries by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Bright Industries's network to support our operations.

Ballard Industries personnel are encouraged to use common sense judgment in securing Ballard Industries Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Ballard Industries Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Ballard Industries Confidential information in question.

3.1 **Minimal Sensitivity:** General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Ballard Industries Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Ballard Industries Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Ballard Industries information is presumed to be "Ballard Industries Confidential" unless expressly determined to be Ballard Industries Public information by a Ballard Industries employee with authority to do so.

Access: Ballard Industries employees, contractors, people with a business need to know.

Distribution within Bright Industries: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Ballard Industries internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Ballard Industries premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 **More Sensitive:** Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Ballard Industries Confidential" or "Ballard Industries Proprietary", wish to label the information "Ballard Industries Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Ballard Industries employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within Bright Industries: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Ballard Industries internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within Bright Industries, but should

be encrypted or sent via a private link to approved recipients outside of Ballard Industries premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on Ballard Industries premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Ballard Industries Confidential information is very sensitive, you may should label the information "Ballard Industries Internal: Registered and Restricted", "Ballard Industries Eyes Only", "Ballard Industries Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Ballard Industries Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Ballard Industries employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within Bright Industries: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of Ballard Industries internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within Bright Industries, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Ballard Industries premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms and Definitions

Appropriate measures

To minimize risk to Ballard Industries from an outside business connection. Ballard Industries computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Ballard Industries corporate information, the amount of information at risk is minimized.

Configuration of Bright Industries-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here...]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Ballard Industries is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the `chmod` command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Bright Industries.

Encryption

Secure Ballard Industries Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to Bright Industries's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that Ballard Industries has control over its entire distance. For example, all Ballard Industries networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. Ballard Industries also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which Ballard Industries has established private links include all announced acquisitions and some short-term temporary links

6.0 Revision History

© SANS Institute 2005, Author retains full rights.

Internal Lab Security Policy

1.0 Purpose

This policy establishes information security requirements for Ballard Industries labs to ensure that Ballard Industries confidential information and technologies are not compromised, and that production services and other Ballard Industries interests are protected from lab activities.

2.0 Scope

This policy applies to all internally connected labs, Ballard Industries employees and third parties who access Ballard Industries labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities

1. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.
2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard Ballard Industries from security vulnerabilities.
3. Lab managers are responsible for the lab's compliance with all Ballard Industries security policies. The following are particularly important: *Password Policy for networking devices and hosts*, *Wireless Security Policy*, *Anti-Virus Policy*, and *physical security*.
4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.
5. The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.
6. The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.
7. The Network Support Organization must record all lab IP addresses, which are routed within Ballard Industries networks, in Enterprise Address Management database along with current contact information for that lab.
8. Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.
9. All user passwords must comply with Bright Industries's *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains Ballard Industries proprietary information, group account passwords must be

changed within three (3) days following a change in group membership.

10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

11. InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements

1. All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

2. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.

3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-Ballard Industries networks. These activities must be restricted within the lab.

4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

5. InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

6. Lab owned gateway devices are required to comply with all Ballard Industries product security advisories and must authenticate against the Corporate Authentication servers.

7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with Bright Industries's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

8. In labs where non-Ballard Industries personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no Ballard Industries confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must adhere to the *Open Areas Policy*.

10. All lab external connection requests must be reviewed and approved by InfoSec. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

11. All labs networks with external connections must not be connected to Ballard Industries corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from InfoSec is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including

termination of employment.

5.0 Definitions

- Internal - A lab that is within Bright Industries's corporate firewall and connected to Bright Industries's corporate production network
- Network Support Organization - Any InfoSec approved Ballard Industries support organization that manages the networking of non-lab networks.
- Lab Manager - The individual responsible for all lab activities and personnel
- Lab - A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
- External Connections (also known as DMZ) - External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
- Lab Owned Gateway Device - A lab owned gateway device is the lab device that connects the lab network to the rest of Ballard Industries network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by InfoSec.
- Telco - A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.
- Traffic - Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
- Firewall - A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by InfoSec.
- Extranet - Connections between third parties that require access to connections non-public Ballard Industries resources, as defined in InfoSec's Extranet policy (link).
- DMZ (De-Militarized Zone) - This describes network that exists outside of primary corporate firewalls, but are still under Ballard Industries administrative control.

6.0 Revision History

© SANS Institute 2005

Internal Lab Security Policy1

1.0 Purpose

This policy establishes information security requirements for Ballard Industries labs to ensure that Ballard Industries confidential information and technologies are not compromised, and that production services and other Ballard Industries interests are protected from lab activities.

2.0 Scope

This policy applies to all internally connected labs, Ballard Industries employees and third parties who access Ballard Industries labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents. DMZ Labs and stand-alone, air-gapped labs are exempt from this policy. DMZ labs must comply with the *DMZ Lab Security Policy*.

3.0 Policy

3.1 Ownership Responsibilities

1. Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.
2. Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard Ballard Industries from security vulnerabilities.
3. Lab managers are responsible for the lab's compliance with all Ballard Industries security policies. The following are particularly important: *Password Policy for networking devices and hosts*, *Wireless Security Policy*, *Anti-Virus Policy*, and *physical security*.
4. The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.
5. The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.
6. The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.
7. The Network Support Organization must record all lab IP addresses, which are routed within Ballard Industries networks, in Enterprise Address Management database along with current contact information for that lab.
8. Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.
9. All user passwords must comply with Bright Industries's *Password Policy*. In addition, individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months). For any lab device that contains Ballard Industries proprietary information, group account passwords must be

changed within three (3) days following a change in group membership.

10. No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

11. InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2 General Configuration Requirements

1. All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

2. Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.

3. Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-Ballard Industries networks. These activities must be restricted within the lab.

4. Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

5. InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

6. Lab owned gateway devices are required to comply with all Ballard Industries product security advisories and must authenticate against the Corporate Authentication servers.

7. The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with Bright Industries's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

8. In labs where non-Ballard Industries personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no Ballard Industries confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

9. Infrastructure devices (e.g. IP Phones) needing corporate network connectivity must adhere to the *Open Areas Policy*.

10. All lab external connection requests must be reviewed and approved by InfoSec. Analog or ISDN lines must be configured to only accept trusted call numbers. Strong passwords must be used for authentication.

11. All labs networks with external connections must not be connected to Ballard Industries corporate production network or any other internal network directly or via a wireless connection, or via any other form of computing equipment. A waiver from InfoSec is required where air-gapping is not possible (e.g., Partner Connections to third party networks).

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including

termination of employment.

5.0 Definitions

- Internal - A lab that is within Bright Industries's corporate firewall and connected to Bright Industries's corporate production network
- Network Support Organization - Any InfoSec approved Ballard Industries support organization that manages the networking of non-lab networks.
- Lab Manager - The individual responsible for all lab activities and personnel
- Lab - A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
- External Connections (also known as DMZ) - External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
- Lab Owned Gateway Device - A lab owned gateway device is the lab device that connects the lab network to the rest of Ballard Industries network. All traffic between the lab and the corporate production network must pass through the lab owned gateway device unless approved by InfoSec.
- Telco - A Telco is the equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include BRI, or Basic Rate Interface - a structure commonly used for ISDN service, and PRI, Primary Rate Interface - a structure for voice/dial-up service.
- Traffic - Mass volume of unauthorized and/or unsolicited network Spamming/Flooding traffic.
- Firewall - A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by InfoSec.
- Extranet - Connections between third parties that require access to connections non-public Ballard Industries resources, as defined in InfoSec's Extranet policy (link).
- DMZ (De-Militarized Zone) - This describes network that exists outside of primary corporate firewalls, but are still under Ballard Industries administrative control.

6.0 Revision History

© SANS Institute 2005

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Ballard Industries entire corporate network. As such, all Ballard Industries employees (including contractors and vendors with access to Ballard Industries systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Ballard Industries facility, has access to the Ballard Industries network, or stores any non-public Ballard Industries information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Bright Industries. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "Bright Industries", "sanjose", "sanfran" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-=\`{}[]:~<?.,/)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for Ballard Industries accounts as for other non-Ballard Industries access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Ballard Industries access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Ballard Industries passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Ballard Industries information.

Here is a list of "don't's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the Ballard Industries Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms

Application Administration Account
(e.g., Oracle database administrator, ISSU administrator).

Definitions

Any account that is for the administration of an application

7.0 Revision History

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to Ballard Industries network from any host. These standards are designed to minimize the potential exposure to Ballard Industries from damages which may result from unauthorized use of Ballard Industries resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Ballard Industries internal systems, etc.

2.0 Scope

This policy applies to all Ballard Industries employees, contractors, vendors and agents with a Bright Industries-owned or personally-owned computer or workstation used to connect to the Ballard Industries network. This policy applies to remote access connections used to do work on behalf of Bright Industries, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of Ballard Industries employees, contractors, vendors and agents with remote access privileges to Ballard Industries corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Bright Industries.
2. General access to the Internet for recreational use by immediate household members through the Ballard Industries Network on personal computers is permitted for employees that have flat-rate services. The Ballard Industries employee is responsible to ensure the family member does not violate any Ballard Industries policies, does not perform illegal activities, and does not use the access for outside business interests. The Ballard Industries employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Ballard Industries network:
 - a. *Acceptable Encryption Policy*
 - b. *Virtual Private Network (VPN) Policy*
 - c. *Wireless Communications Policy*
 - d. *Acceptable Use Policy*
4. For additional information regarding Ballard Industries remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any Ballard Industries employee provide their login or email password to anyone, not even family members.
3. Ballard Industries employees and contractors with remote access privileges must ensure that their Bright Industries-owned or personal computer or workstation, which is remotely connected to Ballard Industries corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Ballard Industries employees and contractors with remote access privileges to Ballard Industries corporate network must not use non-Ballard Industries email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Ballard Industries business, thereby ensuring that official business is never confused with personal business.

5. Routers for dedicated ISDN lines configured for access to the Ballard Industries network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
9. All hosts that are connected to Ballard Industries internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to Ballard Industries networks must meet the requirements of Bright Industries-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Ballard Industries production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Bright Industries-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Ballard Industries and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access Any access to Ballard Industries corporate network through a non-Ballard Industries controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-Ballard Industries network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Ballard Industries corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

© SANS Institute 2005, Author retains full rights.

Exhibit B – MAC TimeLine – Leszczynski Floppy

```
Sat Feb 03 2001 21:44:16 36864 m.. -/-rwxrwxrwx 0 0 5 A:/CamShell.dll( _AMSHLL.DLL) (deleted)
36864 m.. -rwxrwxrwx 0 0 5 <v1_5-_AMSHLL.DLL-dead-5>
Thu Apr 22 2004 19:31:06 33423 m.. -/-rwxrwxrwx 0 0 17 A:/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
32256 m.. -/-rwxrwxrwx 0 0 13 A:/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
Fri Apr 23 2004 13:53:56 727 m.. -rwxrwxrwx 0 0 28 <v1_5-_ndex.htm-dead-28>
727 m.. -/-rwxrwxrwx 0 0 28 A:/_ndex.htm (deleted)
Fri Apr 23 2004 14:54:32 215895 m.. -/-rwxrwxrwx 0 0 23 A:/Remote_Access_Policy.doc (REMOTE~1.DOC)
Fri Apr 23 2004 14:55:26 307935 m.. -/-rwxrwxrwx 0 0 20 A:/Password_Policy.doc (PASSWO~1.DOC)
Fri Apr 23 2004 17:10:50 22528 m.. -/-rwxrwxrwx 0 0 27 A:/Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Fri Apr 23 2004 17:11:10 42496 m.. -/-rwxrwxrwx 0 0 9 A:/Information_Sensitivity_Policy.doc (INFORM~1.DOC)
Mon Apr 26 2004 03:00:00 215895 .a. -/-rwxrwxrwx 0 0 23 A:/Remote_Access_Policy.doc (REMOTE~1.DOC)
42496 .a. -/-rwxrwxrwx 0 0 9 A:/Information_Sensitivity_Policy.doc (INFORM~1.DOC)
36864 .a. -/-rwxrwxrwx 0 0 5 A:/CamShell.dll ( _AMSHLL.DLL) (deleted)
36864 .a. -rwxrwxrwx 0 0 5 <v1_5-_AMSHLL.DLL-dead-5>
727 .a. -rwxrwxrwx 0 0 28 <v1_5-_ndex.htm-dead-28>
32256 .a. -/-rwxrwxrwx 0 0 13 A:/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
33423 .a. -/-rwxrwxrwx 0 0 17 A:/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
727 .a. -/-rwxrwxrwx 0 0 28 A:/_ndex.htm (deleted)
307935 .a. -/-rwxrwxrwx 0 0 20 A:/Password_Policy.doc (PASSWO~1.DOC)
22528 .a. -/-rwxrwxrwx 0 0 27 A:/Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Mon Apr 26 2004 12:46:18 36864 .c -/-rwxrwxrwx 0 0 5 A:/CamShell.dll ( _AMSHLL.DLL) (deleted)
36864 .c -rwxrwxrwx 0 0 5 <v1_5-_AMSHLL.DLL-dead-5>
Mon Apr 26 2004 12:46:20 42496 .c -/-rwxrwxrwx 0 0 9 A:/Information_Sensitivity_Policy.doc (INFORM~1.DOC)
Mon Apr 26 2004 12:46:22 32256 .c -/-rwxrwxrwx 0 0 13 A:/Internal_Lab_Security_Policy1.doc (INTERN~1.DOC)
Mon Apr 26 2004 12:46:24 33423 .c -/-rwxrwxrwx 0 0 17 A:/Internal_Lab_Security_Policy.doc (INTERN~2.DOC)
Mon Apr 26 2004 12:46:26 307935 .c -/-rwxrwxrwx 0 0 20 A:/Password_Policy.doc (PASSWO~1.DOC)
Mon Apr 26 2004 12:46:36 215895 .c -/-rwxrwxrwx 0 0 23 A:/Remote_Access_Policy.doc (REMOTE~1.DOC)
Mon Apr 26 2004 12:46:44 22528 .c -/-rwxrwxrwx 0 0 27 A:/Acceptable_Encryption_Policy.doc (ACCEPT~1.DOC)
Mon Apr 26 2004 12:47:36 727 .c -rwxrwxrwx 0 0 28 <v1_5-_ndex.htm-dead-28>
727 .c -/-rwxrwxrwx 0 0 28 A:/_ndex.htm (deleted)
```

Exhibit C – MAC TimeLine – Test Floppy Image

Fri Apr 23 2004 10:22:44 215895 ..c -/--wx-wx-wx 0 0 9 -r/Remote_Access_Policy.doc (REMOTE~1.DOC)
Fri Apr 23 2004 12:54:32 215895 m.. -/--wx-wx-wx 0 0 13 -r/Remote_Access_Policy_copied.doc (REMOTE~2.DOC)
215895 m.. -/--wx-wx-wx 0 0 9 -r/Remote_Access_Policy.doc (REMOTE~1.DOC)
Wed Mar 02 2005 00:00:00 215895 .a. -/--wx-wx-wx 0 0 13 -r/Remote_Access_Policy_copied.doc (REMOTE~2.DOC)
14 .a. -/-rwxrwxrwx 0 0 3 -r/test.txt
215895 .a. -/--wx-wx-wx 0 0 9 -r/Remote_Access_Policy.doc (REMOTE~1.DOC)
0 .a. -rwxrwxrwx 0 0 6 <floppy4.img-_EMOTE~1.DOC-dead-6>
0 .a. -/-rwxrwxrwx 0 0 6 -r/Remote_Access_Policy.doc (_EMOTE~1.DOC) (deleted)
Wed Mar 02 2005 09:21:48 14 m.. -/-rwxrwxrwx 0 0 3 -r/test.txt
Wed Mar 02 2005 09:22:06 14 ..c -/-rwxrwxrwx 0 0 3 -r/test.txt
Wed Mar 02 2005 09:22:46 0 ..c -rwxrwxrwx 0 0 6 <floppy4.img-_EMOTE~1.DOC-dead-6>
0 ..c -/-rwxrwxrwx 0 0 6 -r/Remote_Access_Policy.doc (_EMOTE~1.DOC) (deleted)
Wed Mar 02 2005 09:22:48 0 m.. -rwxrwxrwx 0 0 6 <floppy4.img-_EMOTE~1.DOC-dead-6>
0 m.. -/-rwxrwxrwx 0 0 6 -r/Remote_Access_Policy.doc (_EMOTE~1.DOC) (deleted)
Wed Mar 02 2005 09:24:10 215895 ..c -/--wx-wx-wx 0 0 13 -r/Remote_Access_Policy_copied.doc (REMOTE~2.DOC)

Exhibit D – Deleted HTML File

```
<HTML>
<HEAD>
<meta http-equiv=Content-Type content="text/html; charset=ISO-8859-1">
<TITLE>Ballard</TITLE>
</HEAD>
<BODY bgcolor="#EDED"ED">

<center>
<OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0"
WIDTH="800" HEIGHT="600" id="ballard" ALIGN="">
<PARAM NAME=movie VALUE="ballard.swf"> <PARAM NAME=quality VALUE=high> <PARAM NAME=bgcolor
VALUE=#CCCCCC> <EMBED src="ballard.swf" quality=high bgcolor=#CCCCCC WIDTH="800" HEIGHT="600"
NAME="ballard" ALIGN=""
TYPE="application/x-shockwave-flash" PLUGINSOURCE="http://www.macromedia.com/go/getflashplayer"></EMBED>
</OBJECT>
</center>
</BODY>
</HTML>
```

Exhibit E – Recovered Letter of Intent to Commit Crime

The following text was in a file recovered using the un-camouflage function. The file was named Opportunity.txt. It could be viewed using any standard text viewer.

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

Exhibit F – Recovered Client Authorized Table Database

The following records were recovered from the un-camouflaged file called CAT.mdb. The records were displayed using Microsoft Access.

Clients										
First	Last	Phone	Company	Address	Address1	City	State	Zipcode	Account	Password
Bob	Esposito	703-233-2048	Cook Labs	245 Main St		Alexandria	VA	20231	espomain	y4NSHMNf
Jerry	Jackson	410-677-7223	Double J's	11561 W. 27 St.		Baltimore	MD	20278	jack27st	JLbW3Pq5
David	Lee	866-554-0922	Tech Vision	300 Lone Grove Lane		Wichita	KS	30189	leetechv	O1A26a3k
Marie	Horton	800-234-king	King Labs, Inc.	700 King Labs Ave	Suite 900	Biloxi	MS	39533	hortking	Yk7Sr4pA
Lenny	Jones	877-Get-done	Quick Printing	99 E. Grand View Dr		Omaha	NE	56098	joneeast	868y48RH
Jeff	Hayes	404-893-5521	Big Sky First	90 Old Saw Mill Rd		Billings	MT	59332	hayeolds	3R30bb7i
Roger	Forrester	210-586-2312	TCFL	188 Greenville Rd		Austin	TX	77239	forrgree	si4OW8UV
Edward	Cash	212-562-0997	E & C Inc.	76 S. King St	Suite 300	Santa Barbara	CA	80124	cashking	Of8uQ1fC
Steve	Bei	616-833-0129	Island Labs	65 Kiwi Way		Honolulu	HA	93991	beikiwiw	JDH20u26
Jodie	Kelly		Data Movers	7256 Beerwah Ave.	Suite 110	Wetherby	U.K.	LS22 6RG	kellbeer	tmu0ENOk
Patrick	Roy		The Magic Lamp	4150 Regents Park	Row #170	Calgary	CAN	R4316DF	roythema	rJag6Q0O

Exhibit G – Recovered Design Schematics

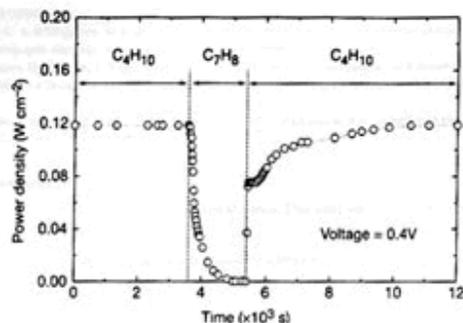


Figure 3 Effect of switching fuel type on the cell with the Cu-ceria composite anode at 973 K. The power density of the cell is shown as a function of time. The fuel was switched from *n*-butane (C₄H₁₀) to toluene (C₇H₈), and back to *n*-butane.

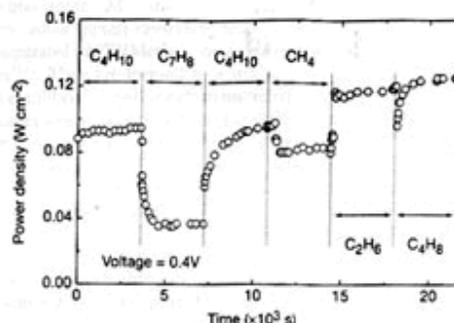
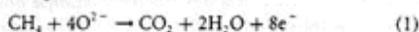


Figure 4 Effect of switching fuel type on the cell with the Cu-doped ceria composite anode at 973 K. The power density is shown as a function of time. The fuels were: *n*-butane (C₄H₁₀), toluene (C₇H₈), *n*-butane, methane (CH₄), ethane (C₂H₆), and 1-butene (C₄H₈).

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 H₂—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 CO₂ and water. (Negligible amounts of CO₂ were formed in a similar experiment with an open circuit.) Second, analysis of the CO₂ formed under steady-state flow conditions, shown in Fig. 2, demonstrates that the rate of CO₂ 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 CO₂ and water according to reactions (1) and (2):



With methane, only trace levels of CO were observed along with CO₂, 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.

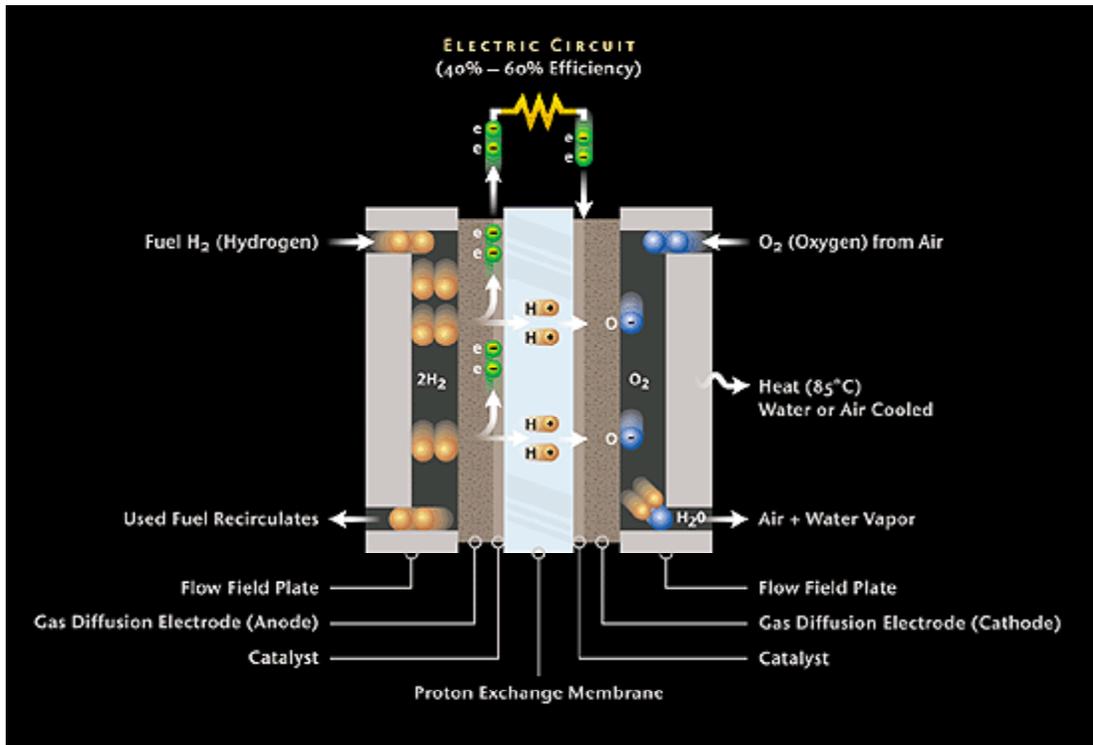
The data in Fig. 4 show that further improvements in cell performance can be achieved. For these experiments, samaria-doped ceria was substituted for ceria in the anode, and the current densities were measured at a potential of 0.4 V at 973 K. The power densities for H₂ and *n*-butane in this particular 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 densities³. 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. □

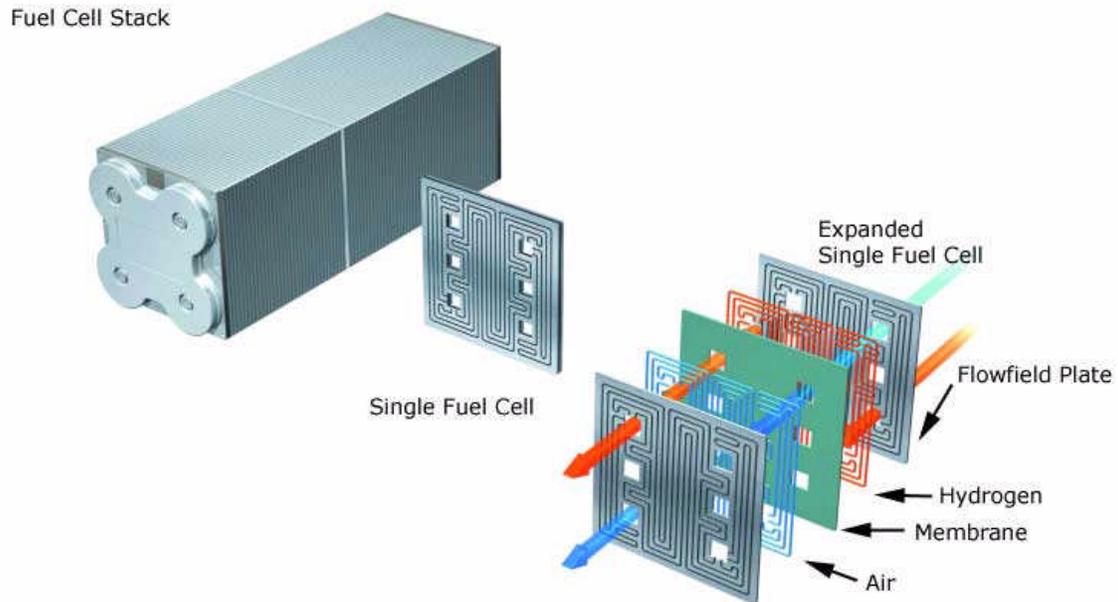
Received 13 September 1999; accepted 26 January 2000.

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., Stubbensach, J., Vohs, J. M. & Gorte, R. J. Ceria-based anodes for the direct oxidation of methane in solid oxide fuel cells. *Langmuir* **11**, 4832–4837 (1995).
5. Park, S., Craciun, R., Vohs, J. M. & Gorte, R. J. Direct oxidation of hydrocarbons in a solid oxide fuel cell: I. methane oxidation. *J. Electrochem. Soc.* **146**, 3603–3605 (1999).
6. Steele, B. C. H., Kelly, I., Middleton, P. H. & Rudkin, R. Oxidation of methane in solid-state electrochemical reactors. *Solid State Ionics* **28**, 1547–1552 (1988).
7. Lloyd, A. C. The power plant in your basement. *Sci. Am.* **281**(1), 80–86 (1999).



© SANS Institute

Design of a PEM Fuel Cell



The preceding three design documents were recovered using the un-camouflage option of the Camouflage tool. The original/recovered file names were respectively:

1. Hydrocarbon%20fuel%20cell%20page2.jpg
2. pem_fuelcell.gif
3. PEM-fuel-cell-large.jpg

© SANS Institute 2005

Appendix A – Camouflage System Modifications

Changes from Snapshot Details for Files

Name

A:\Remote_Access_Policy_copied.doc

New File

A:\Remote_Access_Policy.doc

New File

A:\test.txt

New File

A:\RAP_to_floppy_after_text.doc

New File

C:\WINDOWS\system32\config\software.LOG

File Last Modified Date C:\WINDOWS\system32\config\system.LOG

File Last Modified Date 3/2/2005 9:11:53 PM 3/2/2005 9:06:08 PM

C:\WINDOWS\Prefetch\CAMOUFLAGE.EXE-24B5E0B3.pf

File Size 25342 26218

File Last Modified Date 3/2/2005 9:08:19 PM 3/2/2005 12:28:48 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:05 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\current.bj

File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Files

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:05 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:05 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:05 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Services

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\System

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Users

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes

Folder Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\20050302210606.bj

New File

C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes\baseline.bl

File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes\baseline.log

File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM

C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes\changes.bl

File Size 131 132

File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes\changes.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Users\baseline.bl
 File Size 830 828
 File Last Modified Date 3/2/2005 9:11:54 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Users\baseline.log
 File Last Modified Date 3/2/2005 9:11:54 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Users\changes.bl
 File Size 132 131
 File Last Modified Date 3/2/2005 9:11:54 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Users\changes.log
 File Last Modified Date 3/2/2005 9:11:54 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Users\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\System\baseline.bl
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\System\baseline.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\System\changes.bl
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\System\changes.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\System\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares\baseline.bl
 File Last Modified Date 3/2/2005 9:11:53 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares\baseline.log
 File Last Modified Date 3/2/2005 9:11:54 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares\changes.bl
 File Size 161 157
 File Last Modified Date 3/2/2005 9:11:54 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares\changes.log
 File Last Modified Date 3/2/2005 9:11:54 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Services\baseline.bl
 File Last Modified Date 3/2/2005 9:11:53 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Services\baseline.log
 File Last Modified Date 3/2/2005 9:11:53 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Services\changes.bl
 File Size 145 146
 File Last Modified Date 3/2/2005 9:11:53 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Services\changes.log
 File Last Modified Date 3/2/2005 9:11:53 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Services\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler\baseline.bl
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler\baseline.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler\changes.bl

File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler\changes.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights\baseline.bl
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights\baseline.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights\changes.bl
 File Size 131 132
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights\changes.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\baseline.bl
 File Size 5120698 3686488
 File Last Modified Date 3/2/2005 9:12:00 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\baseline.log
 File Size 182 42
 File Last Modified Date 3/2/2005 9:12:00 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\changes.bl
 File Size 133 135
 File Last Modified Date 3/2/2005 9:12:01 PM 3/2/2005 5:21:28 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\changes.log
 File Last Modified Date 3/2/2005 9:12:01 PM 3/2/2005 5:21:28 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups\baseline.bl
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups\baseline.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups\changes.bl
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups\changes.log
 File Last Modified Date 3/2/2005 9:11:50 PM 3/2/2005 9:06:06 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups\20050302210606.bl
 New File
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\baseline.bl
 File Size 182360 0
 File Last Modified Date 3/2/2005 9:11:55 PM 3/2/2005 9:06:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\baseline.log
 File Size 156 244
 File Last Modified Date 3/2/2005 9:12:01 PM 3/2/2005 9:06:14 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\changes.bl
 File Last Modified Date 3/2/2005 9:06:23 PM 3/2/2005 5:22:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\changes.log
 File Last Modified Date 3/2/2005 9:06:23 PM 3/2/2005 5:22:08 PM
 C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\20050302210606.bl
 New File
 C:\Documents and Settings\WINFORENSICS\ntuser.dat.LOG
 File Last Modified Date 3/2/2005 9:11:47 PM 3/2/2005 9:05:41 PM
 C:\Documents and Settings\WINFORENSICS\Recent

Folder Last Modified Date 3/2/2005 9:11:03 PM 3/2/2005 5:19:17 PM
 C:\Documents and Settings\WINFORENSICS\Recent\3½ Floppy (A).lnk
 File Last Modified Date 3/2/2005 9:11:03 PM 3/2/2005 12:29:01 PM
 C:\Documents and Settings\WINFORENSICS\Recent\camo test.lnk
 File Size 504 765
 File Last Modified Date 3/2/2005 9:10:21 PM 3/2/2005 5:19:17 PM

C:\Documents and Settings\WINFORENSICS\Recent\Remote_Access_Policy.doc.lnk
 File Last Modified Date 3/2/2005 9:10:21 PM 3/2/2005 12:28:44 PM
 C:\Documents and Settings\WINFORENSICS\Recent\RAP_to_floppy_after_text.doc.lnk
 New File
 C:\Documents and Settings\WINFORENSICS\Local Settings\Temp
 Folder Last Modified Date 3/2/2005 9:10:03 PM 3/2/2005 8:24:34 PM

Changes from Snapshot Details for Registry

Name

HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E96C-E325-11CE-BFC1-08002BE10318}\0021
 Key Last Modified Date
 HKLM\SYSTEM\ControlSet001\Control\Class\{4D36E96C-E325-11CE-BFC1-08002BE10318}\0021
 Key Last Modified Date
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\EBD9F446BDECFA54CA8B2E66297BF426\Usage
 Key Last Modified Date
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\EBD9F446BDECFA54CA8B2E66297BF426\Usage\ECDC6
 Value Changed
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\EBD9F446BDECFA54CA8B2E66297BF426\Usage\DragToDisc
 Value Changed
 HKLM\SOFTWARE\Microsoft\Cryptography\ RNG
 Key Last Modified Date
 HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed
 Value Changed
 HKU\S-1-5-21-839522115-1085031214-725345543-1003\SessionInformation

 HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache

 HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\PROGRA~1\BRODER~1\THEPRI~1\ps.exe

 HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Program Files\Microsoft Office\OFFICE11\MSACCESS.EXE

 HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Program Files\Camouflage\Camouflage.exe

 HKU\S-1-5-21-839522115-1085031214-725345543-

1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell\Mode

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell\CollInfo

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell\MinPos1280x1024(1).x

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell\MinPos1280x1024(1).y

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell\WinPos1280x1024(1).left

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell\WinPos1280x1024(1).top

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell\WinPos1280x1024(1).right

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\Bags\13\Shell\WinPos1280x1024(1).bottom

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count\HRZR_HVGBBYONE

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count\HRZR_HVGBBYONE:0k1,133

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUListEx

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\108

HKU\S-1-5-21-839522115-1085031214-725345543-

1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\MRUListEx

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\6

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\1

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder\4

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\doc

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\doc\MRUListEx

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\doc\3

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\doc\4

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\doc\OpenWithList

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\doc\OpenWithList\MRUList

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\doc

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\doc\MRUList

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\doc\4

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*\MRUList

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*\f

HKU\S-1-5-21-839522115-1085031214-725345543-
1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

HKU\S-1-5-21-839522115-1085031214-725345543-

1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\0

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\1
Value Changed A:\Remote_Access_PoliA:\Remote_Access_Policy99.doc

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\2
Value Changed A:\Remote_Access_PoliC:\Documents and Settings\WINFORENSICS\My
Documents\giac\camo test\Remote_Access_Policy_write2.doc

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\3
Value Changed A:\Remote_Access_PoliC:\Documents and Settings\WINFORENSICS\My
Documents\giac\camo test\Remote_Access_Policy_write.doc

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\4
Value Changed C:\Documents and SettC:\Documents and Settings\WINFORENSICS\My
Documents\giac\camo test\Remote_Access_Policy_copied.doc

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\5
Value Changed C:\Documents and SettA:\Remote_Access_Policy.doc ac\camo
test\Remote_Access_Policy_write.doc

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\6
Value Changed C:\Documents and SettA:\Remote_Access_Policy2.doc c\camo
test\Remote_Access_Policy_copied.doc

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\7
Value Changed A:\Remote_Access_PoliA:\camo test\Remote_Access_Policy.doc

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\8
Value Changed A:\camo test\Remote_AC:\Documents and Settings\WINFORENSICS\My
Documents\giac\camo test\Remote_Access_Policy_camod.doc

HKU\S-1-5-21-839522115-1085031214-725345543-1003\Software\Camouflage\OutputFile\9
Value Changed C:\Documents and SettA:\recamo4\recamo_Remote_Access_Policy.doc
mote_Access_Policy_camod.doc

© SANS Institute 2005

Appendix B – Summary of File Info to Aid in Determining Sequence of Events

Filename	md5 checksum	date on floppy listing	dates in camo file	dates on timeline
Acceptable_Encryption_Policy.doc	f785bald99888e68f45dabeddb0b4541	Apr 23 14:10	n/a	M Fri Apr 23 2004 17:10:50 A Mon Apr 26 2004 03:00:00 C Mon Apr 26 2004 12:46:44
Information_Sensitivity_Policy.doc	99c5dec518b142bd945e8d7d2fad2004	Apr 23 14:11	n/a	M Fri Apr 23 2004 17:11:10 A Mon Apr 26 2004 03:00:00 C Mon Apr 26 2004 12:46:20
Internal_Lab_Security_Policy1.doc	e0c43ef38884662f5f27d93098e1c607	Apr 22 16:31	n/a	M Thu Apr 22 2004 19:31:06 A Mon Apr 26 2004 03:00:00 C Mon Apr 26 2004 12:46:22
Internal_Lab_Security_Policy.doc	on floppy - wrapper, see timeline b9387272b11aea86b60a487fbdc1b336 in camo - included, see camo file e0c43ef38884662f5f27d93098e1c607	Apr 22 16:31	M Apr 22 16:31 A Apr 23 14:58 C Apr 22 16:30	M Thu Apr 22 2004 19:31:06 A Mon Apr 26 2004 03:00:00 C Mon Apr 26 2004 12:46:24
Password_Policy.doc	on floppy - wrapper, see timeline ac34c6177ebdcaf4adc41f0e181belbc in camo - included, see camo file e5066b0fb7b91add563a400f042766e4	Apr 23 11:55	M Apr 23 11:55 A Apr 23 14:58 C Apr 23 09:22	M Fri Apr 23 2004 14:55:26 A Mon Apr 26 2004 03:00:00 C Mon Apr 26 2004 12:46:26
Remote_Access_Policy.doc	on floppy - wrapper, see timeline 5b38d1ac1f94285db2d2246d28fd07e8 in camo - included, see camo file 2afb005271a93d44b6a8489dc4635c1c	Apr 23 11:54	M Apr 23 11:54 A Apr 23 15:00 C Apr 23 09:22	M Fri Apr 23 2004 14:54:32 A Mon Apr 26 2004 03:00:00 C Mon Apr 26 2004 12:46:36
CamShell.dll	4e986ab0909d2946bed868b5f896906f	n/a	n/a	M Feb 03 2001 21:44:16 A Mon Apr 26 2004 03:00:00 C Mon Apr 26 2004 12:46:18
_ndex.htm	n/a	n/a	n/a	M Fri Apr 23 2004 13:53:56 A Mon Apr 26 2004 03:00:00 C Mon Apr 26 2004 12:47:36
CAT.MDB	c3a869ff6b71c7be3eb06b6635c864b1	n/a	M Apr 23 11:21 A Apr 23 15:00 C Apr 22 15:57	n/a
Opportunity.txt	3ebd8382a19c88c1d276645035e97ce9	n/a	M Apr 23 14:03 A Apr 23 14:59 C Apr 23 11:19	n/a
Hydrocarbon%20fuel%20cell%20page2.jpg	9da5d4c42fdf7a979ef5f09d33c0a444	n/a	M Apr 23 10:21 A Apr 23 14:59 C Apr 23 10:21	n/a
pem_fuelcell.gif	864e397c2f38ccfb778f348817f98b91	n/a	M Apr 23 10:15 A Apr 23 14:59 C Apr 23 10:19	n/a

PEM-fuel-cell-large.jpg	5e39dcc44acccdca7bba0c15c6901c43	n/a	M A C	Apr 23 11:54 Apr 23 15:00 Apr 23 09:22	n/a
-------------------------	----------------------------------	-----	-------------	--	-----

© SANS Institute 2005, Author retains full rights.

Appendix C – Registry Entries After Tool Removal

Key Name: HKEY_CURRENT_USER\Software\Camouflage
Class Name: <NO CLASS>
Last Write Time: 3/2/2005 - 10:00 PM

Key Name: HKEY_CURRENT_USER\Software\Camouflage\CamouflageFile
Class Name: <NO CLASS>
Last Write Time: 3/2/2005 - 12:04 AM

Value 0

Name: 0
Type: REG_SZ
Data: C:\Documents and Settings\WINFORENSICS\My Documents\giac\camo
test\Remote_Access_Policy.doc

Value 1

Name: 1
Type: REG_SZ
Data: A:\camo test\Remote_Access_Policy.doc

Value 2

Name: 2
Type: REG_SZ
Data: A:\recamo4\Remote_Access_Policy.doc

Value 3

Name: 3
Type: REG_SZ
Data: A:\recamo\recamo2\Remote_Access_Policy.doc

Value 4

Name: 4
Type: REG_SZ
Data: C:\Downloads\gcfa\camo_files\Remote_Access_Policy.doc

Key Name: HKEY_CURRENT_USER\Software\Camouflage\frmMain
Class Name: <NO CLASS>
Last Write Time: 3/2/2005 - 12:04 AM

Value 0

Name: WindowState
Type: REG_DWORD
Data: 0x0

Value 1

Name: Left
Type: REG_DWORD
Data: 0x1392

Value 2

Name: Top
Type: REG_DWORD
Data: 0x1b99

Value 3

Name: Width

Type: REG_DWORD
Data: 0x1ce3

Value 4

Name: Height
Type: REG_DWORD
Data: 0xd5c

Key Name: HKEY_CURRENT_USER\Software\Camouflage\frmMain\CamouflageFileList
Class Name: <NO CLASS>
Last Write Time: 1/26/2005 - 8:14 AM

Value 0

Name: File
Type: REG_DWORD
Data: 0x1130

Value 1

Name: Size
Type: REG_DWORD
Data: 0x4b0

Value 2

Name: Created
Type: REG_DWORD
Data: 0x898

Value 3

Name: Modified
Type: REG_DWORD
Data: 0x898

Value 4

Name: Accessed
Type: REG_DWORD
Data: 0x708

Value 5

Name: Attributes
Type: REG_DWORD
Data: 0x3e8

Key Name: HKEY_CURRENT_USER\Software\Camouflage\frmMain\UncamouflageFileList
Class Name: <NO CLASS>
Last Write Time: 1/26/2005 - 8:14 AM

Value 0

Name: File
Type: REG_DWORD
Data: 0x1130

Value 1

Name: Size
Type: REG_DWORD
Data: 0x4b0

Value 2

Name: Created

Type: REG_DWORD
Data: 0x898

Value 3
Name: Modified
Type: REG_DWORD
Data: 0x898

Value 4
Name: Accessed
Type: REG_DWORD
Data: 0x708

Value 5
Name: Attributes
Type: REG_DWORD
Data: 0x3e8

Key Name: HKEY_CURRENT_USER\Software\Camouflage\OutputFile
Class Name: <NO CLASS>
Last Write Time: 3/2/2005 - 9:11 PM

Value 0
Name: 0
Type: REG_SZ
Data: A:\RAP_to_floppy_after_text.doc

Value 1
Name: 1
Type: REG_SZ
Data: A:\Remote_Access_Policy.doc

Value 2
Name: 2
Type: REG_SZ
Data: A:\Remote_Access_Policy98.doc

Value 3
Name: 3
Type: REG_SZ
Data: A:\Remote_Access_Policy99.doc

Value 4
Name: 4
Type: REG_SZ
Data: C:\Documents and Settings\WINFORENSICS\My Documents\giac\camo
test\Remote_Access_Policy_write2.doc

Value 5
Name: 5
Type: REG_SZ
Data: C:\Documents and Settings\WINFORENSICS\My Documents\giac\camo
test\Remote_Access_Policy_write.doc

Value 6
Name: 6
Type: REG_SZ
Data: C:\Documents and Settings\WINFORENSICS\My Documents\giac\camo

test\Remote_Access_Policy_copied.doc

Value 7

Name: 7
Type: REG_SZ
Data: A:\Remote_Access_Policy2.doc

Value 8

Name: 8
Type: REG_SZ
Data: A:\camo test\Remote_Access_Policy.doc

Value 9

Name: 9
Type: REG_SZ
Data: C:\Documents and Settings\WINFORENSICS\My Documents\giac\camo
test\Remote_Access_Policy_camod.doc

Key Name: HKEY_CURRENT_USER\Software\Camouflage\OutputFolder

Class Name: <NO CLASS>

Last Write Time: 3/1/2005 - 10:48 PM

Value 0

Name: 0
Type: REG_SZ
Data: C:\Documents and Settings\WINFORENSICS\My Documents\giac\camo

© SANS Institute 2005, Author retains full rights.

Appendix D – Relevant Statutes

From Federal Penal Code

<http://www.usdoj.gov/criminal/cybercrime/18usc1832.htm>

18 U.S.C. 1832.

Theft of Trade Secrets

§ 1832. Theft of Trade Secrets

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

- (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
- (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
- (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
- (4) attempts to commit any offense described in paragraphs (1) through (3); or
- (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than \$5,000,000.

From Texas Penal Code

<http://www.capitol.state.tx.us/statutes/docs/PE/content/htm/pe.007.00.000031.00.htm#31.05.00>

§ 31.05. THEFT OF TRADE SECRETS

(a) For purposes of this section:

(1) "Article" means any object, material, device, or substance or any copy thereof, including a writing, recording, drawing, sample, specimen, prototype, model, photograph, microorganism, blueprint, or map.

(2) "Copy" means a facsimile, replica, photograph, or other reproduction of an article or a note, drawing, or sketch made of or from an article.

(3) "Representing" means describing, depicting, containing, constituting, reflecting, or recording.

(4) "Trade secret" means the whole or any part of any scientific or technical information, design, process, procedure, formula, or improvement that has value and that the owner has taken measures to prevent from becoming available to persons other than those selected by the owner to have access for limited purposes.

(b) A person commits an offense if, without the owner's effective consent, he knowingly:

- (1) steals a trade secret;
- (2) makes a copy of an article representing a trade secret; or
- (3) communicates or transmits a trade secret.

(c) An offense under this section is a felony of the third degree.

Acts 1973, 63rd Leg., p. 883, ch. 399, § 1, eff. Jan. 1, 1974.
Amended by Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.

© SANS Institute 2005

Appendix E – PestPatrol Evaluation License

This license applies to the evaluation version of the PestPatrol Home User Edition. If you do not have an evaluation version of PestPatrol Home User Edition, see the section above titled PestPatrol Standard License.

PESTPATROL LICENSE
EVALUATION VERSION
PESTPATROL, INC.

By installing or using PestPatrol, you agree to all of the terms of this License. If you do not agree to any of the terms of this License, then do not install or use PestPatrol.

This is not free software. Subject to the terms below, you are hereby licensed by PestPatrol, Inc. to use this software for evaluation purposes without charge for a period of one year. If you use this software after the one year evaluation period a registration fee equal to the currently applicable manufacturer's suggested retail price is required. Payments must be in US dollars drawn on a US bank, and should be sent to PestPatrol, Inc., 453 Lincoln Street, Carlisle, PA 17013, USA. See the PestPatrol web site at www.pestpatrol.com for information about online ordering and quantity discounts.

Unregistered use of PestPatrol after the one year evaluation period is in violation of U.S. and international copyright laws.

You may, without making any payment to PestPatrol, Inc:

give exact copies of this evaluation version of PestPatrol personally to anyone, except for the purpose of extending their one year evaluation period; distribute exact copies of this evaluation version of PestPatrol, if done exclusively through electronic channels; and make as many exact copies of this evaluation version of PestPatrol as you wish, for purposes of distribution as described in (a) and (b) above.

YOU ARE SPECIFICALLY PROHIBITED FROM CHARGING, OR REQUESTING DONATIONS, FOR ANY COPIES, HOWEVER MADE, AND FROM DISTRIBUTING SUCH COPIES WITH OTHER PRODUCTS OF ANY KIND, COMMERCIAL OR OTHERWISE, WITHOUT PRIOR WRITTEN PERMISSION FROM PESTPATROL, INC. PESTPATROL, INC. RESERVES THE RIGHT TO REVOKE THE ABOVE DISTRIBUTION RIGHTS AT ANY TIME, FOR ANY OR NO REASON.

THIS SOFTWARE, AND ALL ACCOMPANYING FILES, DATA AND MATERIALS, ARE DISTRIBUTED "AS IS" AND WITH NO WARRANTIES OF

ANY KIND, WHETHER EXPRESS OR IMPLIED. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THE AGREEMENT. IN NO EVENT SHALL PESTPATROL, INC., OR ITS PRINCIPALS, SHAREHOLDERS, OFFICERS, EMPLOYEES, AFFILIATES, CONTRACTORS, SUBSIDIARIES, OR PARENT ORGANIZATIONS, BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES WHATSOEVER RELATING TO THE USE OF PESTPATROL, OR YOUR RELATIONSHIP WITH PESTPATROL, INC.

IN ADDITION, IN NO EVENT DOES PESTPATROL, INC. AUTHORIZE YOU TO USE PESTPATROL IN APPLICATIONS OR SYSTEMS WHERE PESTPATROL'S FAILURE TO PERFORM CAN REASONABLY BE EXPECTED TO RESULT IN A SIGNIFICANT PHYSICAL INJURY, OR IN LOSS OF LIFE. ANY SUCH USE BY YOU IS ENTIRELY AT YOUR OWN RISK, AND YOU AGREE TO HOLD PESTPATROL, INC. HARMLESS FROM ANY CLAIMS OR LOSSES RELATING TO SUCH UNAUTHORIZED USE.

This Agreement is the complete statement of the Agreement between the parties on the subject matter, and merges and supersedes all other or prior understandings, purchase orders, agreements and arrangements. This Agreement shall be governed by the laws of the State of Pennsylvania. Exclusive jurisdiction and venue for all matters relating to this Agreement shall be in courts and for a located in the State of Pennsylvania, and you consent to such jurisdiction and venue.

All rights of any kind in PestPatrol which are not expressly granted in this License are entirely and exclusively reserved to and by PestPatrol, Inc. You may not rent, lease, modify, translate, reverse engineer, decompile, disassemble or create derivative works based on PestPatrol. You may not make access to PestPatrol available to others in connection with a service bureau, application service provider, or similar business, or use PestPatrol in a business to provide file compression, decompression, or conversion services to others. There are no third party beneficiaries of any promises, obligations or representations made by PP herein.

###

Appendix F – Listing of Pest Detection Tools CD-ROM

```
/mnt/cdrom:
dr-xr-xr-x  1 root    root          2048 Oct 10 19:31 pestpatrol files
dr-xr-xr-x  1 root    root          2048 Oct 10 19:43 Program Files

/mnt/cdrom/pestpatrol files:
-r-xr-xr-x  1 root    root          36864 Oct 10 19:28 bait.exe
-r-xr-xr-x  1 root    root          40960 Oct 10 19:28 kpbaithook.dll
-r-xr-xr-x  1 root    root         6264805 Oct 10 19:31 setuppestpatroleval.exe

/mnt/cdrom/Program Files:
dr-xr-xr-x  1 root    root          2048 Oct 10 19:34 PestPatrol

/mnt/cdrom/Program Files/PestPatrol:
-r-xr-xr-x  1 root    root           3584 Nov 14 2002 bmstrstr.dll
-r-xr-xr-x  1 root    root           7450 Dec 10 2002 CookieCrunch.wav
-r-xr-xr-x  1 root    root          69632 Apr  2 2004 CookiePatrol.exe
-r-xr-xr-x  1 root    root            74 Sep 17 2002 GettingStarted.url
-r-xr-xr-x  1 root    root          231448 May 15 2003 Help.chm
dr-xr-xr-x  1 root    root           2048 Oct 10 19:35 logs
-r-xr-xr-x  1 root    root         836096 Jun  7 2004 PestPatrolCL.exe
-r-xr-xr-x  1 root    root        1248256 Jun  7 2004 PestPatrol.exe
-r-xr-xr-x  1 root    root           924 May 12 2003 PestPatrol.ini
-r-xr-xr-x  1 root    root           98 Oct 10 19:34
PestPatrolRegistration.ini
-r-xr-xr-x  1 root    root         907776 Oct  6 08:59 PPClean.exe
-r-xr-xr-x  1 root    root         53248 Apr  2 2004 PPControl.exe
-r-xr-xr-x  1 root    root         53248 Mar 26 2003 PPCPLog.exe
-r-xr-xr-x  1 root    root        212992 Jan 26 2003 PPEngine.dll
-r-xr-xr-x  1 root    root       1830538 Oct  6 09:01 PPFile.dat
-r-xr-xr-x  1 root    root         710678 Oct  6 09:00 PPInfo.dat
-r-xr-xr-x  1 root    root        148480 Apr  2 2004 PPMemCheck.exe
-r-xr-xr-x  1 root    root         61440 Jan 26 2003 PPServer.dll
-r-xr-xr-x  1 root    root          3292 Oct  6 08:59 PPSRIndex.dat
-r-xr-xr-x  1 root    root        274944 May  3 2004 PPUdater.exe
-r-xr-xr-x  1 root    root       285369 Oct  6 09:00 Spyware.dat
dr-xr-xr-x  1 root    root           2048 Oct 10 19:34 tmp
-r-xr-xr-x  1 root    root        247296 Apr  2 2004 UnPP.exe
-r-xr-xr-x  1 root    root        102400 Dec 10 2002 unzip32.dll

/mnt/cdrom/Program Files/PestPatrol/logs:
-r-xr-xr-x  1 root    root          5931 Oct 10 19:35 install.log
-r-xr-xr-x  1 root    root          1257 Oct 10 19:34 PPUdater.log

/mnt/cdrom/Program Files/PestPatrol/tmp:
```

Appendix G – PestPatrol System Modifications

Changes on \\WINFORENSICS
(All Changes -- No Severity Filters)

Changes from Snapshot Details for Files

Name

```
C:\WINNT\system32
  Folder Last Modified Date  1/25/2005 12:30:25 AM 1/25/2005 12:28:21 AM
C:\WINNT\system32\config\software
  File Last Modified Date    1/25/2005 12:31:12 AM 1/25/2005 12:17:04 AM
C:\WINNT\system32\config\software.LOG
  File Last Modified Date    1/25/2005 12:31:12 AM 1/25/2005 12:17:04 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Files
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Services
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\System
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Users
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes
  Folder Last Modified Date  1/25/2005 12:30:11 AM 1/25/2005 12:28:19 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes\changes.bl
  File Size                  144                140
  File Last Modified Date    1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Volumes\changes.log
  File Last Modified Date    1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Users\changes.bl
  File Size                  144                140
  File Last Modified Date    1/25/2005 12:34:20 AM 1/25/2005 12:30:12 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Users\changes.log
  File Last Modified Date    1/25/2005 12:34:20 AM 1/25/2005 12:30:12 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\System\changes.bl
  File Size                  202                198
  File Last Modified Date    1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\System\changes.log
  File Last Modified Date    1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares\changes.bl
  File Size                  162                157
  File Last Modified Date    1/25/2005 12:34:19 AM 1/25/2005 12:30:12 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Shares\changes.log
  File Last Modified Date    1/25/2005 12:34:19 AM 1/25/2005 12:30:12 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Services\changes.bl
  File Size                  147                146
  File Last Modified Date    1/25/2005 12:34:19 AM 1/25/2005 12:30:12 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Services\changes.log
  File Last Modified Date    1/25/2005 12:34:19 AM 1/25/2005 12:30:12 AM
```

```

C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler\changes.bl
  File Size      145      141
  File Last Modified Date 1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Scheduler\changes.log
  File Last Modified Date 1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights\changes.bl
  File Size      144      140
  File Last Modified Date 1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Rights\changes.log
  File Last Modified Date 1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\baseline.bl
  File Size      1377814      0
  File Last Modified Date 1/25/2005 12:30:15 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\baseline.log
  File Size      182      42
  File Last Modified Date 1/25/2005 12:30:15 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\changes.bl
  File Size      0      128
  File Last Modified Date 1/25/2005 12:34:19 AM 1/25/2005 12:29:48 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Registry\changes.log
  File Size      42      173
  File Last Modified Date 1/25/2005 12:34:19 AM 1/25/2005 12:29:48 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups\changes.bl
  File Size      142      138
  File Last Modified Date 1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Groups\changes.log
  File Last Modified Date 1/25/2005 12:34:19 AM 1/25/2005 12:30:11 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\baseline.bl
  File Size      88214      0
  File Last Modified Date 1/25/2005 12:30:13 AM 1/25/2005 12:30:12 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\baseline.log
  File Size      292      156
  File Last Modified Date 1/25/2005 12:30:13 AM 1/25/2005 12:30:12 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\changes.bl
  File Size      0      911
  File Last Modified Date 1/25/2005 12:34:20 AM 1/25/2005 12:29:46 AM
C:\Program Files\Winalysis\Archive\WINFORENSICS\Files\changes.log
  File Size      156      288
  File Last Modified Date 1/25/2005 12:34:20 AM 1/25/2005 12:29:46 AM
C:\Documents and Settings\Administrator\NTUSER.DAT
  File Last Modified Date 1/25/2005 12:30:58 AM 1/25/2005 12:30:03 AM
C:\Documents and Settings\Administrator\ntuser.dat.LOG
  File Last Modified Date 1/25/2005 12:30:58 AM 1/25/2005 12:30:03 AM
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
  File Last Modified Date 1/25/2005 12:30:54 AM 1/25/2005 12:16:36 AM
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
  File Last Modified Date 1/25/2005 12:30:54 AM 1/25/2005 12:16:36 AM
C:\Documents and Settings\Administrator\Cookies\index.dat
  File Last Modified Date 1/25/2005 12:30:54 AM 1/25/2005 12:16:36 AM

```

Changes from Snapshot Details for Registry

Snapshot:

Tested:

Name

```

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  Number of Values HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PPMemCheck
  New Value
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PestPatrol Control Center
  New Value D:\PROGRA~8\PESTPA~5\ PControl.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\CookiePatrol
  New Value D:\PROGRA~8\PESTPA~5\ ookiePatrol.exe
HKLM\SOFTWARE\Microsoft\Cryptography\RNG

```

```
Key Last Modified Date HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed
Value Changed
HKLM\SOFTWARE\Classes\.key
Key Last Modified Date
```

(Note ***: The report has the first two entries skewed and must have been a result of Winalysis software glitch as it was repeatable. I verified how the lines should have read by clicking on the Info symbol in the Changes report and manually modified to appear correct in this document.)

© SANS Institute 2005, Author retains full rights.

Appendix H – PestPatrol IKS Output Log

Scan of 1/25/2005 1:39:39 AM
Pests found: 9
Area scanned: C:\
User Name: Administrator
MAC Address: XX-XX-XX-XX-XX-XX (note: author masked for privacy)
Computer Name: WINFORENSICS
Volume Name:
File System Name: NTFS
Volume Serial No: 2089221924
Windows Version: Windows 2000
Product Edition: Evaluation
PestPatrol version: 6/7/2004 4.4.3.24
PPServer.dll version: 1/26/2003
PPClean version: 10/6/2004 4.5.4.14
PPfile.dat version: 10/6/2004
PPInfo.dat version: 10/6/2004
Spyware.dat version: 10/6/2004
PPMemCheck version: 4/2/2004
PestPatrolCL version: 6/7/2004 4.4.3.19
PPUpdater version: 5/3/2004 4.4.3.36

Pest: Invisible Stealth Keylogger?
Pest Info: Category: Adware Background Info: [Click here](#)
File Info: In File: C:\Program Files\iks\readme.txt Date: 1/23/2003 4:30:46 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice:
Delete or quarantine
Action: Ignored

~~~

Pest: Invisible Stealth Keylogger?  
Pest Info: Category: Adware Background Info: [Click here](#)  
File Info: In File: C:\Program Files\iks\order.txt Date: 1/23/2003 4:28:14 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice:  
Delete or quarantine  
Action: Ignored

~~~

Pest: Invisible Stealth Keylogger?
Pest Info: Category: Adware Background Info: [Click here](#)
File Info: In File: C:\Program Files\iks\license.txt Date: 1/23/2003 4:31:24 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice:
Delete or quarantine
Action: Ignored

~~~

Pest: Invisible Stealth Keylogger?  
Pest Info: Category: Adware Background Info: [Click here](#)  
File Info: In File: C:\Program Files\iks\datview.exe Date: 1/23/2003 5:31:36 PM  
Company Name: Amecisco File Description: Datview Translator for IKS 2000/XP File  
Version: 2, 1, 0, 1 Internal Name: datview Legal Copyright: Copyright (C) Amecisco  
Inc. 1998 - 2003 Original Filename: datview.exe Product Name: Datview - Binary Log  
Translator for IKS Product Version: 2, 1, 0, 1  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this  
file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: Invisible Stealth Keylogger Directory
Pest Info: Category: Adware Background Info: [Click here](#)
File Info: In Directory: C:\Program Files\iks Date: 1/25/2005 1:11:52 AM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice:
Delete when empty
Action: Ignored

~~~~~  
Pest: Invisible Stealth Keylogger  
Pest Info: Category: Adware Background Info: [Click here](#)  
File Info: In File: C:\WINNT\system32\drivers\iks.sys Date: 5/25/2001 5:51:54 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this  
file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~~~  
Pest: Invisible Stealth Keylogger
Pest Info: Category: Adware Background Info: [Click here](#)
File Info: In File: C:\WINNT\iks.dat Date: 1/25/2005 1:26:28 AM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice:
Delete or quarantine
Action: Ignored

~~~~~  
Pest: Invisible Stealth Keylogger  
Pest Info: Category: Adware Background Info: [Click here](#)  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\system\controlset002\services\iks  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice:  
Delete or ignore  
Action: Ignored

~~~~~  
Pest: Invisible Stealth Keylogger
Pest Info: Category: Adware Background Info: [Click here](#)
File Info: In Registry: HKEY_LOCAL_MACHINE\system\controlset001\services\iks
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice:
Delete or ignore
Action: Ignored

© SANS Institute 2005, Author retains full rights

Appendix I – Unknown System PestPatrol Output

Scan of 3/3/2005 9:51:17 PM
Pests found: 663
Area scanned: C:\
User Name: Raven
MAC Address: XX-XX-XX-XX-XX-XX
Computer Name: KIM
Volume Name:
File System Name: NTFS
Volume Serial No: 1084409879
Windows Version: Windows XP
Product Edition: Evaluation
PestPatrol version: 6/7/2004 4.4.3.24
PPServer.dll version: 1/26/2003
PPClean version: 10/6/2004 4.5.4.14
PPfile.dat version: 10/6/2004
PPInfo.dat version: 10/6/2004
Spyware.dat version: 10/6/2004
PPMemCheck version: 4/2/2004
PestPatrolCL version: 6/7/2004 4.4.3.19
PPUpdater version: 5/3/2004 4.4.3.36

Pest: Unknown Trojan

Pest Info: Category: Trojan Release Date: 8/15/2004 0:00:00 Background Info: Click here
File Info: In File: C:\WINDOWS\system32\SIntf16.dll PVT: -1649196341 MD5:
c72263a0b16b36e0b4bd2fd442fffd54 Date: 9/25/2004 11:05:00 AM File Analysis: Look up with MD5
(recommended) or PVT.
Certainty: Confirmed Threatens: Confidentiality, Integrity, Availability, Productivity,
Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: 2nd Thought

Pest Info: Category: Adware Author: [CPM Media, Ltd.] Release Date: 8/6/2004 0:00:00  
Background Info: Click here  
File Info: In File: C:\WINDOWS\system32\msxml3.inf PVT: -1369509357 MD5:  
69908ed7545d7458ea097e023c193acc Date: 6/19/2002 5:39:42 PM File Analysis: Look up with MD5  
(recommended) or PVT.  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be  
executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: Twain-Tech

Pest Info: Category: Browser Helper Object Release Date: 8/14/2004 0:00:00 Background Info:
Click here
File Info: In File: C:\WINDOWS>LastGood\twaintec.dll PVT: -2010546968 MD5:
21b05102febcd16d9c41b415223977c2 Date: 2/11/2004 5:30:52 PM Company Name: Twain Tech File
Description: www.twain-tech.com File Version: 0, 1, 4, 19 Internal Name: Twaintec Legal
Copyright: Copyright © 2003 Original Filename: Twaintec.dll Product Name: Twaintec Product
Version: 0, 1, 4, 19 File Analysis: Look up with MD5 (recommended) or PVT.
Certainty: Confirmed Threatens: Liability Risk: Moderate - this file can be executed!
Advice: Delete or quarantine
Action: Ignored

~~~

Pest: TrojanDownloader.Win32.Agent.ae

Pest Info: Category: Downloader Author: [callinghome.biz] Release Date: 8/16/2004 0:00:00  
Background Info: Click here  
File Info: In File: C:\WINDOWS>LastGood\System32\polall1m.exe PVT: -1768750561 MD5:  
fbed7b3d2e7be0a872e1e6a68beadef8 Date: 7/27/2004 2:44:00 PM File Analysis: Look up with MD5  
(recommended) or PVT.  
Certainty: Confirmed Threatens: Liability Risk: Moderate - this file can be executed!  
Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: Twain-Tech
Pest Info: Category: Browser Helper Object Release Date: 8/14/2004 0:00:00 Background Info: Click here
File Info: In File: C:\WINDOWS\LastGood\preInsTT.exe PVT: 718425449 MD5: e2122b80108e0bf53537e64681fc3a72 Date: 2/11/2004 5:30:50 PM File Analysis: Look up with MD5 (recommended) or PVT.
Certainty: Confirmed Threatens: Liability Risk: Moderate - this file can be executed!
Advice: Delete or quarantine
Action: Ignored

~~~

Pest: DyFuCA.Internet Optimizer  
Pest Info: Category: Browser Helper Object Author: [Avenue Media] Release Date: 8/15/2004 0:00:00 Background Info: Click here  
File Info: In File: C:\Temp\msbbhook.dll PVT: -1847281533 MD5: 7a14373df7aabdb7137a5f5d5e179bc5 Date: 9/20/2004 5:56:02 PM File Analysis: Look up with MD5 (recommended) or PVT.  
Certainty: Confirmed Threatens: Liability Risk: Moderate - this file can be executed!  
Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: Advware.BetterInternet
Pest Info: Category: Adware Release Date: 7/21/2004 0:00:00 Background Info: Click here
File Info: In File: C:\Temp\lc.exe PVT: -1028881954 MD5: 00e6c792056805591cf4ef9c385eead9 Date: 9/20/2004 5:55:56 PM Company Name: BetterInternet, Inc. File Description: www.abetterinternet.com - Utility for downloading files and upgrading software. File Version: 1, 0, 0, 12 Internal Name: Install Utility Legal Copyright: BetterInternet, Inc. © 2004 File Analysis: Look up with MD5 (recommended) or PVT.
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: ClientSniffer  
Pest Info: Category: Spyware Author: [Netscape Communications] Release Date: 5/20/2004 0:00:00 Background Info: Click here  
File Info: In File: C:\Documents and Settings\Raven\Local Settings\Temporary Internet Files\Content.IE5\CXIZSP21\vb\_2\_0[1].js PVT: -298229441 MD5: 07738421903d996845f76964ac99b825 Date: 1/25/2005 4:28:56 PM File Analysis: Look up with MD5 (recommended) or PVT.  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: RedV
Pest Info: Category: Adware Author: [RedV] Release Date: 7/12/2004 0:00:00 Background Info: Click here
File Info: In File: C:\Documents and Settings\Raven\Local Settings\Temporary Internet Files\Content.IE5\2N474BAR\clientSniffer_2_0[1].js PVT: 867714113 MD5: 12aefe430c3747c2203f5795c8f89664 Date: 1/25/2005 4:28:58 PM File Analysis: Look up with MD5 (recommended) or PVT.
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: P2P Networking  
Pest Info: Category: Adware Author: [Joltid Ltd.] Release Date: 8/17/2004 0:00:00 Background Info: Click here  
File Info: In File: C:\Documents and Settings\Raven\Local Settings\Temp\p2psetup.exe PVT: -199498276 MD5: b86a437a78799b388238cebb62e86262 Date: 8/9/2003 2:01:18 PM Company Name: Joltid Ltd. File Description: P2P Networking File Version: 1, 23, 10, 40 Internal Name: P2P Networking Legal Copyright: Copyright © 2001 - 2003 Joltid Ltd. All Rights Reserved. Original Filename: P2P Networking.exe Product Name: P2P Networking Product Version: 1, 23, 10, 40 File Analysis: Look up with MD5 (recommended) or PVT.  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: Advware.BetterInternet
Pest Info: Category: Adware Release Date: 7/21/2004 0:00:00 Background Info: Click here
File Info: In File: C:\Documents and Settings\Raven\Local Settings\Temp\DrTemp\speer_v12.exe

PVT: -1028881954 MD5: a784f2cd5682e3eb2c6cd6d118937b3f Date: 1/22/2005 7:03:48 PM Company Name: BetterInternet, Inc. File Description: www.abetterinternet.com - Utility for downloading files and upgrading software. File Version: 1, 0, 0, 12 Internal Name: Install Utility Legal Copyright: BetterInternet, Inc. © 2004 File Analysis: Look up with MD5 (recommended) or PVT. Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine Action: Ignored

~~~

Pest: Powerscan Directory  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Directory: C:\Program Files\power scan Date: 1/26/2005 5:49:54 AM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty  
Action: Ignored

~~~

Pest: NetworkEssentials.SCBar Directory
Pest Info: Category: Adware Background Info: Click here
File Info: In Directory: C:\Documents and Settings\All Users\Start Menu\Programs\web search tools Date: 2/28/2005 4:25:30 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty
Action: Ignored

~~~

Pest: NetPal Directory  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Directory: C:\Documents and Settings\Raven\Favorites\netpal games Date: 1/2/2005 6:13:38 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty  
Action: Ignored

~~~

Pest: Morpheus?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\streamcast\morpheus\mldonkey\mldonkey\mlnet_strings.en Date: 10/30/2004 3:58:20 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: Morpheus Directory  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Directory: C:\Program Files\streamcast\morpheus\mldonkey\mldonkey Date: 7/27/2004 7:32:36 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty  
Action: Ignored

~~~

Pest: Morpheus Directory
Pest Info: Category: Adware Background Info: Click here
File Info: In Directory: C:\Program Files\streamcast\morpheus\mldonkey Date: 1/22/2005 10:11:10 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty
Action: Ignored

~~~

Pest: Morpheus Directory  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Directory: C:\Documents and Settings\Raven\start menu\programs\morpheus Date: 1/22/2005 10:11:10 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty  
Action: Ignored

~~~

Pest: Lycos Sidesearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\lycos\IEagent\FNuninstaller.EXE Date: 11/22/2004 6:04:58 PM

Company Name: Clear Search File Description: FNuninstaller File Version: 1, 0, 0, 2 Internal
Name: FNuninstaller Legal Copyright: Copyright © 2004 Original Filename: FNuninstaller.exe
Product Name: FNuninstaller Product Version: 1, 0, 0, 2
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be
executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\versions.dat Date: 9/12/2003 8:59:32 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or  
quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\zoo.xmd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\zip.xmd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or  
quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\z.xmd Date: 4/3/2002 12:00:10 AM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\xishield.xmd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or  
quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\viza.xmd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\vedata.cvd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or  
quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\ve.xmd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\ve.ivd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or

quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\ve.cvd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\uudecode.xmd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\unpack.xmd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\unpack.cvd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\tnef.xmd Date: 7/15/2002 1:48:44 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\thebat.xmd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\td0.xmd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\tar.xmd Date: 8/14/2002 1:41:24 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\swf.xmd Date: 8/5/2002 6:31:26 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\sfx.xmd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\sdx.xmd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\sdx.ivd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\sdx.cvd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\rup.xmd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\rup.cvd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\rtf.xmd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\rpm.xmd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\rar.xmd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\pst.xmd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\pdf.xml Date: 9/4/2003 8:02:12 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\objd.xml Date: 4/3/2002 12:00:10 AM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\nelf.xml Date: 9/4/2003 8:02:12 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\nelf.cvd Date: 9/4/2003 8:02:12 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\na.xml Date: 9/4/2003 8:02:12 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\mso.xml Date: 9/4/2003 8:02:12 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\mime.xml Date: 9/4/2003 8:02:12 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\mdx_xf.cvd Date: 9/4/2003 8:02:12 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\mdx\_x95.cvd Date: 9/4/2003 8:02:12 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: C:\Program Files\kazaa\plugins\mdx_w95.cvd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\mdx\_97.ivd Date: 9/4/2003 8:02:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\mdx_97.cvd Date: 9/4/2003 8:02:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\mdx.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\mbx.xmd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\mbox.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\lnk.xmd Date: 4/3/2002 12:00:10 AM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\lha.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\java.xmd Date: 8/5/2002 6:36:50 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\iso.xmd Date: 6/24/2002 7:04:38 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~~  
Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\instyler.xmd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~~  
Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\inno.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~~  
Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\imp.xmd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~~  
Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\html.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~~  
Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\hqx.xmd Date: 4/3/2002 12:00:10 AM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~~  
Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\hpe.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~~  
Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\hpe.cvd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~~  
Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\hlp.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~~  
Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\ha.xmd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~~  
Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\gzip.xmd Date: 4/3/2002 12:00:10 AM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\emalware.xml Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\emalware.ivd Date: 9/12/2003 1:53:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\emalware.cvd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\docfile.xml Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\dbx.xml Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\cran.xml Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\cran.cvd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\cpio.xml Date: 4/3/2002 12:00:10 AM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?

Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\chm.xml Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\ceva\_vfs.cvd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\cevakrnl.xmd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\cevakrnl.rvd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\cevakrnl.iyd Date: 9/12/2003 1:53:00 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\cevakrnl.cvd Date: 9/20/2002 4:07:22 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\cab.xmd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\bzip2.xmd Date: 9/19/2002 5:18:22 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\bach.xmd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\arj.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins\arc.xmd Date: 9/4/2003 8:02:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\plugins\ace.xmd Date: 9/4/2003 8:02:10 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA Directory
Pest Info: Category: Adware Background Info: Click here
File Info: In Directory: C:\Program Files\kazaa\plugins Date: 9/12/2003 1:53:12 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\My Shared Folder\[Real McCoy] - Another Night (Club Mix).mp3 Date: 9/7/2003 12:36:30 AM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\Db\tss3.cab Date: 9/4/2003 7:49:10 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\Db\tsi030904.cab Date: 9/12/2003 1:54:36 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\Db\tsi030902.cab Date: 9/10/2003 6:00:56 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\Db\tsi030828.cab Date: 9/5/2003 3:11:22 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\Db\tsi030822.cab Date: 8/29/2003 3:55:54 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\Db\tsi030819.cab Date: 8/26/2003 5:57:20 AM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\Db\tsi030813.cab Date: 8/20/2003 2:56:30 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\Db\tsi030808.cab Date: 8/9/2003 2:04:24 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\Db\str030826.cab Date: 9/5/2003 5:21:50 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\Db\str030810.cab Date: 8/20/2003 4:56:56 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\Db\str030702.cab Date: 8/9/2003 4:05:12 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\Db\np.tmp Date: 9/13/2003 7:38:12 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~

Pest: KaZaA?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\Db\data256.dbb Date: 9/16/2003 9:05:36 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~~

Pest: KaZaA?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\kazaa\Db\data1024.dbb Date: 9/16/2003 9:05:36 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~~

Pest: KaZaA Directory
Pest Info: Category: Adware Background Info: Click here
File Info: In Directory: C:\Program Files\kazaa\Db Date: 9/16/2003 9:05:50 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty
Action: Ignored

~~~~

Pest: KaZaA Directory  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Directory: C:\Program Files\kazaa Date: 9/16/2003 9:05:50 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when

empty  
Action: Ignored

~~~

Pest: ISTbar.XXXToolbar Directory
Pest Info: Category: Adware Background Info: Click here
File Info: In Directory: C:\Program Files\istsvc Date: 2/28/2005 5:03:26 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: High! This file is now running! Advice: Delete when empty
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\FNuninstaller.EXE Date: 11/22/2004 6:04:58 PM  
Company Name: Clear Search File Description: FNuninstaller File Version: 1, 0, 0, 2 Internal Name: FNuninstaller Legal Copyright: Copyright © 2004 Original Filename: FNuninstaller.exe  
Product Name: FNuninstaller Product Version: 1, 0, 0, 2  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\CSTVINST.DLL Date: 10/5/2004 12:12:54 PM Company Name: ClearSearch File Description: TotalVelocity File Version: 4, 0, 0, 0 Internal Name: TotalVelocity Legal Copyright: Copyright © 2004 Original Filename: TotalVelocity.dll Product Name: ClearSearch TotalVelocity Product Version: 4, 0, 0, 0
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\CSTMINST.DLL Date: 10/5/2004 12:13:02 PM Company Name: Clear Search File Description: csTMinst File Version: 4, 0, 0, 0 Internal Name: csTMinst Legal Copyright: Copyright © 2004 Original Filename: csTMinst.dll Product Name: csTMinst Product Version: 4, 0, 0, 0  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\CSSSINST.DLL Date: 4/5/2004 3:24:10 PM Company Name: Clear Search File Description: CSss File Version: 1, 0, 0, 4 Internal Name: CSss Legal Copyright: Copyright © 2003, 2004 Original Filename: CSss.dll Product Name: CSss Product Version: 1, 0, 0, 4
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\CSLDUPDATER.DLL Date: 10/5/2004 12:12:46 PM Company Name: ClearSearch File Description: LoaderUpdater File Version: 1, 7, 0, 2 Internal Name: LoaderUpdater Legal Copyright: Copyright © 2004 Original Filename: LoaderUpdater.dll Product Name: ClearSearch LoaderUpdater Product Version: 1, 7, 0, 2  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csie_usb_sbhour.dat Date: 10/6/2004 2:55:40 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\csie\_usb\_sbdays.dat Date: 10/6/2004 2:55:40 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored  
~~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csie_ss_idomainsd.dat Date: 9/17/2004 5:15:16 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored
~~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\csie\_srchrules.dat Date: 5/19/2004 3:41:50 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored  
~~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csie_rules.dat Date: 6/8/2004 9:06:16 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored
~~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\csie\_ron\_sbdays.dat Date: 10/6/2004 2:55:42 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored  
~~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csie_ron_sbdays.dat Date: 10/6/2004 2:55:42 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored
~~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\csie\_patterns.dat Date: 6/8/2004 9:06:16 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored  
~~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csie_idomainsd.dat Date: 7/1/2004 3:40:22 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored
~~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\csie\_edomains.dat Date: 5/21/2004 9:33:06 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored  
~~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\CSIEINST.DLL Date: 10/5/2004 12:12:42 PM Company Name: ClearSearch File Description: CSieINST File Version: 1, 0, 69, 5 Internal Name: CSieINST

Legal Copyright: Copyright © 2004 Original Filename: CSieINST.dll Product Name: ClearSearch
CSieINST Product Version: 1, 0, 69, 5
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be
executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\CSBIINST.DLL Date: 4/5/2004 3:24:12 PM Company  
Name: Clear Search File Description: CSbi File Version: 1, 0, 0, 3 Internal Name: CSbi Legal  
Copyright: Copyright © 2003, 2004 Original Filename: CSbi.dll Product Name: CSbi Product  
Version: 1, 0, 0, 3  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be  
executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csbb_usb_shour.dat Date: 11/24/2004 10:05:14 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\csbb\_usb\_sday.dat Date: 11/24/2004 10:05:14 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or  
quarantine  
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csbb_usb_rules.dat Date: 10/6/2004 3:00:42 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\csbb\_usb\_patterns.bin Date: 10/22/2004 11:51:50 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or  
quarantine  
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csbb_usb_campaigns.bin Date: 10/22/2004 11:51:50
PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\progra~1\lycos\ieagent\csbb\_tsb\_rules.dat Date: 10/6/2004 3:00:42 PM  
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or  
quarantine  
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csbb_tsb_patterns.bin Date: 10/6/2004 3:00:42 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here  
 File Info: In File: c:\progra~1\lycos\ieagent\csbb\_tsb\_edomains.bin Date: 10/6/2004 3:00:44 PM  
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
 Action: Ignored  
 ~~~

Pest: IGetNet.ClearSearch?
 Pest Info: Category: Adware Background Info: Click here
 File Info: In File: c:\progra~1\lycos\ieagent\csbb_tsb_campaigns.bin Date: 10/6/2004 3:00:44 PM
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
 Action: Ignored
 ~~~

Pest: IGetNet.ClearSearch?  
 Pest Info: Category: Adware Background Info: Click here  
 File Info: In File: c:\progra~1\lycos\ieagent\csbb\_ss\_rules.dat Date: 10/22/2004 11:51:50 PM  
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
 Action: Ignored  
 ~~~

Pest: IGetNet.ClearSearch?
 Pest Info: Category: Adware Background Info: Click here
 File Info: In File: c:\progra~1\lycos\ieagent\csbb_ss_idomains.bin Date: 10/6/2004 3:00:44 PM
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
 Action: Ignored
 ~~~

Pest: IGetNet.ClearSearch?  
 Pest Info: Category: Adware Background Info: Click here  
 File Info: In File: c:\progra~1\lycos\ieagent\csbb\_ss\_edomains.bin Date: 10/6/2004 3:00:44 PM  
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
 Action: Ignored  
 ~~~

Pest: IGetNet.ClearSearch?
 Pest Info: Category: Adware Background Info: Click here
 File Info: In File: c:\progra~1\lycos\ieagent\csbb_ron_shour.dat Date: 11/24/2004 8:23:28 PM
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
 Action: Ignored
 ~~~

Pest: IGetNet.ClearSearch?  
 Pest Info: Category: Adware Background Info: Click here  
 File Info: In File: c:\progra~1\lycos\ieagent\csbb\_ron\_sday.dat Date: 11/24/2004 8:23:28 PM  
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
 Action: Ignored  
 ~~~

Pest: IGetNet.ClearSearch?
 Pest Info: Category: Adware Background Info: Click here
 File Info: In File: c:\progra~1\lycos\ieagent\csbb_ron_rules.dat Date: 10/6/2004 3:00:44 PM
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
 Action: Ignored
 ~~~

Pest: IGetNet.ClearSearch?  
 Pest Info: Category: Adware Background Info: Click here  
 File Info: In File: c:\progra~1\lycos\ieagent\csbb\_ron\_campaigns.bin Date: 10/6/2004 3:00:44 PM  
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
 Action: Ignored  
 ~~~

Pest: IGetNet.ClearSearch?
 Pest Info: Category: Adware Background Info: Click here
 File Info: In File: c:\progra~1\lycos\ieagent\csbb_promos.bin Date: 11/8/2004 4:27:56 PM
 Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
 Action: Ignored

Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: c:\progra~1\lycos\ieagent\csbb\_mpu\_rules.dat Date: 10/6/2004 3:00:44 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: c:\progra~1\lycos\ieagent\csbb_mpu_mirrors.bin Date: 10/6/2004 3:00:44 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: c:\progra~1\lycos\ieagent\csbb\_dictionary.bin Date: 10/6/2004 3:00:42 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: c:\progra~1\lycos\ieagent\csbb_checks.dat Date: 11/23/2004 11:13:32 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: c:\progra~1\lycos\ieagent\csAOLLdr.exe Date: 11/22/2004 6:05:02 PM Company

Name: Clear Search File Description: CSAOLLDR File Version: 1, 0, 0, 1 Internal Name: CSAOLLDR

Legal Copyright: Copyright © 2004 Original Filename: CSAOLLDR.exe Product Name: CSAOLLDR

Product Version: 1, 0, 0, 1

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine

Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: c:\progra~1\lycos\ieagent\CSAOLINST.DLL Date: 10/5/2004 12:12:48 PM Company

Name: cntrc File Description: CTAOLINST File Version: 1, 25, 0, 1 Internal Name: CTAOLINST

Legal Copyright: Copyright © 2004 Original Filename: CTAOLINST.dll Product Name: CTAOLINST

Product Version: 1, 25, 0, 1

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine

Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: c:\progra~1\lycos\ieagent\control.dat Date: 10/5/2004 12:13:08 PM

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine

Action: Ignored

~~~

Pest: IGetNet.ClearSearch?

Pest Info: Category: Adware Background Info: Click here

File Info: In File: c:\progra~1\lycos\ieagent\A_ClearSearch.DLL Date: 11/22/2004 6:05:02 PM

Company Name: Clear Search, Inc. File Description: CS A Target File Version: 1, 24, 0, 1

Internal Name: A_ClearSearch Legal Copyright: Copyright © 2003-2004 Clear Search, Inc. Original

Filename: A_ClearSearch.dll Product Name: A_ClearSearch Product Version: 1, 24, 0, 1

Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine

Action: Ignored

~~~

Pest: IGetNet.ClearSearch Directory  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Directory: c:\progra~1\lycos\ieagent Date: 11/24/2004 10:10:02 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty  
Action: Ignored

~~~

Pest: DyFuCA.Internet Optimizer Directory
Pest Info: Category: Adware Background Info: Click here
File Info: In Directory: C:\Program Files\internet optimizer\update Date: 1/26/2005 2:48:22 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty
Action: Ignored

~~~

Pest: DyFuCA.Internet Optimizer Directory  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Directory: C:\Program Files\internet optimizer Date: 1/26/2005 2:48:22 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty  
Action: Ignored

~~~

Pest: ClearSearch?
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\WINDOWS\temp\clrsch\ss_revcol3_setup.exe Date: 4/5/2004 3:24:14 PM
Certainty: Suspected Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: ClearSearch Directory  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Directory: C:\WINDOWS\temp\clrsch Date: 4/5/2004 3:24:12 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty  
Action: Ignored

~~~

Pest: AdDestroyer Directory
Pest Info: Category: Adware Background Info: Click here
File Info: In Directory: C:\Documents and Settings\Raven\start menu\programs\AdDestroyer Date: 11/24/2004 10:10:56 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete when empty
Action: Ignored

~~~

Pest: Unknown Trojan  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Documents and Settings\Raven\local settings\temp\sintfnt.dll Date: 9/25/2004 11:07:58 AM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: Unknown Trojan
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Documents and Settings\Raven\local settings\temp\sintf32.dll Date: 9/25/2004 11:07:58 AM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: Unknown Trojan  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Documents and Settings\Raven\local settings\temp\glb1a2b.exe Date: 9/28/2001 4:00:28 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: Unknown Pest
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\WINDOWS\system32\msrev41.dll Date: 11/22/2004 6:05:26 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: Unknown Pest  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\WINDOWS\system32\msrev21.dll Date: 11/24/2004 10:10:08 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: TV Media Display
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Documents and Settings\Raven\application data\tvmknwr.dll Date: 11/15/2004 5:03:18 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: TrojanDownloader.Win32.IstBar.eo  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Documents and Settings\Raven\locals~1\temp\sidefind.exe Date: 1/26/2005 5:49:28 AM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: TrojanDownloader.Win32.Istbar.ce
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\istsvc\istsvc.exe Date: 2/28/2005 5:03:26 PM Company Name: File Description: istsvc File Version: 1, 0, 0, 2 Internal Name: istsvc Legal Copyright: Copyright © 2004 Original Filename: istsvc.exe Product Name: istsvc Product Version: 1, 0, 0, 2
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: High! This file is now running! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: TrojanDownloader.Win32.Intexp  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\WINDOWS\wupdt.exe Date: 2/28/2005 5:03:02 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: SAHAgent
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\WINDOWS\system32\sahhtml.exe Date: 6/27/2004 9:07:24 PM File Description: Popup MFC Application File Version: 2, 0, 0, 3 Internal Name: Popup Legal Copyright: Copyright (C) 2004 Original Filename: Popup.EXE Product Name: Popup Application Product Version: 2, 0, 0, 3
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: SAHAgent  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\WINDOWS\downloaded program files\sahuninstall\_.exe Date: 11/30/2004 3:36:08 PM Company Name: ShopAtHomeSelect File Description: SAHUninstall File Version: 2, 0, 0, 8 Internal Name: SAHUninstall Legal Copyright: Copyright © 2004 Original Filename: SAHUninstall.dll Product Name: SAHUninstall Product Version: 2, 0, 0, 8  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: SAHAgent
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\WINDOWS\downloaded program files\sahhtml_.exe Date: 6/27/2004 9:07:24 PM
File Description: Popup MFC Application File Version: 2, 0, 0, 3 Internal Name: Popup Legal
Copyright: Copyright (C) 2004 Original Filename: Popup.EXE Product Name: Popup Application
Product Version: 2, 0, 0, 3
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be
executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: SAHAgent  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\WINDOWS\downloaded program files\sahagent\_.exe Date: 11/30/2004 3:27:20  
PM Company Name: ShopAtHomeSelect File Description: SahAgent File Version: 2, 0, 0, 8  
Internal Name: SahAgent Legal Copyright: Copyright © 2004 Original Filename: SahAgent.exe  
Product Name: ShopAtHomeSelect SahAgent Product Version: 2, 0, 0, 8  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be  
executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: SAHAgent
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\WINDOWS\downloaded program files\lsp_.dll Date: 4/27/2004 6:06:14 AM
Company Name: ShopAtHomeSelect File Description: LSP File Version: 2, 0, 0, 1 Internal Name:
LSP Legal Copyright: Copyright © 2004 Original Filename: LSP.DLL Product Name:
ShopAtHomeSelect LSP Product Version: 2, 0, 0, 1
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be
executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: Powerscan  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: c:\program files\power scan\powerscan.exe Date: 1/26/2005 5:49:54 AM File  
Description: PowerScan v1.1 File Version: 1, 1, 0, 2 Internal Name: PowerScan v1.1 Legal  
Copyright: Copyright (C) 2004 Original Filename: Power-Scan.exe Product Name: PowerScan v1.1  
Product Version: 1, 1, 0, 2  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be  
executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: NCASE
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\WINDOWS\system32\fleok\msbb.exe Date: 4/28/2004 6:14:02 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be
executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: MX-Targeting  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Documents and Settings\Raven\locals~1\temp\dummy.htm Date: 2/28/2005  
5:02:28 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or  
quarantine  
Action: Ignored

~~~

Pest: MX-Targeting
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Documents and Settings\Raven\local settings\temp\dummy.htm Date:
2/28/2005 5:02:28 PM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or
quarantine
Action: Ignored

~~~

Pest: LinkGrabber 99  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Documents and Settings\All Users\Start Menu\Programs\startup\mywebsearch  
email plugin.lnk Date: 4/2/2004 3:08:34 PM

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: KaZaA
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\kazaa\plugins.htm Date: 9/9/2003 2:46:36 AM
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine
Action: Ignored

~~~

Pest: ISTbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\WINDOWS\alchem.ini Date: 11/14/2004 1:32:22 AM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\WINDOWS\systb.dll Date: 10/13/2004 9:06:00 PM File Description: wwho Module File Version: 1, 0, 8, 1 Internal Name: wwho Legal Copyright: Copyright 2004 Original Filename: wwho.DLL Product Name: wwho Module Product Version: 1, 0, 8, 1
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: IGetNet.ClearSearch  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Program Files\lycos\ieagent\csie.dll Date: 10/5/2004 12:12:20 PM File Description: CSIE Module File Version: 1, 65, 0, 8 Internal Name: CSIE Legal Copyright: Copyright 2003, 2004 ClearSearch, Inc. Original Filename: CSIE.DLL Product Name: CSIE Module Product Version: 1, 65, 0, 8  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: IGetNet.ClearSearch
Pest Info: Category: Adware Background Info: Click here
File Info: In File: c:\progra~1\lycos\ieagent\csie.dll Date: 10/5/2004 12:12:20 PM File Description: CSIE Module File Version: 1, 65, 0, 8 Internal Name: CSIE Legal Copyright: Copyright 2003, 2004 ClearSearch, Inc. Original Filename: CSIE.DLL Product Name: CSIE Module Product Version: 1, 65, 0, 8
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: DyFuCA.Internet Optimizer  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\Documents and Settings\Raven\local settings\temp\optimize.exe Date: 1/26/2005 5:49:32 AM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: Ares
Pest Info: Category: Adware Background Info: Click here
File Info: In File: C:\Program Files\ares\ares.exe Date: 1/25/2005 11:33:18 AM Company Name: Ares Development Group File Description: Ares File Version: 1.8.1.2956 Internal Name: Ares Original Filename: ARES.EXE Product Name: Ares for windows Product Version: 1.8.1
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine
Action: Ignored

~~~

Pest: AdDestroyer  
Pest Info: Category: Adware Background Info: Click here  
File Info: In File: C:\WINDOWS\system32\swrt01.dll Date: 10/22/2003 6:14:06 PM

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or quarantine  
Action: Ignored

~~~

Pest: XoloX
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\typelib\{2850bdc7-2330-4e31-9fa0-88268846539a}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: XoloX  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\gnutella  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: XoloX
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\clsid\{f02c0aef-d796-42c9-81e1-084d88f79b8e}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: WinFavorites  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\explorer\browser helper objects\{9c691a33-7dda-4c2f-be4c-c176083f35cf}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: Virtual Bouncer
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\wise solutions\wise installation system\repair\c:/windows/system32/innervbininstall.log|2\software\microsoft\cryptography\services\url
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: Unknown Toolbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\microsoft\internet explorer\toolbar\{2cdela7d-a478-4291-bf31-elb4c16f92eb}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: UCSearch
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry:
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\sharedlls\c:/windows/downloaded program files\ucsearch.ocx
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or ignore
Action: Ignored

~~~

Pest: UCSearch  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\moduleusage\c:/windows/downloaded program files\ucsearch.ocx  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Moderate - this file can be executed! Advice: Delete or ignore

Action: Ignored

~~~

Pest: TrojanDropper.Win32.Siboco.a

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry: HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run|mswsp1

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: TrojanDownloader.Win32.Istbar.ce

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\run|ist service

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: TrojanDownloader.Win32.Intexp

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry: HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run|win server updt

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: TrojanDownloader.Win32.Dyfuca.gen

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry:

HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\explorer\browser helper objects\{00000010-6f7d-442c-93e3-4a4827c2e4c8}

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: SpediaBar

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry: HKEY_LOCAL_MACHINE\software\microsoft\cryptography\services\vurl

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: SpediaBar

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\classes\swrt01.rt

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: SpediaBar

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry: HKEY_LOCAL_MACHINE\software\classes\interface\{0f2a4adc-dabf-4980-8db4-19f67d7b1f95}

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: Shareaza

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry: HKEY\_CURRENT\_USER\software\microsoft\windows\currentversion\run|shareaza

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: [Click here](#)

File Info: In Registry: HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\app management\arpache\p2p networking

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\magnet  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\kazaa\localcontent\databasedir
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\kazaa\localcontent\downloadir  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\kazaa\connectioninfo\kazaanet
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\kazaa\connectioninfo  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\kazaa\cloudload\sharedir
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\kazaa\bandwidth\out|b1  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\kazaa\bandwidth\out|b0seconds
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA

Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\kazaa\bandwidth\out|b0  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\kazaa\bandwidth\lastestimate|b
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\kazaa\bandwidth\lastestimate|time  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\kazaa\bandwidth\in|b0seconds
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\kazaa\bandwidth\in|b1  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\kazaa|tmp
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\kazaa|listenport  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\kazaa
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: KaZaA  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\classes\clsid\{66fc8717-efa7-4546-8c4a-e224f3a80c76}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: KaZaA
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CURRENT_USER\software\kazaa
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ISTbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:

HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\istsvc|displayname  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ISTbar
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry:
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\uninstall\istsvc|nomodify
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ISTbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\istsvc|uninstallstring  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ISTbar
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry:
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\uninstall\istsvc
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: High! This file is now running! Advice: Delete or ignore
Action: Ignored

~~~

Pest: ISTbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc|config\_interval  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ISTbar
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc|config_last
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ISTbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc|config\_url  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ISTbar
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc|app_name
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ISTbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc|update\_interval  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ISTbar
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc|update_version

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc\config\_count

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc\update_last

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc\update\_url

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc\update_count

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc\popup\_url

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc\version

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc\popup\_count

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc\popup_initial_delay

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar

Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc\popup\_interval

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore

Action: Ignored

~~~

Pest: ISTbar
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc|popup_last
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ISTbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc|app\_date  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ISTbar
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\istsvc|account_id
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ISTbar  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\istsvc  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: High! This file is now running! Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ISTbar
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CURRENT_USER\software\ist
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: High! This file is now running! Advice: Delete or ignore
Action: Ignored

~~~

Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\explorer\browser helper objects\{01f44a8a-8c97-4325-a378-76e68dc4ab2e}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{98b2ddba-6da2-4421-af2b-814e98f53649}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\interface\{7371ad3f-c419-4dc0-8e8a-e21fafad53e0}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{6a288140-3e1c-4cd9-aac5-e20fdd4f5d64}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here

File Info: In Registry: HKEY\_CLASSES\_ROOT\interface\{220959ea-b54c-4201-8df2-1cfac8b59fd7}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\imitoolbar.popupwindow.1
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\imitoolbar.popupwindow  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\imitoolbar.popupbrowser.1
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\imitoolbar.popupbrowser  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\imitoolbar.leftframe.1
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\imitoolbar.leftframe  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\imitoolbar.bottomframe.1
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\imitoolbar.bottomframe  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\clsid\{f3155057-4c2c-4078-8576-50486693fd49}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~~~  
Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\clsid\{e2bf1bf3-1fdb-4c93-8874-0b09e71c594c}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~~~  
Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\clsid\{d36f70b1-7df5-4fd4-a765-70ccc8f72cd7}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~~~  
Pest: ImIServer IEPlugin  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\clsid\{1c896551-8b92-4907-8c06-15db2d1f874a}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~~~  
Pest: ImIServer IEPlugin
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\clsid\{01f44a8a-8c97-4325-a378-76e68dc4ab2e}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~~~  
Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\typelib\{e0d3b292-a0b0-4640-975c-2f882e039f52}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~~~  
Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\typelib\{d0c29a75-7146-4737-98ee-bc4d7cf44af9}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~~~  
Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\typelib\{5e594162-60a9-487d-84b8-dbdd716cb862}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~~~  
Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{d7eac2d8-2d52-4010-a4ad-dfdf60c1706c}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~~~  
Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\interface\{c0f88e9e-dceb-4655-968a-ae508a677c39}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~~~  
Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{bccab53d-0895-40c3-a942-a03538ce227a}

Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\interface\{b288f21c-a144-4ca2-9b70-8afafae4b06}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{a986f4db-792e-4571-8974-0bb6e024766f}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\interface\{9bccd51b-4a7b-446c-8452-d32d38004582}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{8c53bd8e-b12d-4c8f-ad0e-c9ddc39d1273}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\interface\{830d3aed-2fa9-454f-b266-d931862bbf34}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{795398d0-dc2f-4118-a69c-592273ba9c2b}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\interface\{6e0ed53c-9908-49ed-b055-7cb31b162577}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{6cdc3337-01f7-4a79-a4af-0b19303cc0be}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\interface\{10d7db96-56dc-4617-8eab-ec506abe6c7e}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\clsid\{d52433a9-a44c-43ab-a013-24b3c756dd2b}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: Ezula  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_CLASSES\_ROOT\clsid\{8940e505-72c6-44de-be85-1d746780efbf}  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: Ezula
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\clsid\{417386c3-8d4a-4611-9b91-e57e89d603ac}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: BearShare  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\classes\gnutella\shell\open\ddeexec  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: BearShare
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\classes\gnutella\shell\open\command
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: BearShare  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\classes\gnutella\defaulticon  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: BearShare
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\classes\gnutella|url protocol
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: BearShare  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\classes\ed2k\shell\open\ddeexec  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: BearShare
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\classes\ed2k\shell\open\command
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: BearShare  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\classes\ed2k\defaulticon  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or

ignore  
Action: Ignored  
~~~~

Pest: BearShare
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_LOCAL_MACHINE\software\classes\ed2k?url protocol
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored
~~~~

Pest: BearShare  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry: HKEY\_LOCAL\_MACHINE\software\classes\ed2k  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored  
~~~~

Pest: 2nd Thought
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry:
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\uninstall\urlsidebar\uninstallstring
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored
~~~~

Pest: 2nd Thought  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\urlsidebar\displayname  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored  
~~~~

Pest: 2nd Thought
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry:
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\uninstall\spidersidebar\displayname
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored
~~~~

Pest: 2nd Thought  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\spidersidebar\uninstallstring  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored  
~~~~

Pest: 2nd Thought
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry:
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\uninstall\ronsidebar\uninstallstring
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored
~~~~

Pest: 2nd Thought  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\ronsidebar\displayname  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored  
~~~~

Pest: 2nd Thought

Pest Info: Category: Adware Background Info: Click here
File Info: In Registry:
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\uninstall\mirrorunder|displayname
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: 2nd Thought  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\mirrorunder|uninstallstring  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: 2nd Thought
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry:
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\uninstall\contextsidebar|uninstallstring
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: 2nd Thought  
Pest Info: Category: Adware Background Info: Click here  
File Info: In Registry:  
HKEY\_LOCAL\_MACHINE\software\microsoft\windows\currentversion\uninstall\contextsidebar|displayname  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore  
Action: Ignored

~~~

Pest: 2nd Thought
Pest Info: Category: Adware Background Info: Click here
File Info: In Registry: HKEY_CLASSES_ROOT\interface\{0f2a4adc-dabf-4980-8db4-19f67d7b1f95}
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete or ignore
Action: Ignored

~~~

Pest: Zedo Spyware Cookie  
Pest Info: Category: Spyware Cookie Background Info: Click here  
File Info: In File: C:\Documents and Settings\Raven\Cookies\raven@zedo[1].txt Tracking URL:  
zedo.com Hits: 10 Received: 3/3/2005 5:05:14 PM Expires: 2/28/2015 3:00:28 PM  
Certainty: Confirmed Threatens: Confidentiality, Liability Risk: Low. Advice: Delete  
Action: Ignored

## References

- Bartlett, John. "Steganography: The Ease of Camouflage". SANS Reading Room. March 2002.  
URL: <http://www.sans.org/rr/papers/20/762.pdf> (July 2004)
- Carnegie Mellon SEI. "Using MD5 to verify the integrity of file contents." CERT Coordination Center. March 2000.  
URL: <http://www.cert.org/security-improvement/implementations/i002.01.html> (July 2004)
- Department of Justice. "Theft of Commerical Trade Secrets". Section VIII Computer Crime and Intellectual Property Section (CCIPS), April 2001.  
URL: <http://www.usdoj.gov/criminal/cybercrime/ipmanual/08ipma.htm> (Jan 2005)
- Eshelman, James. "The Parasite Flight." Windows Support Center. August 2004  
URL: <http://aumha.org/a/parasite.htm>. (October 2004)
- Grossman, Mark. "Trade Secrets in a Dot-Com World." Gigalaw.com. May 2000.  
URL: <http://www.gigalaw.com/articles/2000-all/grossman-2000-05c-all.html> (September 2004)
- Hamilton, David. "The Growing Web of Internet Law: The Regulation of Internet Crime." Attorney in Paris. 2004.  
URL: <http://www.attorneyinparis.com/publwork.htm> (October 2004)
- Honeynet Project, The. Know Your Enemy. Boston: Addison-Wesley, Inc., 2001.
- Kruse, Warren, et al. Computer Forensics. Boston: Addison-Wesley, Inc., 2001.
- Lee, Rob. Forensic and Investigative Essentials. SANS Institute, 2004.
- Rivest, Ronald. "The MD5 Message-Digest Algorithm." RFC 1321. April 1992.  
URL: <http://www.faqs.org/rfcs/rfc1321.html> (July 2004)
- Scambray, Joel, et al. Hacking Exposed, 2<sup>nd</sup> Edition. Berkeley: McGraw-Hill, 2001.
- Seamons, Kent. FAT File System Tutorial. BYU CS345.  
URL: <http://faculty.cs.byu.edu/~seamons/cs345/FatTutorial-Seamons.pdf>
- Stang, David. "Testing Detection and Removal." PestPatrol Center for Pest Research. July 2004.  
URL: [http://research.pestpatrol.com/WhitePapers/Testing\\_Detections.asp](http://research.pestpatrol.com/WhitePapers/Testing_Detections.asp) (October 2004)

Stang, David. "Internet Intruders: Spyware, Adware, Hijackers and Other Pests."  
PestPatrol Center for Pest Research. undated.  
URL: [http://research.pestpatrol.com/WhitePapers/Testing\\_Detections.asp](http://research.pestpatrol.com/WhitePapers/Testing_Detections.asp) (October 2004)

Weil Gall, Barbara. "An Overview of Intellectual Property." GigaLaw.com. October 2000.  
URL: <http://www.gigalaw.com/articles/2000-all/gall-2000-10-all.html>. (August 2004)

© SANS Institute 2005, Author retains full rights.

## Summary of Informational References

1. CERT entry titled “Using MD5 to verify the integrity of file contents. Gives a brief description of the MD5 tool and provides examples of its use.  
<http://www.cert.org/security-improvement/implementations/i002.01.html>
2. Internet Request For Comments (RFC) 1321 – The MD5 Message-Digest Algorithm. This discusses the MD5 algorithm itself and how it works.  
<http://www.faqs.org/rfcs/rfc1321.html>
3. FAT12 filesystem tutorial presentation that provides details of the format.  
<http://faculty.cs.byu.edu/~seamons/cs345/FatTutorial-Seamons.pdf>
4. Pest management tools comparison information.  
<http://spywarewarrior.com/asw-test-guide.htm#descript>
5. Pest Patrol searchable or browsable encyclopedia of approximately 26,000 pests. These entries include general information and manual removal instructions.  
<http://research.pestpatrol.com/Search/Search.aspx>
6. Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the US Department of Justice “Theft of Commercial Trade Secrets” section.  
<http://www.usdoj.gov/criminal/cybercrime/ipmanual/08ipma.htm>

© SANS Institute 2005

## Summary of Download Site References

1. Retrieve The Sleuth Kit, Autopsy and other forensic investigation tools.  
<http://www.sleuthkit.org/proj.php>
2. Retrieve Foremost utility that is used to extract files from an image based on header and footer definitions.  
<http://foremost.sourceforge.net/>
3. Download free flash intros for websites.  
<http://toolittletime.com/free/f01.htm>
4. The Camouflage tool used to hide data in the Ballard case.  
<http://camouflage.unfiction.com>
5. Demo version of Pest Patrol pest management software. Demo does scan only, not removal.  
[http://www.pestpatrol.com/Products/PestPatrolHE/Single\\_User\\_Evaluation.asp](http://www.pestpatrol.com/Products/PestPatrolHE/Single_User_Evaluation.asp)
6. WinAnlysis audit tool that helps management of system change.  
<http://www.winalysis.com>
7. Invisible Keylogger Steath (IKS) keyboard tracking software.  
<http://www.invisiblekeylogger.com/>
8. Elitewrap is a utility for packing executables.  
<http://homepage.ntlworld.com/chawmp/elitewrap/elitewrap.zip>
9. Back Orifice is a backdoor remote access tool.  
<http://www.cultdeadcow.com/tools/bo.html>