CCSI460 Final Forensic Lab Report

Investigator’s Name: *Matt Ferry*

Date of Investigation: *9/23/2013*

Lab Number and Title: 4: Hard Drive Image Analysis

Summary of Findings:

Denny Vette (dvette@hotmail.com) sent an email to mrbig@second.source.ru on Tuesday Jan 1, 2002 at 23:09:06 -0500 that contained an attachment, pic2.jpg. Hidden within this attachment was source code information that was leaked out (see **Stegout-contents**).

Other findings of Note:

 Username: ewilson

 FileName: realhot.jpg

 File Path: Week4Image.dd\SYS-FAT16\Documents and Settings\ewilson\My Documents\My Pictures\realhot.jpg

 The above file is a pornographic file and should be brought to the attention of the lead investigator / prosecution / company to determine the next course of action, as this could create civil issues within the company related to sexual harassment (at the very least).

 Username: spook

 FileName: Dc1.xls

 File Contents: This file appears to contain a manual record of email information: Subject, Body, FromName, FromAddress, FromType, ToName, ToAddress, ToType, CCName, CCAddress, CCType, BCCNAME, BCCAddress, BCCType, BillingInformation, Categories, Importance, Mileage, and Sensitivity (spelling error on Sensitivity maintained from the file)

 This raises a red flag, because there should be no need to manually track this type of information. All of the messages are Security / Network / Hacking related.

 The lead investigator / prosecutor / company should be informed in case further investigation is required.

Details of Investigation:

Investigation into an Intelligent Imaging Solutions image to determine how their source code was exposed. Who exposed it and when it happened.

The investigation should also look for any other questionable activity including civil and criminal activities.

 Also noting that at the start of the investigation, this is when warrant /subpoena information and details would be verified to determine the scope of the investigation. This is also when you want to verify that chain of custody logs have been maintained and properly filled out so that your investigation is documented and covered within that chain, preserving the credibility of the any evidence that may be found during the investigation.

9/23/2013

 8:40 AM – Downloaded the Image.zip file and extracted its contents.

 8:42 AM – Noting MD5 Sum from the included MD5 Hash file

 b24b5e52d27682af6634c16ce70671db

 8:43: AM – Obtaining Image hash and verifying match.



 8:46 AM – Hash verified as the same, Opening FTK and creating case with the image.dd file selected as the evidence file to be examined.

 8:51 AM – Notating the goals of this investigation.

Your case is to investigate the Intelligent Imaging Solutions (IIS) image and determine the following.

1. How their source code was exposed, who did it, and when it happened.
2. All other questionable activity within IIS to include civil liability and criminal activity.
3. As this is a real investigation, please ensure that you follow the proper procedures for forensic work (which might include further warrants, subpoenas, chain of custody forms, etc.).

8:52 AM – Taking particular note of number three. Even though this assignment is setup to be as close to the real world as possible it is still a college assignment, as such I am e-mailing the professor to see how he wants us to handle number three of this lab.

12:55 PM – No Response yet from the professor.

12:59 PM - Beginning to look into the first point of this investigation. Because this point is specifically in regards to whom, when, and how, I will start with the basics and look at emails first to see if anything unusual stands out.

1:02 PM – discovered the following email. $100k is a lot of money for a single picture something else may be going on here.

|  |
| --- |
| **Message0001** |
| **Subject:** | **A Pic** |
| **From:** | "denny vette" <dvette@hotmail.com> |
| **Date:** | Tue, 1 Jan 2002 23:09:06 -0500 |
| **To:** | <mrbig@second.source.ru> |
| **Message Body** |
| Big, here's the picture that I promised you.  As agreed, you'll pay me $100k now and the rest later. denny |
| **Attachment** |
| -----Attachment2-----File name = "pic2.jpg" |

|  |
| --- |
| **Main Message Header** |
| From: "denny vette" <dvette@hotmail.com>To: <mrbig@second.source.ru>Subject: A PicDate: Tue, 1 Jan 2002 23:09:06 -0500MIME-Version: 1.0Content-Type: multipart/mixed; boundary="----=\_NextPart\_000\_000D\_01C19319.4FAC1E30"X-Priority: 3X-MSMail-Priority: NormalX-Mailer: Microsoft Outlook Express 5.00.2919.6700X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700 |
| **Sub Header** |
| Content-Type: multipart/alternative; boundary="----=\_NextPart\_001\_000E\_01C19319.4FAC1E30" |
| **Sub Header** |
| Content-Type: text/plain; charset="iso-8859-1"Content-Transfer-Encoding: quoted-printable |
| **Sub Header** |
| Content-Type: text/html; charset="iso-8859-1"Content-Transfer-Encoding: quoted-printable |
| **Sub Header** |
| Content-Type: image/jpeg; name="pic2.jpg"Content-Transfer-Encoding: base64Content-Disposition: attachment; filename="pic2.jpg" |

Email was sent from Denny Vette (dvette@hotmail.com) to mrbig@second.source.ru (an email address hosted in Russia).

Date sent Jan 1 2002 23:09:06 -0500 containing attachment pic2.jpg.

1:13 PM - Located multiple pic2.jpg

1:15 PM – Located the specific file related to the email

File Name Full Path

pic2.jpg Week4Image.dd\SYS-FAT16\Documents and Settings\dvette\Local Settings\Application Data\Identities\{5770B94C-E082-4088-B8BD-DFEAE489C6EE}\Microsoft\Outlook Express\Sent Items.dbx>>Message0001>>pic2.jpg

1:17 PM – Exported this file and ran steghide checking for hidden information, outputting any found information to a file called stegout.

1:19 PM – Stegout was written to, attempting to open as a text file.

1:20 PM – File successfully opened as a text file in notepad and editpad lite.

1:25 PM – Stegout now contains header and program information of a classified project.

1:28 PM – I believe that this information successfully answers the first point of this assignment. Denny Vette (dvette@hotmail.com) sent an email to mrbig@second.source.ru on Tuesday Jan 1, 2002 at 23:09:06 -0500 that contained an attachment pic2.jpg. Within this attachment was the source code information that was leaked out.

1:30 PM – Still no response from the professor, so I am pausing the investigation while awaiting a reply.

6:15 PM – Received an email response from the professor. Writing the first part of the summary for this week’s assignment, as there is enough information to answer the first point of this investigation.

6:24 PM – Continuing Investigation

6:29 PM – Discovered evidence that another employee may be surfing porn websites using company equipment,

File Name Full Path

realhot.jpg Week4Image.dd\SYS-FAT16\Documents and Settings\ewilson\My Documents\My Pictures\realhot.jpg

This information should be brought to the attention of the Lead Investigator / Prosecutor / Company to determine if a separate investigation is required and if any further actions are required at this time. (Username: ewilson)

6:41 PM – Located several more images under the dvette username. Checking those images for steganography.

6:55 PM – Steghide did not reveal any other concealed images at this time.

6:57 PM – Noting a excel spreadsheet file in the recycle bin called Dc1.xls

This file appears to contain a manual record of some emails including Subject,

Body, FromName, FromAddress, FromType, ToName, ToAddress, ToType, CCName, CCAddress, CCType, BCCNAME, BCCAddress, BCCType, BillingInformation, Categories, Importance, Mileage, Sensitivity

This raises a red flag, because in general there should not be a need to manually keep track of this type of information. All of the messages are Security / Network / Hacking related. Again, this is something that the lead investigator / company should be informed of in case further investigation is needed (username: spook)

7:19 PM – Located Steghide documentation files in a \bin directory indicating

7:23 PM – Located the steghide program within the \bin directory

7:45 PM – At this time I see nothing else of immediate interest. Closing FTK.

9/29/2013

 2:00 PM - Reviewed report before submission to this the dropbox.

Appendix

**Stegout-contents**

/\*

 \* $Header: /cvs/cvs/PCS/include/pcs.h,v 2.2.1.2 1997/07/07 17:13:26 larry Exp $

 \*

 \* $Log: pcs.h,v $

 \* Revision 2.2.1.2 1997/07/07 17:13:26 larry

 \* Stripped old headers and control characters

 \*

 \* Property of Military Security Agency (MSA)

 \* Classification: Top Secret

 \*

 \* Development by Intelligent Imaging Solutions (IIS) for US Threat Detection

 \* System.

 \*/

#ifndef \_\_PCS\_H

#define \_\_PCS\_H

#include <sys/types.h>

#include <sys/ipc.h>

#include <sys/shm.h>

#include <sys/stat.h>

#include <errno.h>

#include <fcntl.h>

#include <string.h>

#include <syslog.h>

#include <time.h>

#include <stdarg.h>

#include <termio.h>

#include <stropts.h>

#include <libgen.h>

#include <stdlib.h>

#include <stdio.h>

#ifndef \_CASLINC

typedef unsigned int U32;

typedef int S32;

typedef unsigned short U16;

typedef short S16;

typedef unsigned char U8;

typedef char S8;

typedef int BOOL;

#endif

#ifndef TRUE

#define TRUE ( 1 )

#endif

#ifndef FALSE

#define FALSE ( 0 )

#endif

/\* PCS application define section \*/

/\* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \*/

#define MGR\_NAME "PCSM"

#define SRV\_NAME "PCSS"

#define APP\_NAME "PCS"

#define MSG\_LOCK\_FNAME "MSG.LCK"

#define CTX\_LOCK\_FNAME "CTX.LCK"

#define STAT\_LOCK\_FNAME "STAT.LCK"

#define TRAN\_DPC\_FNAME "tran-dpc.cfg"

#define X25NAB\_FNAME "x25nabanco.cfg"

#define X25TBR\_FNAME "x25tbr.cfg"

#define X25LCN\_FNAME "x25lcn.cfg"

#define USERID\_PC\_FNAME "userid-pc.cfg"

#define PC\_SSN\_FNAME "pc-ssn.cfg"

#define MSR\_164\_FNAME "msr164.cfg"

#define MSR\_212\_FNAME "msr212.cfg"

#define MSR\_ROUTE\_FNAME "msrroute.cfg"

#define ITU\_GTT\_FNAME "addrmap.cfg"

#define MGR\_TERMINATE\_MSG 0xabba

#define PCS\_RESTART\_APP 0xabbb

#define PCS\_WAKEUP\_CALL 0xabbc

#define PCS\_PROCESS\_STATS 0xabbd

#define FILE\_MODE (S\_IRUSR | S\_IWUSR | S\_IRGRP | S\_IWGRP | S\_IROTH)

#define SHM\_MODE ( SHM\_R | SHM\_W )

#define GET\_LOCK ( 0 )

#define RELEASE\_LOCK ( 1 )

#define MAXLINE ( 1024 )

#define MAX\_TRANDPC\_ENTRIES ( 50 )

#define MAX\_X25NB\_ENTRIES ( 500 )

#define MAX\_X25TBR\_ENTRIES ( 500 )

#define MAX\_X25LCN\_ENTRIES ( 500 )

#define MAX\_PC\_SSN\_ENTRIES ( 500 )

#define MAX\_UID\_PC\_ENTRIES ( 5000 )

#define MAX\_MSR\_164\_ENTRIES ( 1000 )

#define MAX\_MSR\_212\_ENTRIES ( 1000 )

#define MAX\_ITU\_GTT\_ENTRIES ( 1000 )

#define MAX\_MSR\_ROUTE\_ENTRIES ( 3000 )

#define MAX\_BILLING\_ENTRIES ( 20000 )

#define USE\_CURRENT\_FILE ( 0 )

#define CREATE\_NEW\_FILE ( 1 )

#define REWIND\_FILE ( 2 )

#define NO\_REWIND\_FILE ( 3 )

#define CURRENT\_MONTH ( 0 )

#define PREVIOUS\_MONTH ( 1 )

#define CURRENT\_DAY ( 2 )

#define PREVIOUS\_DAY ( 3 )

#define BATCH\_COUNT ( 1 )

#define TC\_COUNT ( 255 )

#define QUEUE\_LEN ( 128 )

#define MIN\_SERVERS ( 2 )

#define MAX\_SERVERS ( 16 )

#define CLG\_CARD\_QUERY ( 0 )

#define CLG\_CARD\_RESPONSE ( 0 )

#define COL\_CALL\_QUERY ( 1 )

#define COL\_CALL\_RESPONSE ( 1 )

#define THIRD\_NUM\_QUERY ( 2 )

#define THIRD\_NUM\_RESPONSE ( 2 )

#define TBR\_QUERY ( 3 )

#define TBR\_RESPONSE ( 3 )

#define NABANCO\_QUERY ( 4 )

#define NABANCO\_RESPONSE ( 4 )

#define X25CNAMQUERY ( 9 )

#define X25CNAMRESPONSE ( 9 )

/\* phase 2 getdata messages \*/

#define GD\_OLNS\_QUERY ( 0 )

#define GD\_OLNS\_RESPONSE ( 0 )

#define GD\_CCV\_QUERY ( 1 )

#define GD\_CCV\_RESPONSE ( 1 )

#define GD\_NAB\_QUERY ( 2 )

#define GD\_NAB\_RESPONSE ( 2 )

/\* Function prototype section \*/

/\*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \*/

void SegVSigHandler(int);

void TermSigHandler(int);

void IPCSigHandler(int);

void ChildSigHandler(int);

void RestartApp(void);

int Initialize(char \*);

int CreateChild(U32);

int TerminateChild(int);

void TerminateChildren(void);

void Terminate(int);

void SetTimer(U32, long);

void AttachSHMemory(int, void \*);

void SychronizeAccess(int, int);

int CreateLockFile(char \*);

int set\_applenv(char\*);

char \*cur\_time(time\_t);

char \*cur\_date(time\_t);

char \*mmitok(char \*, char );

void log\_open(const char\*, const char \*, int, int);

void log\_syserr\_terminate(const char \*fmt, ...);

void log\_syserr\_dump(const char \*fmt, ...);

void log\_syserr\_continue(const char \*fmt, ...);

void log\_err\_terminate(const char \*fmt, ...);

void log\_err\_continue(const char \*fmt, ...);

char \*tcapName;

#endif