GUIDANCE SOFTWARE

From beginning to endpoint.

Examiner Report

Case Information

Case Number	001
Examiner Name	Shona Start – w17019752
Description	Confidential spreadsheet containing the names and salaries of the company's key employees was leaked from company M57.Biz. This spreadsheet only existed on the hard drive of employee Jeans laptop. This report aims to detail an analysis of this hard drive.

Evidence

Name	Acquisition MD5	Verification MD5	Evidence Number	Examiner Name
Jean's hard drive from the first M57 project	78a52b5bac78f4e711607707ac0e3f93	78a52b5bac78f4e711607707ac0e3f93	2008-M57-Jean	Donny

Examination

Below is an analysis of a forensic image, of the hard disk recovered from Jean's laptop computer.

I never came in contact with the original hard drive and therefore to the best of my knowledge this evidence has not been edited or tampered with.
The following tools were used to analysis the image:

- EnCase Forensic 8

The 'boot.ini' file present on the hard disk allows us to determine that Windows XP Professional is the operating system for this machine. It also lists only one partition present. (See 19).

Data stored in the 'system' registry tells us that the device is set to the GMT time zone, meaning that all time stamps on the device will match up with this time zone. (See 20)

Accessing the 'SAM' (Security Accounts Manager) reveals that there are a number of accounts present on the disk (See accounts 10 to 18). No passwords are in place for any of these accounts meaning that anyone with access to the physical device could have access to the contents of the hard drive. The Jean account can be assumed to be the suspects account, due to matching names.

As a device using Windows XP, Windows XP search assistant will be present. The history of the search assistant, which was located in each of the user's 'NTUSER.DAT' file, brought up nothing of use to the case. The 'NTUSER.DAT' files also contain details on MRU (Most Recently Used). For the Jean account the last opened MRU is the My Pictures folder present on the account, however nothing of use to the case is stored in this folder. The other accounts don't have any MRU's.

Further analysis of the Jean account reveals many notable resources. An analysis of the recycle bin, AIM account history, external device usage, Prefetch, images and videos on the device brought up nothing of interest to the case. On the Desktop, however, there is a spreadsheet called 'm57biz.xls' (See 8), this file contains the personal details of M57.biz employees. It includes full names, the employees position in the company, their salaries and their social security number. Employees listed include Alison, Jean, Bob, Carol, Dave, Emmy, Gina, Harris and Indy.

A search of all files on the Jean account for occurrences of 'm57biz', leads to an email in Jeans email history, 'jean@m57.biz', where the file 'm57biz.xls' has been attached to an email from Jean to 'tuckgorge@gmail.com' (see email 7). 'tuckgorge@gmail.com' is not a company email. In my opinion it is highly likely that this is where the leak occurred. It can be determined that the 'm57biz.xls' file has not been edited or changed since before this email. 'm57biz.xls' was created, lasted accessed and written on the 20/07/08 at 02:28:03 and this email was sent at 20/07/08 02:28:03:47. From those times it can be established that the file (as it is now) is exactly the same as when it was sent to 'tuckgorge@gmail.com'.

By further analysing the email history for Jeans account using comprehensive processing, it is evident that Jean had been in regular connect with another user called Alison. The name Alison appears in the 'm57biz.xls' as the company's President, and it could be concluded through dialogue throughout emails where Alison asks Jean about business plans and financial projections that this is in fact the same person.

Alison seems to have two email addresses and it is suggested during email communications on the 20/07/08, in email 5, that there was confusion between Alison and Jean on which email is the genuine

email address. The two email addresses are ‘alison@m57.biz’ and alex@m57.biz.
Upon asking which email is the correct email, Jean receives responses from both. The first to respond is ‘alex@m57.biz’, using the display name Alex, which clams it is the correct email, ‘alison@m57.biz’, also using the display name Alex, then replies to this claiming Alison’s “email was misconfigured”. Correspondences with ‘alex@m57.biz’ only occur on the 20/07/08 whereas; correspondence with ‘alison@m57.biz’ lasts from 06/07/08 till 21/07/08. It is not clear exactly what has occurred here, an error with Alison’s email accounts could have occurred. However, in my opinion it is also possible that one of these replies is not genuine and these timings would suggest ‘alex@m57.biz’ is not genuine as it is the newer contact.

However, an email sent shortly after these communications in my opinion suggests ‘alison@m57.biz’ is actually the disingenuous one. On the 20/07/08 (see email 3), ‘alison@m57.biz’, asks Jean to “put together a spread sheet specifying each employee in the company, their current salary, and their SSN?”. This email suggests Jean created the ‘m57biz.xls’ file for Alison. However, there are irregularities in this email. In my opinion, the structure of this email differs from Alison regular emails, it takes a more formal approach, whereas most other emails from ‘alison@m57.biz’ have a less formal and direct structure. For instance, they don’t always address each other or close off their emails, they often don’t talk in paragraphs and they have rarely used use pleasantries such as please and thank you. In my opinion, the structure of this email more closely resembles emails from ‘tuckgorge@gmail.com’, such as email 7. Another irregularity is this email was sent using the display name ‘alison@m57.biz’, this is the first and last occurrence of this display name being used with this email address. However, the display name is always used alongside emails from ‘tuckgorge@gmail.com’.

This email also raises suspicion because it is only ever mentioned again in emails received from ‘tuckgorge@gmail.com’. For instance, in email 7, as was discussed earlier, when Jean sends the ‘m57biz.xls’ file she is replying to an email from ‘tuckgorge@gmail.com’ where they ask for the information already requested. The owner of tuckgorge@gmail.com should not be able to see correspondence between ‘alison@m57.biz’ and ‘jean@m57.biz’. In my opinion, this suggests that the original email between ‘alison@m57.biz’ and ‘jean@m57.biz’ requesting employee details could possibly be the result of an email spoof. This would also explain why a different display name was used, as an attacker may not have knowledge of the display name that is usually used. This theory is supported by email 4. This is a reply from Jean to email 3 where ‘alison@m57.biz’. using the display name “alex”, shows confusion at Jeans reply, this would make sense if email 4 is a spoof as Alison would have no idea the email existed.

Another notable email is email 6 from ‘alison@m57.biz’ using the display name ‘AlisonM57’, it mentions three names as programmers employed by the company. Two of these names, Bob and Carol, are included in the ‘m57biz.xls’ alongside their personal details. However, the other programmer mentioned, Alice, is not included in this document. There are also no examples of communication with anyone called Alice, whereas emails from Bob and Carol with addresses ‘bob@m57.biz’ and ‘carol@m57.biz’ are present in the history. A search of the drive for other occurrences of ‘Alice’ does not bring up anything of note.

On analysis of the internet history from the Jean account, collected using a comprehensive search, the domains www.who.is and www.who.is/ stand out from her regular activity (See Internet records 1 and 2). These domains have been visited a total of eight times with five different variations of the URL’s visited, this would suggest four different searches were performed on this website. This stands out from Jeans regular internet history because it is unusual compared to the other web browsing activities shown in her history.

From the evidence collected, it is my opinion emails from ‘alison@m57.biz’ with the display name ‘alison@m57.biz’ are not from Alison but instead from the owner of the address ‘tuckgorge@gmail.com’. Taking this into consideration, in my opinion, Jean was a victim of email spoofing and phishing. It is my belief the display name ‘alison@m57.biz’ was used with emails from ‘tuckgorge@gmail.com’ to trick Jean in to believing she was communicating with Alison when in fact she was not in order to retrieve sensitive information.

Internet Records

1) index.dat

Item Path Internet Explorer (Windows)\History\Weekly\index.dat
Comment

Type	URL
Visit Count	1
Url Name	www.who.is
Url Host	www.who.is
Net Show Url	:Host: www.who.is
Start Date	30/06/08 00:00:00
End Date	07/07/08 00:00:00
Internet Artifact Type	History\Weekly
Record Last Accessed	06/07/08 08:49:54
Created	07/07/08 06:26:04
Browser Type	Internet Explorer (Windows)
Profile Name	Jean
Message Size	256

2) index.dat

Item Path Internet Explorer (Windows)\History\Weekly\index.dat
Comment

Type	URL
Visit Count	1
Url Name	http://www.who.is/whois_index/m/domain_list.m.0002.php
Url Host	www.who.is/
Expiration	01/08/08 07:42:46
Start Date	30/06/08 00:00:00
End Date	07/07/08 00:00:00
Internet Artifact Type	History\Weekly
Record Last Accessed	06/07/08 08:49:54
Created	07/07/08 06:26:04
Browser Type	Internet Explorer (Windows)
Profile Name	Jean
Message Size	256

Email

3) Root folder\Top of Personal Folders\Inbox\background checks

Comment Appears to be an email from Alison to Jean. Alison is requesting Jean to create a spreadsheet containing the personal details of employees at M57.biz.

From	alison@m57.biz <alison@m57.biz>
To	jean@m57.biz <jean@m57.biz>
Sent	20/07/08 00:39:57
Received	20/07/08 00:39:57

Subject	background checks

Jean,

One of the potential investors that I've been dealing with has asked me to get a background check of our current employees. Apparently they recently had some problems at some other company they funded.

Could you please put together for me a spreadsheet specifying each of our employees, their current salary, and their SSN?

Please do not mention this to anybody.

Thanks.

(ps: because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)

4) Root folder\Top of Personal Folders\Inbox\RE: background checks

Comment: Appears to be a response from Jean to Alison's "background checks" email, implying that she created the spreadsheet. Then another response from Alison to Jean where Allison expresses confusion.

From	alex <alison@m57.biz>
To	Jean User <jean@m57.biz>
Sent	20/07/08 00:50:20
Received	20/07/08 00:50:20
Subject	RE: background checks

What's a "sure thing." ?

-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:46 AM
To: alison@m57.biz
Subject: RE: background checks

Sure thing.

5) Root folder\Top of Personal Folders\Inbox\RE: which email address are you using?

Comment: Correspondence between 'jean@m57.biz', 'alison@m57.biz' and 'alex@m57.biz'. Confusion on which email address is Alison's.

From	alex <alison@m57.biz>
To	Jean User <jean@m57.biz>
Sent	20/07/08 00:43:48
Received	20/07/08 00:43:48
Subject	RE: which email address are you using?

Whoops. It looks like my email was misconfigured.

My email is alison@m57.biz, not alex. Sorry about that.

-----Original Message-----
From: alex [mailto:alex@m57.biz]
Sent: Sunday, July 20, 2008 12:33 AM
To: Jean User; alison@m57.biz
Subject: RE: which email address are you using?

This one, obviously.

-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:32 AM
To: alison@m57.biz
Subject: which email address are you using?

Are you going to use alex@m57.biz or alison@m57.biz?

6) Root folder\Top of Personal Folders\Inbox\RE: programmers

Comment Correspondence between Jean and Alison. See response at 12:44am for mention of Alice.

From	alex <alison@m57.biz>
To	Jean User <jean@m57.biz>
Sent	20/07/08 00:50:20
Received	20/07/08 00:50:20
Subject	RE: programmers

Well, make it happen.

-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:46 AM
To: alex
Subject: RE: programmers

Not yet.

-----Original Message-----
From: alex [mailto:alison@m57.biz]
Sent: Sunday, July 20, 2008 12:44 AM
To: Jean User
Subject: programmers

Have you heard anything yet from Alice, Bob and Carol? They were all supposed to start last week.

-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:32 AM
To: alison@m57.biz
Subject: which email address are you using?

Are you going to use alex@m57.biz or alison@m57.biz?

7) Root folder\Top of Personal Folders\Sent Items\RE: Please send me the information now

Comment: Communications between 'tuckgorge@gmail.com' and Jean. Attachment 'm57biz.xls' contains confidential information.

From	Jean User <jean@m57.biz>
To	alison@m57.biz <tuckgorge@gmail.com>
Sent	20/07/08 02:28:47
Received	20/07/08 02:28:00
Subject	RE: Please send me the information now

I've attached the information that you have requested to this email message.

-----Original Message-----
From: alison@m57.biz [mailto:tuckgorge@gmail.com]
Sent: Sunday, July 20, 2008 2:23 AM
To: jean@m57.biz
Subject: Please send me the information now

Hi, Jean.

I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?

Thanks.

Alison

Attachments

Name	m57biz.xls
Last Modification Time	20/07/08 02:28:03
Logical Size	291,840

m57biz.xls

Desktop

8) m57biz.xls

Item Path	Jean's hard drive from the first M57 project\C\Documents and Settings\Jean\Desktop\m57biz.xls
File Created	20/07/08 02:28:03
Last Written	20/07/08 02:28:03
Last Accessed	20/07/08 02:28:03
MD5	e23a4eb7f2562f53e88c9dca8b26a153
Comment	Spreadsheet containing information which was leaked

9) m57biz.lnk

Item Path	Jean's hard drive from the first M57 project\C\Documents and Settings\Jean\Recent\m57biz.lnk
File Created	20/07/08 02:28:04
Last Written	20/07/08 02:28:04
Last Accessed	20/07/08 02:28:04

MD5	267c4ad8a74c278fa0d5013342b43b64
Comment	m57biz.xls was a recently accessed file

Accounts

10) Abijah

Item Path	SAM\SAM\Domains\Account\Users\Names\Abijah
File Created	
Last Written	14/05/08 06:34:43
Last Accessed	
MD5	525f1634a6b7a5d4700179ff76188ba1
Comment	An account present on the system

11) Addison

Item Path	SAM\SAM\Domains\Account\Users\Names\Addison
File Created	
Last Written	14/05/08 06:34:03
Last Accessed	
MD5	c1a7f3693d1e2e5f5821b1b351260e9b
Comment	An account present on the system

12) Administrator

Item Path	SAM\SAM\Domains\Account\Users\Names\Administrator
File Created	
Last Written	13/05/08 23:20:14
Last Accessed	
MD5	7b7bc2512ee1fedcd76bdc68926d4f7b
Comment	Administrator account, created with Windows machines

13) Devon

Item Path	SAM\SAM\Domains\Account\Users\Names\Devon
File Created	
Last Written	14/05/08 06:34:54
Last Accessed	
MD5	ca9b33c206e08498e2e4ad87b6197473
Comment	An account present on the system

14) Guest

Item Path	SAM\SAM\Domains\Account\Users\Names\Guest
File Created	
Last Written	13/05/08 23:20:14
Last Accessed	
MD5	adb831a7fdd83dd1e2a309ce7591dff8
Comment	Guest account, created with Windows machines

15) HelpAssistant

Item Path	SAM\SAM\Domains\Account\Users\Names\HelpAssistant
File Created	
Last Written	13/05/08 22:24:45
Last Accessed	
MD5	18a1dbb4a2ad97a88c432a5a2bc0f3c5
Comment	HelpAssistant account, created with Windows machines

16) Jean

Item Path	SAM\SAM\Domains\Account\Users\Names\Jean
File Created	
Last Written	14/05/08 06:33:08
Last Accessed	
MD5	2a5ea26afb2c1fdbd0e7ab0941b9b9ab
Comment	Suspects (Jeans) account

17) Kim

Item Path	SAM\SAM\Domains\Account\Users\Names\Kim
File Created	
Last Written	14/05/08 06:32:56
Last Accessed	

MD5	f55fbaaca148300ac11f7752528cae3d
Comment	An account present on the system

18) Sacha

Item Path	SAM\SAM\Domains\Account\Users\Names\Sacha
File Created	
Last Written	14/05/08 06:35:35
Last Accessed	
MD5	d9fa428dd3e986c39b7458de8e5d66a9
Comment	An account present on the system

Device Details

19) boot.ini

Item Path	Jean's hard drive from the first M57 project\C\boot.ini
File Created	13/05/08 23:19:59
Last Written	13/05/08 22:23:41
Last Accessed	21/07/08 02:27:28
MD5	fa579938b0733b87066546afe951082c
Start Sector	6,298,545
Sector offset	389
File Offset	101
Length	79
Comment	

```
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
```

20) StandardName

Item Path	$$$PROTO.HIV\ControlSet001\Control\TimeZoneInformation\StandardName
File Created	
Last Written	
Last Accessed	
MD5	a2163a4b4cce1987668d4617a3562999
Start Sector	1,851
Sector offset	36
File Offset	0
Length	36
Comment	

```
G M T   S t a n d a r d   T i m e
```

21) setupapi.log

Item Path	Jean's hard drive from the first M57 project\C\WINDOWS\setupapi.log
File Created	13/05/08 23:20:18
Last Written	20/07/08 02:26:23
Last Accessed	20/07/08 02:26:23
MD5	e240f4e8ceaed8d99d8323b33d59d906
Comment	Plug and play log files

Glossary

The following terms and definitions may be used throughout the report:

Email Spoof

The forgery of the header of an email so that it appears as if the email has originated from a different source than its real source. This tactic is often used alongside phishing and spam as a person is more likely to open an email they believe is from a familiar source.

Phishing

A form of fraud, where an attacker pretends to be a legitimate entity or person in email and/or other online communications in order to trick victims into sharing confidential information or opening malicious links or attachments.