DIGITAL FORENSIC REPORT

CASE: Investigation #1

EVIDENCE ITEM

DATE
09/30/2022

PREPARED BY: ALEXANDER SMETANA

REVISION SUMMARY

DATE	*REVISION HISTORY*	*COMMENTS*
09/30/2022	1.0	Document Creation

INVENTORY

Hardware	Details	
Jeans Laptop (nps-2008-jean.E01)	Hostname	Nps-2008-jean.E01
	Timezone	America/Chicago
	HDD/SSD	11 GB
	OS	Microsoft Windows XP Service Pack 3
	Version	Version: 20101104

Software	Details	
Microsoft Outlook	Version	

Accounts	Details	
Email	Jeans Email	jean@m57.biz
Email	Alison's Email	alison@m57.biz
Email	Bobs Email	bob@m57.biz
Email	Carols Email	carol@m57.biz
Email		accounts-noreplay@google.com
		admin@associatedcontent.com

EXECUTIVE SUMMARY

The company involved is a small startup company m57.biz. A few weeks after launch, a confidential spreadsheet containing the names and salaries of the company's keys employees was posted to the public forum of one of m57. biz's competitors. The spreadsheet only existed on the computer of one of M57s' officers, Jean.

Initially, Jean says that she has no idea how the data left her laptop, and that she must have been hacked. After interviewing Jean would later change her story. She claims that Alison asked her to prepare the spreadsheet as part of a new rounding fund. Alison asked to send the information by email. That is all the information that she provided.

After interviewing, Alison story contradicts Jeans, claiming that she doesn't know what Jean was talking about. She denies ever asking for the spreadsheet from Jean nor receiving any sort of spreadsheet. Allison's email account is allson@m57.biz with a password of "ab=8989". Jean's email account is jean@m57.biz with a password of "gick*1212".

OBJECTIVES

The goal is to find out how the spreadsheet m57.xsl left Jeans laptop. If possible, find the perpetrator since confidential information was exposed since both stories contradict each other.

EVIDENCE

Images	Details	
M57biz.xls	Start	2008-07-19 20:28:03 CDT
	End	2008-07-19 20:28:03 CDT
	MD5	e23a4eb7f2562f53e88c9dca8b26a153
	SHA1	34456b5f714dc9d8dd23c742d54c3f5f582ecb042bc1c4d3042b88203863779f
nps-2008-jean.E01	Start	Acquired Date: Mon Jan 31 15:38:29 2011
	End	System Date: Mon Jan 31 15:38:29 2011
	MD5	78a52b5bac78f4e711607707ac0e3f93
	SHA1	Not calculated

EXAMINATION OF EVIDENCE

Item #1 – Can be described as an xls document found on Jean's computer. Contains confidential information that has been leaked to a competitor's website.

Item #2 – Can be described as the image on Jeans computer.

HASH OF ORIGINAL EVIDENCE

The hash values obtained from the original evidence were as follows:

MD5	e23a4eb7f2562f53e88c9dca8b26a153
SHA1	34456b5f714dc9d8dd23c742d54c3f5f582ecb042bc1c4d3042b88203863779f
Other	

DRIVE GEOMETRY

10.74 GB (10737418240/512 BYTES/SECTOR)

VIRUS SCAN RESULTS

N/A

BIOS EXAMINATION

60869 total files

File Types:

8,611 Images	15,679 Executables
34 videos	4,398 Unknown
9,004 Documents	291 audios
4,972 Other	2 Not Analyzed

EXAMINATION OF FILES

ANALYSIS

After reviewing the file m57biz.xls file was found with confidential information with the created time and date. Emails were identified which contain evidence on how the file left the computer.

TIMELINE

Table 4-1 Timeline

Timestamp (UTC 24hr)	Event	Evidence Source
2008-06-12 20:28:03 CDT	Spreadsheet m57biz.xls is created with confidential information about workers. MD5: e23a4eb7f2562f53e88c9dca8b26a153 Sha256: 34456b5f714dc9d8dd23c742d54c3f5f582ecb042bc1c4d3042b882f	nps-2008-jean.E01_1Host
2008-07-19 18:39:57 CDT	From: alison@m57.biz To: jean@m57.biz Alison requests information via email (alison@m57.biz) requesting confidential information to Jean (jean@m57.biz) regarding employee's name, salary, and SSN.	nps-2008-jean.E01_1Host
2008-07-19 20:22:45 CDT	From: alison@m57.biz To: jean@m57.biz Alison requests information again being very persistent, via email (alison@m57.biz) requesting confidential information to Jean (jean@m57.biz) regarding employee's name, salary, and SSN.	nps-2008-jean.E01_1Host
2008-07-19 20:28:00 CDT	From: jean@m57.biz To: alison@m57.biz	nps-2008-jean.E01_1Host

	Jean (jean@m57.biz) agrees to send the information to Alison (alison@m57.biz). She attaches the file "M57.biz" via an email attachment.	
2008-07-20 00:03:40 CDT	From: alison@m57.biz To: jean@m57.biz Alison sends an email thanking Jean for submitting the file and agrees to handle it from here.	nps-2008-jean.E01_1Host

RELEVANT FINDINGS

Jean sent the biz.xls document containing confidential information to Alison via email. Once received, Alison exposed this information to competitors. Jean and Alison would later go onto deny any knowledge of the information leak as an attempt to cover up.

SUPPORTING DETAILS

Allison requested the data from Jean via email using the email address alison@m57.biz. Jean later complied and sent the information via attachment using the email address jean@m57.biz. Both Alison and Jean are both liable for the information leak.

The XLS file was kept on the drive on Jeans computer. The security on the computer and drive was very low.

INVESTIGATIVE LEADS

Given the evidence, both Jean and Alison were both involved in the information leak. The emails history demonstrates intent by Alison to get the information and Jean being compliant.

M57.biz should further investigate Jean and Alison by questioning them. Afterwards, they should turn them over to authorities regarding the information leak. Going forward, the company should strengthen the policies on who has access to confidential information. They should make use of encryption and store crucial information in a better place rather than on an xml document on a computer.

The passwords of "ab=8989" of Alison and "gick*1212" needs to be strengthened. It is unacceptable to contain PII information on a desktop with passwords so poor. Multi factor authentication is not mentioned however should be used going forward to prevent any sort of data breach.