DIGITAL FORENSIC REPORT

CASE Investigation #2

EVIDENCE ITEM

10/24/2022

PREPARED BY:

REVISION SUMMARY

DATE	*REVISION HISTORY*	*COMMENTS*
10/24/2022	1.0	Creation of document
10/30/2022	1.1	Finalization of the document

INVENTORY

Hardware	Details	
Dell Latitude Cpi Laptop	Hostname	/img_4Dell Latitude CPI.E01
	Timezone	America/Chicago
	HDD/SSD	4.87 GB
	OS	Microsoft Windows XP
	Version	4.19a
	Device ID	002c29e1-0c69-43ef-acb3-1fb2e26dc9bd
Software	Details	
Microsoft Windows XP	Version	4.19a
Accounts	Details	
Local Account	User	Mr. Evil (Greg Schartt)
Email	Mr. Evil	whoknowsme@sbcglobal.net

EXECUTIVE SUMMARY

In the past couple weeks, confidential have gone missing. After tracing the exfiltration of confidential files two weeks ago, Acme Unlimited believes their attacker is determined and will continue to strike again.

A few days ago, the nighttime security guard was making his rounds and was surprised to see an intruder trespassing on company property. While making his escape, the intruder dropped a laptop. Our night guard reported an intruder the other day. Nothing was thought of it at first because it's not uncommon for homeless people to trespass onto the dock. The guard seized a laptop from intruder as they fled.

An image was taken of it and are hoping it helps identify the intruder and maybe what stole or what they were after. It is believed that this individual and the stolen information might be connected.

OBJECTIVES

The objective is to analyze the image on the laptop, determine the identity of the perpetrator and ultimately find the motivations of the individual. If possible, see if this individual has any connections to the confidential data that has been stolen. Determine why an individual would have intent of trespassing on private property.

EVIDENCE

Images	Details	
Dell Latitude Cpi.E01	Start	2022/10/21 12:34:53
	End	2022/10/21 14:15:40
	MD5	aee4fcd9301c03b3b054623ca261959a
	SHA1	Not Given

EXAMINATION OF EVIDENCE

Item #1 – Can be described as an image of the Dell Latitude Cpi Laptop found left by the person.

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

MD5	aee4fcd9301c03b3b054623ca261959a

DRIVE GEOMETRY

4.87 GB (4871301120/512 BYTES/SECTOR)

VIRUS SCAN RESULTS

ZIP BOMB

BIOS EXAMINATION

Date/time accurate

EXAMINATION OF FILES

File Types:

3,384 Images
10 Videos
4,744 Documents
4,767 Other

3,384 Executables
2,166 Unknown
145 Audio
2 Not Analyzed

ANALYSIS

After review of the image, the perpetrator was identified. The image was found to contain many suspicious software that could be used in an attack, most notably password stealing software.

TIMELINE

Timeline of 2004-08-27		
Timestamp (UTC 24hr)	Event	Evidence Source
2004-08-27 10:12:35 CDT	NETSTUMBLER.EXE-0BFEE568 Net stumbler is run installed, a packet sniffing software.	Dell Latitude Cpi.E01
2004-08-27 10:31:17 CDT	RUNDLL32.EXE-16B6BC1C Rundull32 is run, allows for a user to detect other networks for interference.	Dell Latitude Cpi.E01
2004-08-27 10:33:03 CDT	CAIN.EXE-23D61279.pf Cain.exe is run, allowing a user to record inputs and manipulation programs.	Dell Latitude Cpi.E01
2004-08-27 10:34:54 CDT	ETHEREAL.EXE-1C148EEF Ethereal is run, allows a user to view traffic flow of packets.	Dell Latitude Cpi.E01
2004-08-27 10:46:27	Computer was shut down for the last time by Mr. Evil	Dell Latitude Cpi.E01

RELEVANT FINDINGS

The Dell Latitude Cpi has metadata identifying the registered owner of Greg Schardt attached to it. The device has 6 users but the main user on the device has the name “Mr. Evil” attached to it.

A plethora of suspicious software was found on the laptop. Every single one of these programs listed below were run at least once in the past week leading up until the discovery of the laptop. The computer contained password cracking software on it along with other notable hacker tools. A file identified as “biglist” contained 2,856,700 passwords used for cracking passwords. Malware identified as a “ZipBomb” was identified on the device.

Suspicious Software Found:

- **123Wasp** -> Will displays all passwords of the currently logged on user that are sotred in the Microsoft PWL file
- **Anonymizer** -> A Virtual Private Network that hides user Internet Protocol addresses with the help of online servers.

- **Cain** -> Cain.exe can record keyboard and mouse inputs, monitor applications and manipulate other programs.
- **Ethereal** -> Ethereal (Wireshark) is a popular network protocol analyzer and it is free software without licensing fees. Ethereal is used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education.
- **Look@Lan** -> is an advanced network monitor that allows you to monitor your network in a few clicks.
- **Rundull32** -> is a process registered as a backdoor vulnerability which may be installed for malicious purposes by an attacker allowing access to your computer from remote locations, stealing passwords
- **NetStumbler** -> It helps detect other networks that may cause interference to your network, and is generally used for war driving purposes by attackers.

Malware Found:

- **ZipBomb** -> Opening a file labeled as a decompression bomb will cause the system to instantly hang, ultimately crashing and causing data loss.

Chat logs in the folder path "/Program Files/mIRC/logs" contain chat logs between hacking individuals. Pornography was discussed and discovered in the chat.

SUPPORTING DETAILS

Since Gregg Schardt is the registered owner and Mr. Evil is the main account, we can assume that Greg Schardt and Mr. Evil are the same person.

The use of password stealing software and malware, indicates that the owner has strong knowledge of cybersecurity skills. The timing of when the software was run last in correlation to the timing of getting caught, is a strong indicator of malicious intent.

Mr. Evil's search histories of "Maktoob" and "Mosnews" have the potential to have international ties.

INVESTIGATIVE LEADS

There is enough evidence to prove that Mr. Greg Schardt is indeed Mr. Evil and is the owner of the laptop. Given the malicious software and malware that was installed onto the device, it can be assumed that Mr. Schardt is very proficient in cyber security and had malicious intentions.

Authorities should be contacted as there is enough incriminating evidence to prove that he had password cracking software which was in use when the perpetrator was caught. Mr. Schardt should be brought in for questioning and questioning to why he was trespassing on the property.

Security should be ramped up in the company and cybersecurity training should be emphasized to prevent further attacks from happening in the future. Individuals should not be able to just walk into the building.