CHAPTER 1

Case Scenario

An alarming trend is on the rise within educational environments, characterized by trends in Bitcoin-related extortion schemes. These scams articulated in Filipino, deliver ominous messages outlining the use of advanced malware capable of bypassing the victim's antivirus software, thereby gaining control over their computer and webcam. The extortionist takes it a step further, claiming the ability to access potentially compromising videos involving the victim. Non-compliance with the demand to transfer funds to the scammer's Bitcoin wallet carries severe consequences: the imminent threat of public exposure. If the victim fails to meet the specified 48-hour deadline, the perpetrator pledges to publicize the alleged footage across the victim's network of contacts, intensifying the potential harm inflicted by this intimidating tactic.

Type of Attack

The current criminal activity under inspection manifests as a form of ransomware assault: a malicious software crafted explicitly to obstruct access to computer files. Operating as a cyber threat, ransomware holds individuals or organizations hostage by encrypting their data, rendering it inaccessible. Subsequently, victims find themselves in a predicament where paying the ransom emerges as the most direct and economically viable route to reclaiming access to their files. This insidious tactic involves encrypting crucial data and demanding payment in exchange for the decryption key, exploiting the urgency and desperation of those affected.

Perpetrators of such schemes often employ alarming tactics within their messages, intending to unsettle and coerce individuals into complying with their demands. Complying to these

pressures, victims may feel compelled to submit to the ransom demands. Nevertheless, it is crucial to underscore the significance of vigilance and caution. Responding to unsolicited emails, often the initial point of entry for such schemes is strongly discouraged. An initiative-taking approach, involving awareness of these fraudulent methods and a refusal to engage with unexpected or suspicious correspondence, is advised to mitigate the risk of falling victim to these scams.

Systematic Procedures Taken

1. What procedure are you going to perform in this instance?

In this instance, the following procedure would be undertaken:

1. Acquisition of Search Warrant
    - Initiate the process by obtaining a search warrant, a crucial legal step for the lawful seizure of evidence to be presented in court.
2. Crime Scene Examination:
    - Conduct a meticulous examination of the crime scene, necessitating isolation and thorough documentation. In digital forensics, isolation involves disconnecting computers from networks to prevent further data compromise or leaks. It is imperative to refrain from using these devices to prevent potential evidence tampering or destruction.
3. Documentation of Physical and Digital Environments
    - Upon seizing physical evidence, meticulously document both the physical and digital environments, highlighting potential evidential elements. This documentation should

include capturing threatening messages, emails, blackmail demands, and relevant digital evidence.

4. Digital Evidence Gathering:
    - Gather necessary digital evidence, focusing on capturing running memory and creating storage device images. This can be achieved using forensic tools such as Access Data FTK (Forensic Toolkit).
5. Preservation of System Data:
    - Preserve the data on the affected systems, ensuring the integrity of the evidence. This involves capturing running memory and creating images of storage devices.

By following these steps, the investigation aims to legally acquire and preserve crucial evidence, both physical and digital, to build a comprehensive case for further analysis and potential legal proceedings.

2. As a Forensic Investigator, perform the steps in digital forensics.

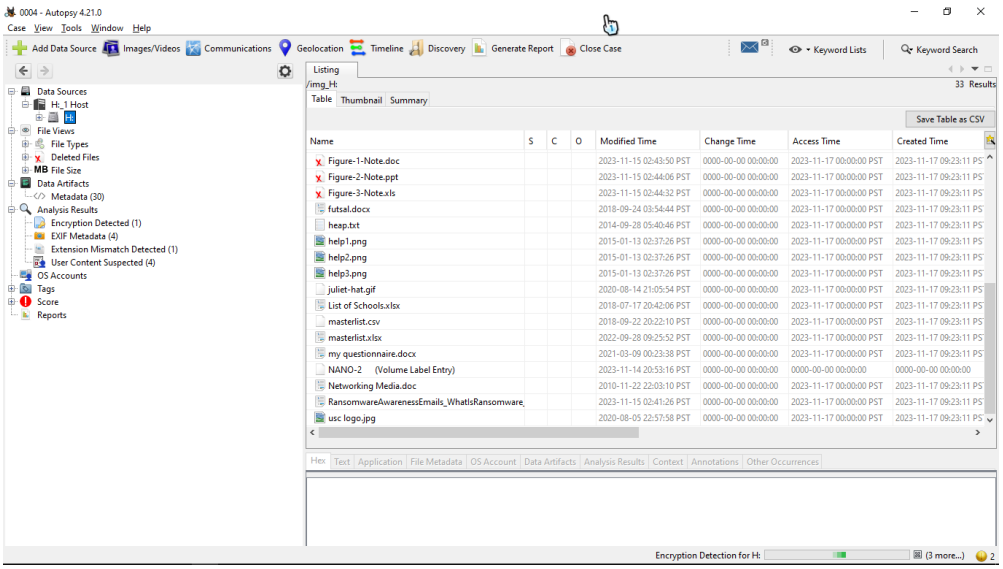
1. Identification
    - Determine the potential evidence items in the crime scene for building up data against the suspect and eventually defining the scope of the investigation.
2. Acquisition/Imaging
    - Once potential evidence items are identified, proceed with their acquisition to create images for analysis. Ensure that the original sources remain untouched, preserving their integrity. Establish and maintain a clear chain of custody to safeguard the evidence.
3. Analysis

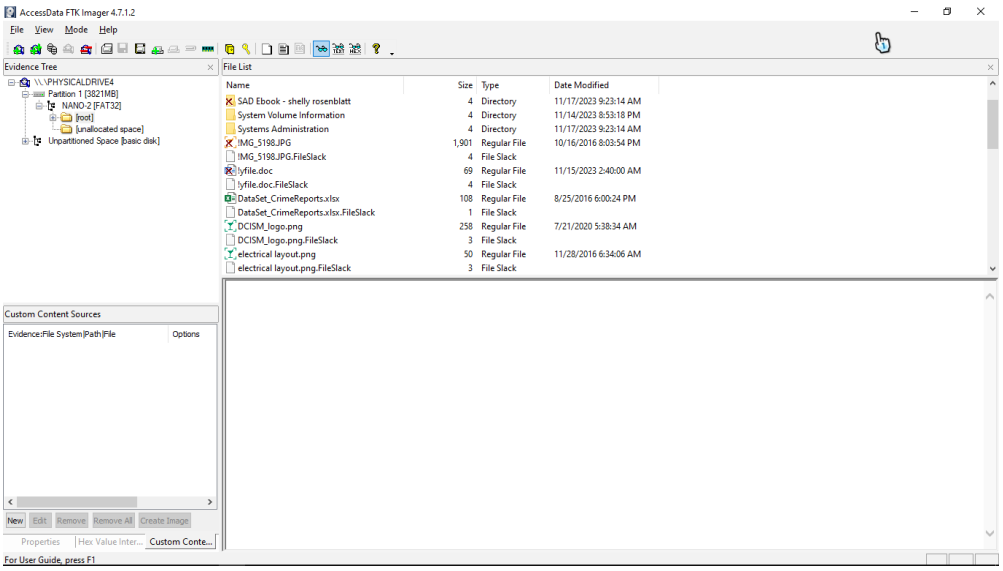
- Conduct a meticulous analysis of the collected data. This involves:
    - Examining the captured memory of devices.
    - Analyzing the images/copies, including hashing to verify integrity.
    - Identifying hidden, deleted, or altered files.
    - Analyzing network, webcam, communication, and other logs.
    - Scrutinizing metadata and timestamps to determine the creation, modification, or deletion of files.
    - Investigating the Bitcoin wallet address, examining transaction history, and identifying patterns or connections to criminal activities.

4. Reporting
    - Compile a comprehensive report detailing the results, methods, and conclusions of the investigation. Provide a thorough account of the analytical process and present the evidence in a manner that supports the investigation's findings.
5. Presentation to Court
    - Prepare the evidence, documents, and reports, then ensure that the evidence gathered is properly documented and that a chain of custody is maintained to ensure its admissibility in court.

3. Analysis should be thorough. What did you do?

- The tools Windows File Explorer, Access Data FTK, and Autopsy are utilized.





CHAPTER 2

Evidence Listed

The following evidence found from the crime was discovered and labeled as the source drive: Imation Nano USB Device, measured in Megabytes is 3720 MB, 1.5 inches long, 0.5 inches wide, and 0.25 inches thick. AccessData FTK and Autopsy were utilized to further analyze the present evidence to view the modifications made on the USB through Imaging.

1. **Destination Location (where the image was stored for analysis)**
    - C:\Users\kynee\Documents\Cases\Images
2. **Target Filename**
    - C:\Users\kynee\Documents\Cases\Images\0004.001
    - C:\Users\kynee\Documents\Cases\Images\0004.002
    - C:\Users\kynee\Documents\Cases\Images\0004.003
3. **Estimated time to finish developing the image**
    - 4:54
4. **Hash Value MD5**
    - 811b120d0d67e4eec2374b8ef6ed9979
5. **Hash Value SHA1**
    - 40cd7cc5632220f3ca6e18675e63e38f42d4b2d4

CHAPTER 3

Evidence Analysis

Disk Analysis

1. File Count in Source Drive – 64
2. File Count in Target Image – 151 (includes file slacks)
3. Folder Count in Source Drive – 3 initial folders
4. Folder Count in the Target Image – 4 folders
5. Deleted File Count – 20 (including the files inside the deleted folder)
6. Deleted Folder Count – 1 folder
7. Hidden folders and data are not found.

Data Recovery

1. After extracting the deleted files from the root folder,
    - 5 files were extracted.
2. After extracting the deleted folder
    - 1 folder was extracted named “SAD Ebook - shelly rosenblatt”, containing 15 pdf files.

Data Analysis

1. After thorough examination
    - 38 JPEG files were found
    - 5 PNG files were found
    - 7 doc files were found.

2. JPEG and PNG have the following digital signatures:
    - JPEG - `FF D8 FF E0 / ÿØÿà`
    - PNG - `50 4E 47 / PNG`
3. Based on those given digital signatures, it has been found that the following files have been altered:
    - 1 jpeg file → doc file
    - 1 PNG file → doc file
    - 2 png files → XLS file
    - 1 PNG from unallocated space
4. After recovering the original files
    - 39 JPEG files
    - 10 PNG files

CHAPTER 4

Detected Extension Mismatch

Upon post-analysis, it is revealed that out of the scrutinized files, 5 showcased contents intricately linked to the ransomware attack. Interestingly, the suspects endeavored to conceal their involvement by resorting to tactics such as deletion and modification of the file formats.

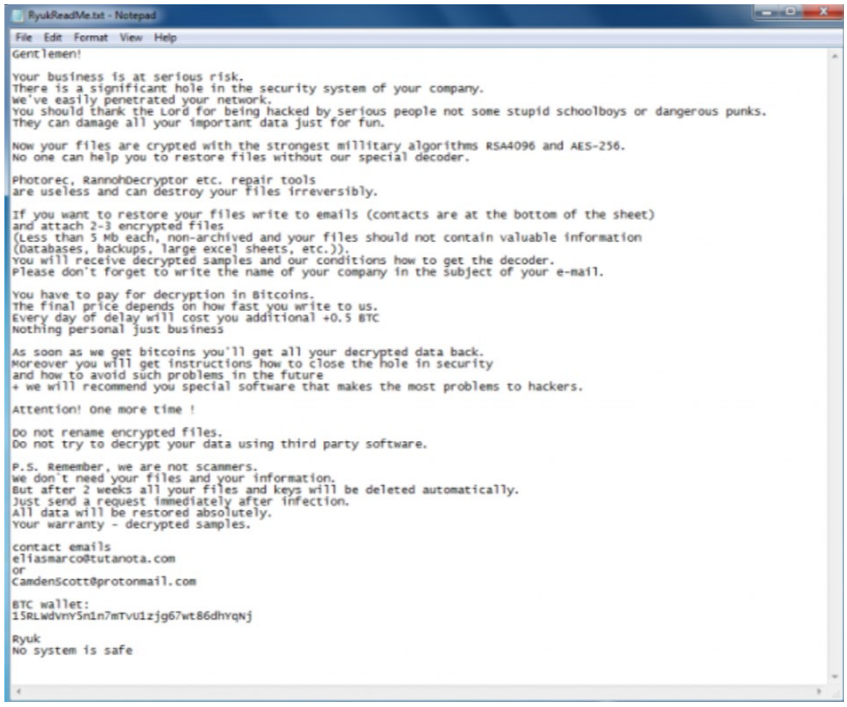
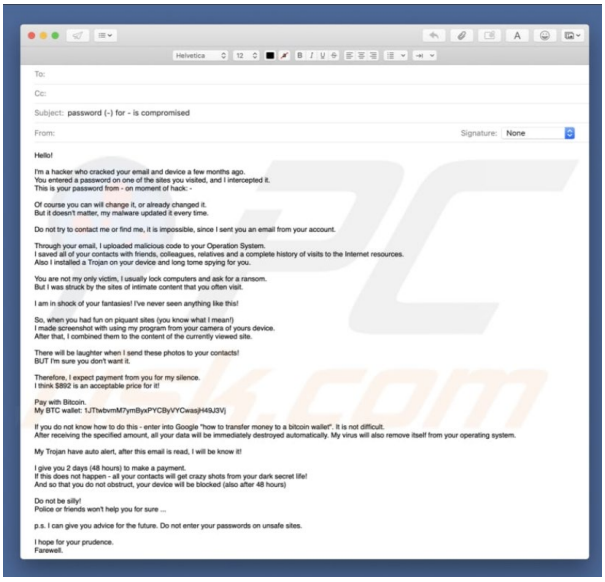


Figure-2-Note.png

The image file "Note.png" unveils threatening communication wherein the suspect explicitly acknowledges their involvement in an extortion scheme with a victim. The message explicitly states the act of holding the victim's files hostage for ransom. The content outlines a demand for payment in Bitcoins as a condition for decrypting the files, coupled with a menacing warning of permanent deletion should the victim fail to comply. The perpetrator goes further by threatening irreversible file deletion in the event of the victim attempting independent decryption or exhibiting any delay in cooperation.

Moreover, the message includes a set of instructions for the victim to follow in order to comply with the demands. This includes specific contact details and a designated Bitcoin wallet address for the ransom payment, providing a clear roadmap for the victim to adhere to in their response to the extortion attempt.



To:

Cc:

Subject: password (-) for - is compromised

From: Signature: None

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from - on moment of hack: -

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.

I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!)
I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.

There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence.
I think $892 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: 1JTtwbvmM7ymBysPYCByVYCwasjH49JJ3Vj

If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult.
After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove itself from your operating system.

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

I hope for your prudence.
Farewell.

myfile.doc

The image file "myfile.jpeg" depicts a disturbing scene wherein the perpetrator is shown actively hacking the victim's password, gaining unauthorized access to sensitive information such as contacts and internet history. Subsequently, the perpetrator exploits this unauthorized access for blackmail, demanding a payment of $892 in Bitcoins to maintain silence. This includes a threat to disseminate the victim's files if the specified amount is not paid within a two-day timeframe. This malicious act is a clear attempt to intimidate the victim through the compromise of their personal information and underscores the severity of the blackmailing scheme.

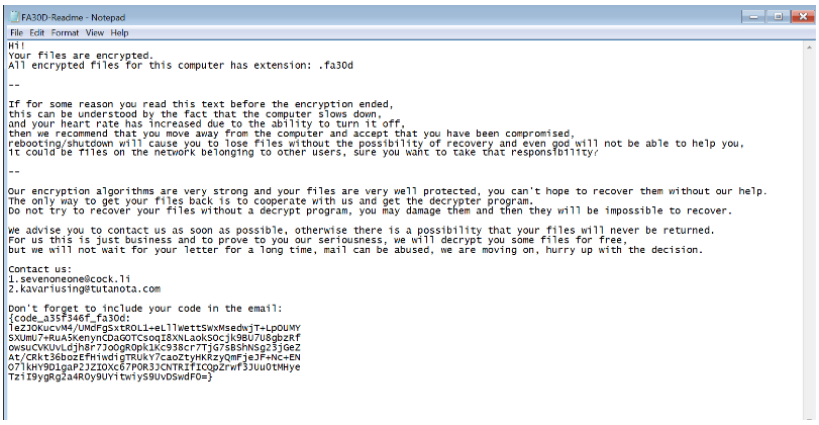
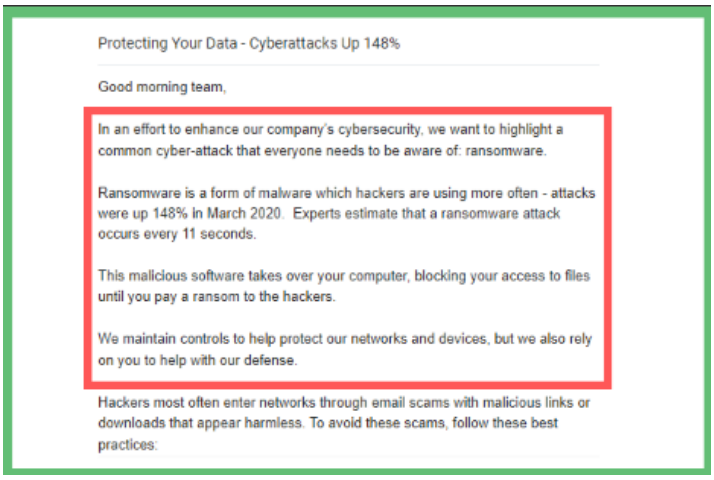


Figure-1-Note.doc

The image labeled "Figure-1-Note.png" portrays a message from the suspect to an extortion victim. The message explicitly communicates the suspect's ransom demand for the victim's files, emphasizing the importance of cooperation for their safe return. It cautions against various actions such as attempting to shut down the computer, self-decrypting the files, or delaying cooperation, with a chilling threat of permanent file deletion as consequence. Furthermore, the perpetrator includes contact information, for further communication related to the extortion scheme. This image serves as a stark representation of the coercive tactics employed by the suspect in their attempt to extort the victim.



RansomwareAwarenessEmails_WhatIsRansomware_1221.xls

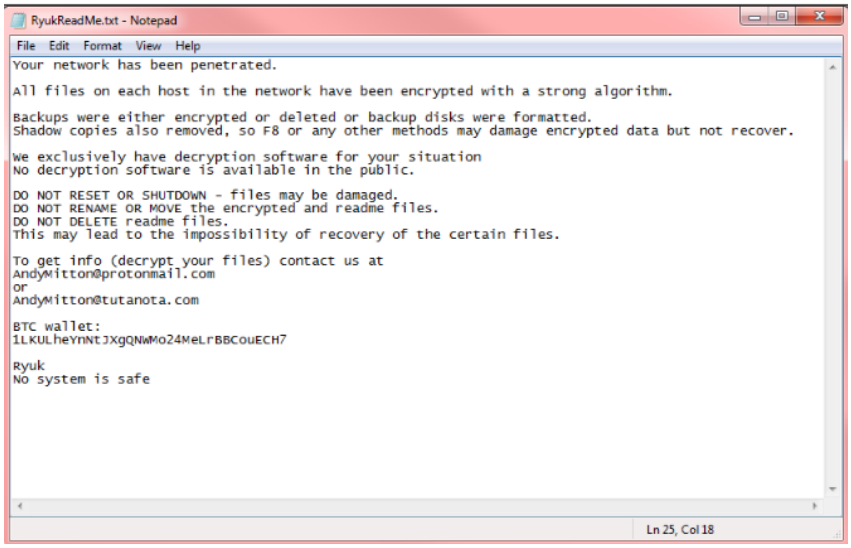


Figure-3-Notes.xls

The image labeled "Figure-3-Note.png" portrays a message from the suspect to an extortion victim, providing explicit details about the ransom demand for the victim's files. The message emphasizes the necessity of a Bitcoin payment for the decryption of files, thereby averting permanent deletion. It issues a unambiguous warning of increasing ransom prices in the event of delayed payment and threatens irreversible file deletion if the victim attempts to shut down the computer, decrypt the files independently, or delays cooperation. Additionally, the perpetrator includes contact details and a Bitcoin wallet address, for facilitating the required transaction. This image serves as a tangible representation of the suspect's coercive tactics and the specific conditions imposed upon the victim in this extortion scenario.

Image Summary (Using Access FTK)

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 0004-11-18-2023
Evidence Number: 0004
Unique description: Ransomware
Examiner: Kyne Sia
Notes: Ransomware

---------------------------------------------------------------

Information for C:\Users\kynee\Documents\Cases\Images\0004:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 487
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 7,827,456
[Physical Drive Information]
 Drive Model: Imation Nano USB Device
 Drive Serial Number: 078415351879
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 3822 MB
 Sector count:    7827456
[Computed Hashes]
 MD5 checksum:    811b120d0d67e4eec2374b8ef6ed9979
 SHA1 checksum:   40cd7cc5632220f3ca6e18675e63e38f42d4b2d4

Image Information:
 Acquisition started:   Sat Nov 18 22:26:35 2023
 Acquisition finished:  Sat Nov 18 22:31:29 2023
 Segment list:
  C:\Users\kynee\Documents\Cases\Images\0004.001
  C:\Users\kynee\Documents\Cases\Images\0004.002
  C:\Users\kynee\Documents\Cases\Images\0004.003

Image Verification Results:
 Verification started:  Sat Nov 18 22:31:32 2023
 Verification finished: Sat Nov 18 22:32:01 2023
 MD5 checksum:    811b120d0d67e4eec2374b8ef6ed9979 : verified
 SHA1 checksum:   40cd7cc5632220f3ca6e18675e63e38f42d4b2d4 : verified
```

CHAPTER 5

CONCLUSION AND FINDINGS

Upon careful examination of the evidence, it became clear that about five files were unmistakably linked to the ransomware attack. In an initial attempt to obscure their connection, the suspects manipulated file formats, deleting some and modifying others. However, meticulous data analysis successfully unraveled these efforts, laying bare the original files through their digital signatures. Remarkably, these files turned out to be screenshots of ransom notes written in the Windows application "Notepad".

Contained within these screenshots was a ominous message detailed earlier, written narrative accounts of how the perpetrator employed malware in order to seize control of the victim's computer and webcam and bypassing antivirus software in the process. The evidence overwhelmingly substantiates the occurrence of a ransomware attack, where the victim is coerced with the threat of data exposure unless a specific amount of cryptocurrency is surrendered. These threats, notably unrefined, directly emanate from personal emails such as CamdenScott@protonmail.com and eliasmarco@tutanota.com. Noteworthy examples of these threats involve the implementation of encryption algorithms, namely RSA4096 and AES-256.

Drawing from this compelling evidence, it is to be asserted the culpability of the suspect in orchestrating the ransomware attack. The files, coupled with their content and the broader context of the crime, compellingly point towards the suspect's active involvement in this illicit activity.