INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment II

Ransomware on Halloween

2018/2019

nuno.m.santos@tecnico.ulisboa.pt

Introduction

This assignment is about solving a case named "Ransomware on Halloween". This exercise will help you develop your skills on the topics of memory and file system analysis, among other digital forensics techniques. The files that you need to examine can be downloaded from the course website. As in the previous exercises, we recommend you to use the Kali Linux distribution running on a forensically sound virtual machine in order to perform your analysis.

Scenario presentation

Sally Jones is a PhD student working on molecular biology. Her research is about finding a cure for a specific type of cancer. A couple of days after the Halloween day in 2018, while she was intensely working on her next paper submission (which was due in less than a week), a pop-up window has suddenly appeared on her laptop's screen displaying the following chilling message:

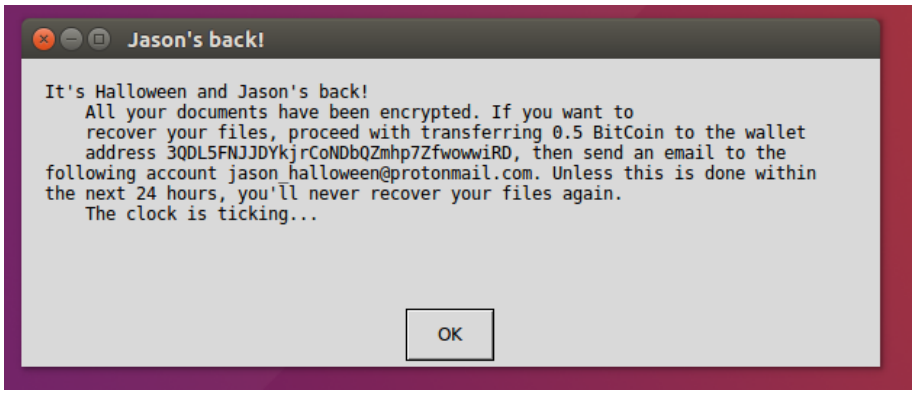

Figure 1: Pop-up window displaying ransomware message.

All of her precious work encrypted and potentially lost? She couldn't believe what was happening! To check if this message was for real, she opened a terminal and listed the folders where she kept images of human cancer cells, along with the main draft of her paper. In the list, she confirmed the existence of the original filenames along with a set of new files named after the original filenames with an extra prefix *".encrypted"*, as shown in the figure below.

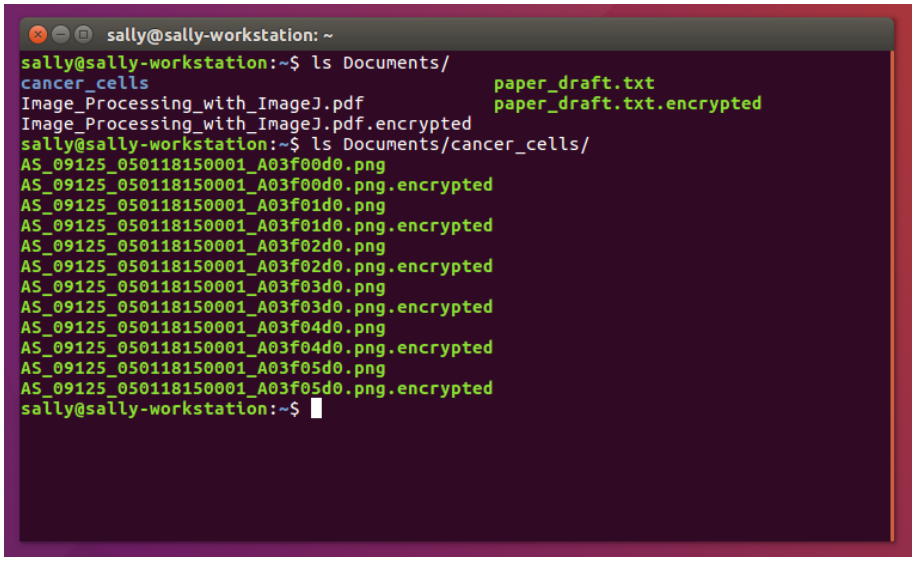

Figure 2: List of encrypted images inside folder `cancer_images`.

She opened the original files and all she could see was the text message: "Jason's back!" Sally then tried to open a few files with extension *".encrypted"* and confirmed that their contents seemed to have been encrypted. Sally had no money to pay for that ransom, and even if she had, what guarantees could she obtain that the attacker would restore her files? Unfortunately, she had no backups of her files...

In order to get help, she hired a forensic analyst by the name of Ted Silver who told her immediately, on the phone, to stop making any changes to her computer. In particular, he told her to leave the pop-up message open and to not power down or suspend her laptop. Ted visited Sally, interviewed her, and collected several digital artifacts for further analysis in the lab. These are the facts he was able to learn:

- The targeted files were located in the Documents's folder of her home directory: `/home/sally/Documents`. Inside this folder she kept one directory with images of human cancer cells (`cancer_images`), a text file for writing the draft of her paper (`paper_draft.txt`), and a `.pdf` file related to ImageJ (`Image_Processing_With_ImageJ.pdf`) containing instructions on how to visually analyze her images. The original resolution for each image is 512×512.
- Upon asking Sally to describe what kind of actions she has performed over the day, she said: "I came up to the lab and did my usual things, browsed the web, checked my email, and worked on my paper. Today I needed to use a program that allows me to count and measure the size of organelles with cells. I asked a lab colleague for an advice, and he suggested me the ImageJ software, which I've downloaded from the Internet onto my laptop. I tried ImageJ on my laptop and checked that it works. Eventually, I was editing my paper, and that's when it happened."

Based on these facts, Ted decided to extract the following artifacts and take them to the lab:

File	**MD5**	**Description**
sally_disk	`382c7ae1e99380601ec3bffbe762f60d`	A forensic image of Sally's hard drive.
sally_mem	`8864691bed9d3712894ea0eff8f21f2e`	A memory dump of Sally's computer.

You may obtain the above files by downloading and extracting the data found in the following locations. These artifacts may also be downloaded from the course's webpage.

- `http://turbina.gsd.inesc-id.pt/csf1819/sally_disk.tar.gz`
- `http://turbina.gsd.inesc-id.pt/csf1819/sally_mem.tar.gz`

Your job is to analyze the digital artifacts extracted by Ted, and answer the following four questions. Justify your answers by providing all the relevant evidence you can find. Make sure to explain your hypotheses and how you have proceeded to validate them.

1. Can you determine how the malware has taken over Sally's computer?
2. Can you recover Sally's original files? If you do not succeed at retrieving the original files, can you at least extract some of their fragments?
3. What can you tell about the identity of the attacker?
4. Elaborate a timeline of the most significant events of the case.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is November 23^{th}. Until then, you must upload to Fenix a compressed zip file containing three deliverables:

- **Digital Forensic Report**: A document in which you answer the aforementioned questions. You must identify all relevant evidentiary items that support your claims. We recommend you to use the template that can be downloaded from the course website.
- **Evidence Artifacts:** All relevant evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and MD5 values are indicated in the report.
- **Auxiliary Items:** Programs, scripts, and additional documents that you have produced during the investigation which are important to justify your results must also be included.

TIPS: The cryptographic algorithm used by the malware was AES in `AES_CTR_MODE` with a 128 bit key size. The initial value for the AES counter corresponds to the first 128 bits of each encrypted file. Use the Volatility profile available in `http://turbina.gsd.inesc-id.pt/csf1819/Ubuntu160405.zip` to help parse the memory dump.

Good luck!