GENERAL CONFEDERATION OF LABOR OF VIETNAM

**TON DUC THANG UNIVERSITY**

**FACULTY OF INFORMATION TECHNOLOGY**



**THE MIDTERM REPORT Na**

Instructing Lecturer: **PhD HUYNH NGOC TU**

Student’s Name: **NGUYEN DUC TOAN – 520H0690**

**NGUYEN DONG HUNG – 520H0535**

Class**: 20H50304 – 20H50301**

Course**: 24**

**HO CHI MINH CITY, 2022**

GENERAL CONFEDERATION OF LABOR OF VIETNAM

**TON DUC THANG UNIVERSITY**

**FACULTY OF INFORMATION TECHNOLOGY**



**THE MIDTERM REPORT OF INFORMATION SECURITY**

Instructing Lecturer: **PhD HUYNH NGOC TU**

Student’s Name: **NGUYEN DUC TOAN – 520H0690**

**NGUYEN DONG HUNG – 520H0535**

Class**: 20H50304 – 20H50301**

Course**: 24**

**HO CHI MINH CITY, 2022**

# THE REPORT WAS COMPLETED AT TON DUC THANG UNIVERSITY

We pledge that this is a product of our own project under the guidance of PhD Nguyen Thanh Phuoc. The content of research, results in this subject is honest and not published in any form before. The data in the tables used for the analysis, comment, and evaluation were collected by the authors themselves from various sources indicated in the reference section.

In addition, many comments and assessments as well as data from other authors and organizations have been used in the project, with references and annotations.

**If any fraud is found, I am fully responsible for the content of my report.** Ton Duc Thang University is not involved in any copyright infringement or copyright infringement in the course of implementation (if any).

*Ho Chi Minh, October 15th 2022*

*Author*

*(sign and write full name)*

*Nguyễn Đức Toàn*

*Nguyễn Đồng Hưng*

*Trương Quang Khôi*

EVALUATION OF INSTRUCTING LECTURER

**Confirmation of the instructor**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ho Chi Minh City, 2022

(sign and write full name)

**The assessment of the teacher marked**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ho Chi Minh City, 2022

(sign and write full name)

# SUMMARY

# TABLE CONTENT

[THE REPORT WAS COMPLETED AT TON DUC THANG UNIVERSITY I](#_Toc118117828)

[SUMMARY III](#_Toc118117829)

[TABLE CONTENT IV](#_Toc118117830)

[TABLE OF FIGURES, GRAPHS, TABLES V](#_Toc118117831)

[CHAPTER 1: SEARCH OVERVIEW 1](#_Toc118117832)

[1.1. What is search overview? 1](#_Toc118117833)

[1.2. What is SearchView? 1](#_Toc118117834)

[1.3. Creating a Search Interface 2](#_Toc118117835)

[1.4. Adding Recent Query Suggestions 2](#_Toc118117836)

[1.5. Adding Custom Suggestions 3](#_Toc118117837)

[CHAPTER 2: COPY AND PASTE 7](#_Toc118117838)

[CHAPTER 3: DRAG AND DROP 11](#_Toc118117839)

[3.1. Overview 11](#_Toc118117840)

[3.2. Drag and Drop Operation 15](#_Toc118117841)

[CHAPTER 4: CREATE BACKWARD-COMPATIBLE Uis 18](#_Toc118117842)

[4.1. Overview 18](#_Toc118117843)

[4.2. Abstract the new APIs 18](#_Toc118117844)

[4.3. Proxy to the new APIs 20](#_Toc118117845)

[4.4. Create an implementation with older APIs 21](#_Toc118117846)

[4.5. Use the version-aware component 22](#_Toc118117847)

[CHAPTER 5: CONTROL EXTERNAL DEVICES 25](#_Toc118117848)

[CHAPTER 6: REFERENCES 29](#_Toc118117849)

# TABLE OF FIGURES, GRAPHS, TABLES

**FIGURES:**

# CHAPTER 1: INTRODUCTION

1. What is Ransomware?

Ransomware is an encrypted virus, considered by the US Department of Justice as a modern model of cybercrime with the risk of damaging global networks. When ransomware infects a computer, it encrypts or blocks access to data on the disk. To return to normal operation, users must transfer money to the account to remove the ransomware.

Source

## 2. The Origin

### 2.1 Formation stage

Ransomware was discovered in Russia in 2005-2006. In the first stage, the ransomware takes the form of the variant TROJ\_CRYZIP.A. Data analysts discovered that when this Trojan variant entered the machine, the data was immediately encrypted, requiring a password to access it again. And to get the password, the data owner is required to pay $300.

### 2.2 Development direction

Over time, Ransomware expands its scope, eating text files, spreadsheets with extensions such as \*.doc, \*.xl, \*.exe, ...

In 2011, the world information world recorded the appearance of another form of Ransomware called SMS Ransomware. In addition to the usual features, SMS Ransomware also sends a message that requires users to contact the hacker via the provided phone number until the money is transferred as requested.

In addition, another version of Ransomware also stormed when it attacked the MBR of the host operating system. In other words, it will render the operating system inoperable.  
Graphical user interface, text

Description automatically generated

**The ability of ransomware to spread**

First appeared in Russia, but within a short time, the virus spread throughout Europe. The peak was in 2012, a large number of ransomware attacks were recorded in Europe and also in the US and Canada. By now, Ransomware can appear anywhere in the world.

Classify

### 3.1 Locker ransomware

Locker ransomware is also known as Non-encrypting ransomware. This type of software does not encrypt files, but instead completely blocks users from accessing the device. For example, a computer infected with locker ransomware will not be able to do anything but turn it on and off. On the machine screen, a message will appear on how to send money to return the device to normal.

### 3.2 . Crypto Ransomware

Crypto Ransomware or Encrypting Ransomware is the most common type of ransomware. They encrypt data files by secretly connecting to the hacker's server, generating a key to encrypt and renaming the files. At the same time, these hackers will send ransom notices to the machine and sometimes even create time pressure for the victim. If you do not pay within the specified time, the file may be upgraded to encryption, adversely affecting the data.

### 3.3 Other types of danger

Currently, people have recorded many strains of ransomware with different levels of danger. Of the known types of ransomware, the three most dangerous are WannaCry, CryptoLocker, and Petya. In addition, other names that can harm your computer include Locky, TeslaCrypt, ...

## 4. Distinguish Ransomware from normal software.

### 4.1 Differences

Ransomware or other malicious malware usually have in common that they do everything to hide and destroy files silently. However, the big difference of ransomware is the extremely complex encryption mechanism. These encryptions pave the way for malware to infiltrate data files, overcoming even the barriers created by anti-virus software. However, anti-virus software is also gradually becoming more "sensitive" to ransomware.

### 4.2 Ransomware method of ransomware

Ransomware is equipped by hackers with many "hidden" algorithms, the most common are the following:

* Detection: This is the method of reconnaissance. Malware will scan the environment for the risk that they are in a virtualized environment and evade detection by security researchers. But in return, this method makes it impossible for them to generate an up-to-date security signature.
* Timing: Everything can't be perfect and neither can anti-virus software. Despite constantly issuing warnings, they are still difficult to protect every aspect of the system, especially in the face of dangerous viruses like ransomware. Ransomware will take advantage of the time when the device is on / off, when the anti-virus software has not started yet.
* Communication: When infiltrating the data file, the ransomware will immediately contact the command machine (C&C server) to receive instructions. But anti-virus software can take advantage of this feature to detect specific IP addresses and block those communications.
* False Operation: When a computer is infected with ransomware, a fake program may appear. Unskilled users will mistake this as a normal program of the operating system and follow their instructions, causing viruses to spread faster.

## 5. How to prevent ransomware

Until now, ransomware is still very difficult to remove. Therefore, to save a lot of time and effort, you should protect your data as a prerequisite.

If you want to prevent ransomware, you can apply some of the following ways:

* Do not use free wifi networks, the origin is not clear.
* Limit clicking on strange links, unknown email addresses.
* Regularly back up data, install anti-virus software and regularly update.
* Change the default password on all access points.
* Create multiple barriers on your networks.
* Have a recovery plan in case of data loss.

## 6. What to do when infected with ransomware?

In case of being infected with Ransomware, take the following steps:

* Step 1: Isolate and separate the network and system: isolate the infected part from the system, turn off those systems, unplug the network to prevent the virus from spreading.
* Step 2: Identify and remove the ransomware: Try to find the malicious parts that are infecting the machine, identify the strain and plan to remove them.
* Step 3: Erase infected machine and restore from backup: In case ransomware remains, delete all infected data and restore from scratch via backups.
* Step 4: Analyze and monitor the system: After completely removing the ransomware, you should sit back and analyze the infection factors to have the right way to protect your data.

If not, you can prepare in advance in case of data backup, you can wipe the data in the device and reinstall them.

If more than you have data but still don't have a backup, then you have to accept data loss and delete, reinstall your computer or pay a hacker to get the data back.

# CHAPTER 6: REFERENCES

Website check file exits virus

<https://www.virustotal.com/gui/home/upload>

Website tool decryption ransomware

<https://www.nomoreransom.org/en/decryption-tools.html>

<https://www.emsisoft.com/en/ransomware-decryption/>

<https://www.canauri.com/landing-pages/download-your-ransomware-prevention-checklist/>