**VIETNAM NATIONAL UNIVERSITY - HO CHI MINH CITY**

**UNIVERSITY OF INFORMATION TECHNOLOGY**

**FACULTY OF COMPUTER NETWORK AND COMMUNICATION**

**LÊ THANH BÌNH**

**CHÂU THIỆN HƯNG**

**THESIS REPORT**

**STUDY MALICIOUS BEHAVIOR ANALYSIS METHODS TO DETECT SECURITY RISKS ON WINDOWS**

**BACHELOR OF ENGINEERING INFORMATION SECURITY**

**HỒ CHÍ MINH CITY, 2017**

**VIETNAM NATIONAL UNIVERSITY - HO CHI MINH CITY**

**UNIVERSITY OF INFORMATION TECHNOLOGY**

**FACULTY OF COMPUTER NETWORK AND COMMUNICATION**

**LÊ THANH BÌNH**

**CHÂU THIỆN HƯNG**

**THESIS REPORT**

**STUDY** **MALICIOUS BEHAVIOR ANALYSIS METHODS TO DETECT SECURITY RISKS ON WINDOWS**

**BACHELOR OF ENGINEERING INFORMATION SECURITY**

**Instructor**

**PhD. NGUYỄN ANH TUẤN**

**HỒ CHÍ MINH CITY, 2017**

# **DANH SÁCH HỘI ĐỒNG BẢO VỆ KHÓA LUẬN**

Hội đồng chấm khóa luận tốt nghiệp, thành lập theo Quyết định số

…………………… ngày ………………….. của Hiệu trưởng Trường Đại học Công nghệ Thông tin.

1. …………………………………………… - Chủ tịch
2. …………………………………………… - Thư ký
3. …………………………………………… - Ủy viên
4. …………………………………………… - Ủy viên

# **COMMENT OF INSTRUCTOR**

# **COMMENT OF REVIEWER**

# **ACKNOWLEDGEMENT**

With supports and helps of many individuals, this thesis has become reality. We would like to express our appreciation to all of them. First of all, we would like to thank not only teachers in faculty of computer network and communications but also teachers in University of Information Technology who have taught us very useful lectures with all of their passion, which provide necessary knowledge for us to finish this thesis. Especially, we would like to express our appreciation to professor Nguyen Anh Tuan, our instructor, who has inspired and guided us to dive deeply into information security with this thesis. Secondly, we would like to thank our friends who has helped, supported and exchanged knowledge with us since we started studying at University of Information Technology. Finally, we would like to thank our family for supporting us during the time we develop this project.

**ABSTRACT**

We have developed a malicious behavior analysis solution for Windows Operation System called APTIDS, which is an open source solution combined of a System Monitoring Software, a Distributed Log Collector Hardware and a Centralized Log Storage on Cloud. Just like OSSEC [1] and others well know open source host IDS, the software agent of APTIDS has abilities to monitor some common sectors of Windows OS like Registry, Service. Furthermore, we have developed an ability to allow APTIDS to send collected logs to the Collector Hardware, which is a Log Collector built on a Raspberry Pi, and from that hardware another collector will push all the collected log to the centralized log storage on cloud. APTIDS can monitor and alert on its runtime, that means if any malicious activity takes place at where APTIDS is monitoring, APTIDS will capture that activity, write log, and alert to the log storage.

# INTRODUCTION

## Motivation

Nowadays, with the rapid advance and wide spread of modern threats, computer users are facing threats from everywhere. From the most complicated malwares those can transform themselves to create many variants, to those that encrypt the whole computer and keep our information as hostage. For fighting back those advanced threats that are terrorizing the Internet, many company have developed antivirus softwares. To protect the innocent Internet civilians from the cyberwar that are taking place, antivirus softwares come from a free price for basic protection, to some hundred dollars for full protection against most modern attack vectors. Personal Antivirus software is very powerful for protecting a normal user from many security threats. But their shortcoming is that they can only protect a single user at one, and if there are more than one user who want to be protected, they have to buy more than one AV software, install them separately and there is no way to monitor and manage logs from all those softwares simultaneously.

Enterprise Antivirus Systems come as a full qualified protection for big enterprise, campus or company. They support for monitoring and protecting hundreds of users, and manage their logs of activities in some central cloud storage systems. However, the price for such titanium protections are very expensive, and they are sophisticated for maintaining and operating and especially for protecting small companies or households.

From all those shortcomings of modern Antivirus Softwares amd Security Protection Systems, we want to develop a solution for helping small companies and households to protect themselves against advance threats.

## Thesis’ statement

Successfully develop and run APTIDS for monitoring malicious behaviors of software on Windows Operating Systems. APTIDS monitor registry and service for detecting softwares that are trying to write the path of their executable files.

Testing APTIDS by using some common malwares running in a controllable environment.

## Subject

Research on how malwares store themselves on Windows System for running on start up. In addition, research on how Graylog work, the method for collector logs and push them to SIEM for storage and analyzing.

## Scope

APTIDS can monitor activities in some factions of Registry and the creation and deletion of Windows Services. Since it has been developed in a limited time, it does not have full features like others well-known antivirus softwares.

## The needs of registry monitoring module

Malwares usually store the path lead to their executables in Registry in case the system has to be restarted, they can run with the start up. Monitoring the Registry allows us to capture any malicious activity and know what is happening in the Registry Hive.

## The needs of service monitoring module

Windows Service allows us to create a so call long-running executable, which can start automatically at system boot. Knowing that, malicious programs write entries in the Service Control Manager which help them to run their executables when system boot up.

## The needs of distributed log collector hardware

## the needs of centralized cloud log storage

# 