**Hsiang Lo**

**CS 370 Introduction to Security Week 9: Problem Set 9**

Instructor Name: Rakesh Bobba

# Introduction/Purpose

The purpose of this assignment is to help you work on the concepts of Malware covered in Week 9

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

* Malware: Viruses
* Malware: Worms
* Malware: Other

Chapter 6 from the reference book Stallings and Brown

# Instructions/Questions

Please answer the questions below.

## Malware

Q1 [5 pts] What is the difference between a metamorphic virus and a stealth virus? How are they similar?

The main difference between metamorphic virus and stealth virus is that metamorphic virus mutates with every infection that makes complete rewrite. Stealth virus on the other hand actively tries to hide all signs of its presence. It is capable of intercepting calls to read a file and return correct values about file sizes. They are similar in that they are both signatures avoiding viruses. This means they are both viruses, so they are both malicious software that replicates copies itself on to other programs when executed.

Q2 [5 pts] Traditionally, what is the difference between a Virus and a Worm? Can a malware exhibit the traits of both a Virus and a Worm?

The main difference between a virus and a worm is that a worm propagates from one computer to another, it is self-directed propagation. Virus is a malicious software that replicates/copies itself on to other programs when executed.

Worm propagates from an infected host such as choosing IP address, look around local areas for hosts, attachment through file or attachment to removable storage. Virus propagates by attaching itself to a program or to data by appending itself to files, integrate itself to program, integrate into data such as executable text, macro, scripting and email attachment.

Q3 [5 pts] What is a rootkit? Name two ways a kernel mode rootkit can change the

underlying system programs?

A rootkit is a sophisticated cloaking malware that can hide itself and enables an unauthorized user to gain control of a computer system without being detected.

With the kernel sits between individual applications and underlying hardware, kernel mode and user mode processes run at different level. Flow is similar to User Mode->System Libraries->System Call Table->Kernel where System Call Table is used to map the code branch for each system call inside kernel. Two ways a kernel rootkit can change the underlying system programs are

1. The attacker can use insmod to get a hold of the call table, and then map malicious instructions. So the flow would now be User Mode -> System Libraries -> Altered System Call Table. And then after inserting the malicious kernel code, the flow of control is now User Mode-> System Libraries->Altered System Call Table-> Evil Kernel Code.
2. They may also abuse SSDT and IDT functions calls to make changes at kernel-level.

Q4 [5 pts] What is difference between a polymorphic virus and an encrypted virus?

Polymorphic virus differs from encrypted virus in that polymorphic virus produces varying but operationally equivalent copies of itself. This means that it uses alternative but equivalent instructions and gets around signature scanners. while encrypted virus stores bulk of itself encrypted. This means that encrypted virus focuses on small decrypt routine in clear and having the key stored in the clear.

# Submission Details

Submit a PDF file with the questions and your corresponding answers

The assignment is worth 20 points. It is due Saturday of Week 9 at Midnight.