Malware analysis and design
Homework No. 3

Vincenzo Arceri VR386484
Giovanni Liboni VR387955
Alberto Marini

May 20, 2016

1 Introduction

The purpose is to design a virus similar to the *vbash* one, except that it will be encrypted. Its structure is divided in two parts:

- The first part of the code will be unencrypted and will simply consist of the decryption function. The key will be made of the first bytes of the infected virus.
- The second part (the most important one) will consist of the main body of the virus.

The virus will be an appending one. It will spread as follows:

- It looks for infected is executed.
- During the infection, it creates a specific key for each file (once again, a few bytes are taken from the target file), then encrypts its own main body and adds both the decrypting routine and the (encrypted) main viral body to the target file.
- A potential payload may be triggered (with or without a delayed action mechanism).

2 Virus design

We decide to write the homowork assigned using the language Python.

The virus is divived in two principle parts:

- virus decryption routine: it is not encrypted and it has to decrypt the encrypted virus program body and execute it;

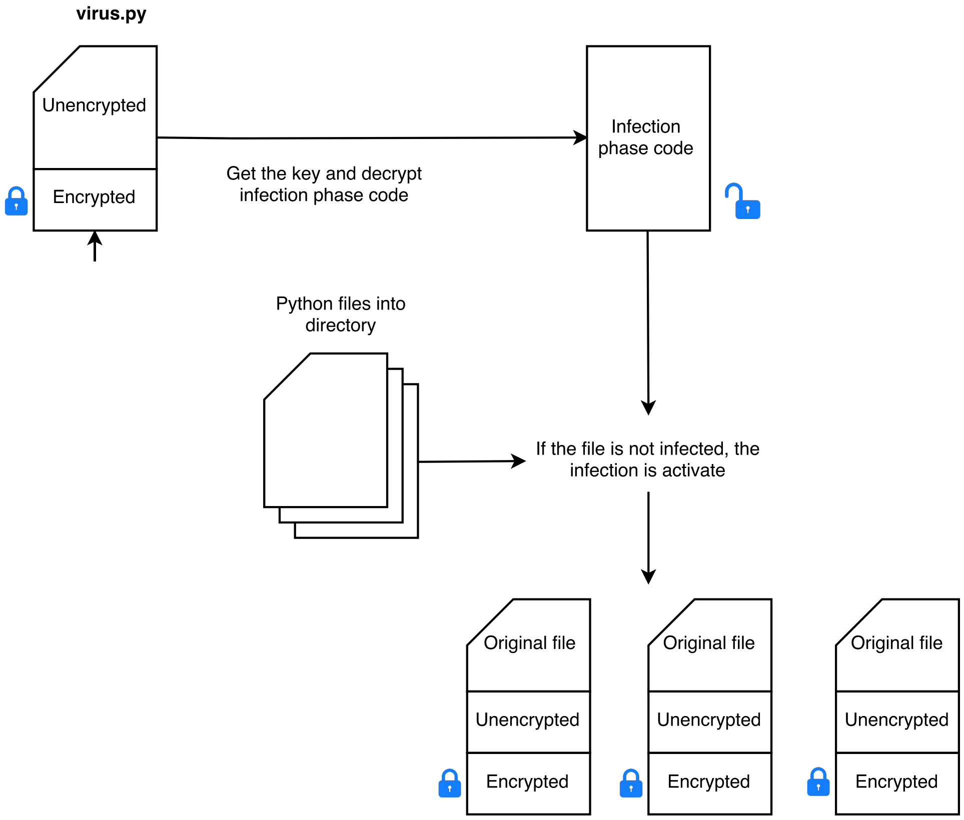

Figure 1: Virus design

- encrypted virus program body: it is encrypted (with the first line of the virus) and contains the infection and payload phases.

When the encrypted virus program body is decrypted and executed, it will do the following operations:

3 Implementation