Lab 3: Malware Detection

> Igor Mpore
>
> BS19-CS01
>
> i.mpore@innopolis.university

0. Definitions

1. **Malware**

   This is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive users access to information or which unknowingly interferes with the user's

2. **Malware detection**

   Malware detection refers to the process of detecting the presence of malware on a host system or of distinguishing whether a specific program is malicious or benign.

1. Tools

There are a couple tools that can be used for Malware detection such as Cuckoo Sandbox. Cuckoo is a tool that allows you to perform Sandboxed malware analysis.

A sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third-parties, suppliers, untrusted users and untrusted websites. More about it from here .

There are more other on-line tools that can help in malware detection such as ANYRUN which we will be using in this exercise.

Note: I didn't use Cuckoo Sandbox because I was having issues installing some libraries and dependencies to be able to run Cuckoo locally.

2. ANYRUN Malware Detector

Step 0: Why analyzing this chosen Malware

Malware: Ransomware WannaCry

A Ransomware is a type of malicious software which blocks access to a computer system until a sum of money is paid. WannaCry is a famous ransomware that I had interest into and I wanted to get a deep understanding of how it works and exploits a system. WannaCry Initially tries to access a specific web address that turns out to be an unregistered nonsense name. If the program is able to open the URL, WannaCry can not execute, so it acts as a sort of kill switch.

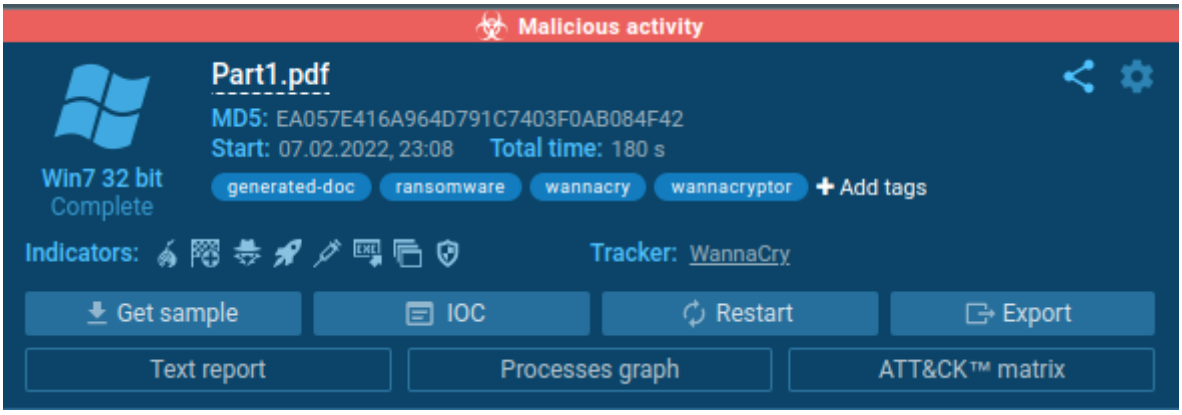
Targeted OS: Microsoft Windows Operating System

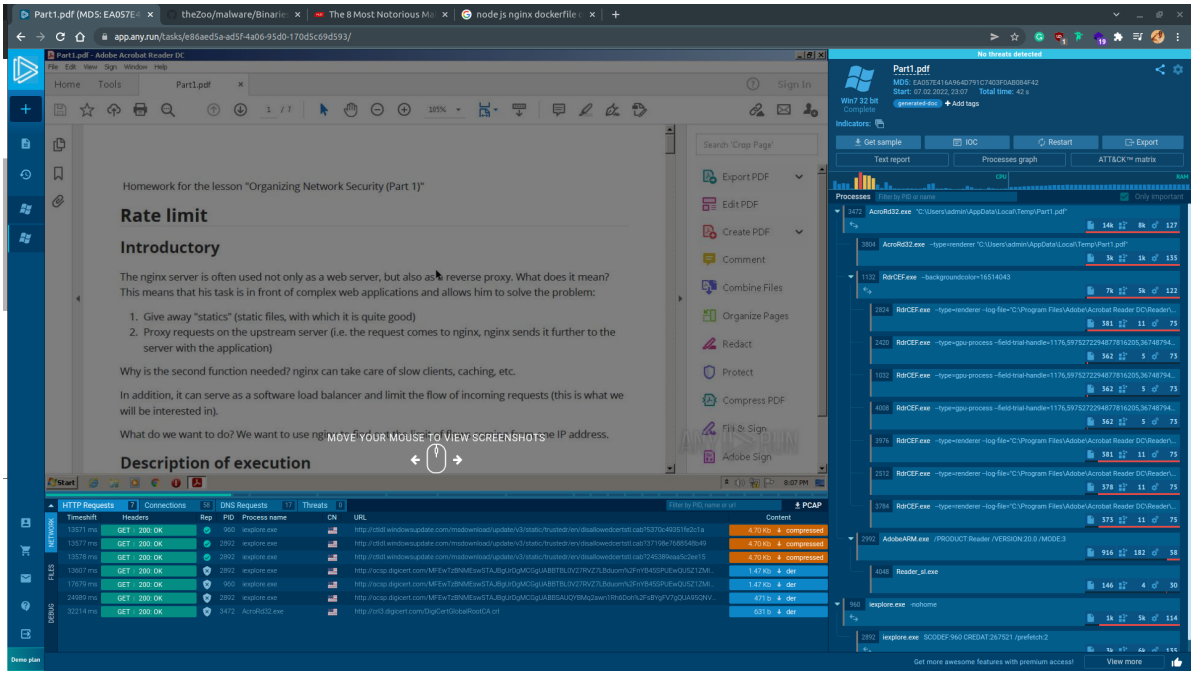
Years Active: From May 2017 - Now (Since new versions of it are still improved) Never Safe :)

The full analysis can be found through [this link]

Step 1: Environment Preparation

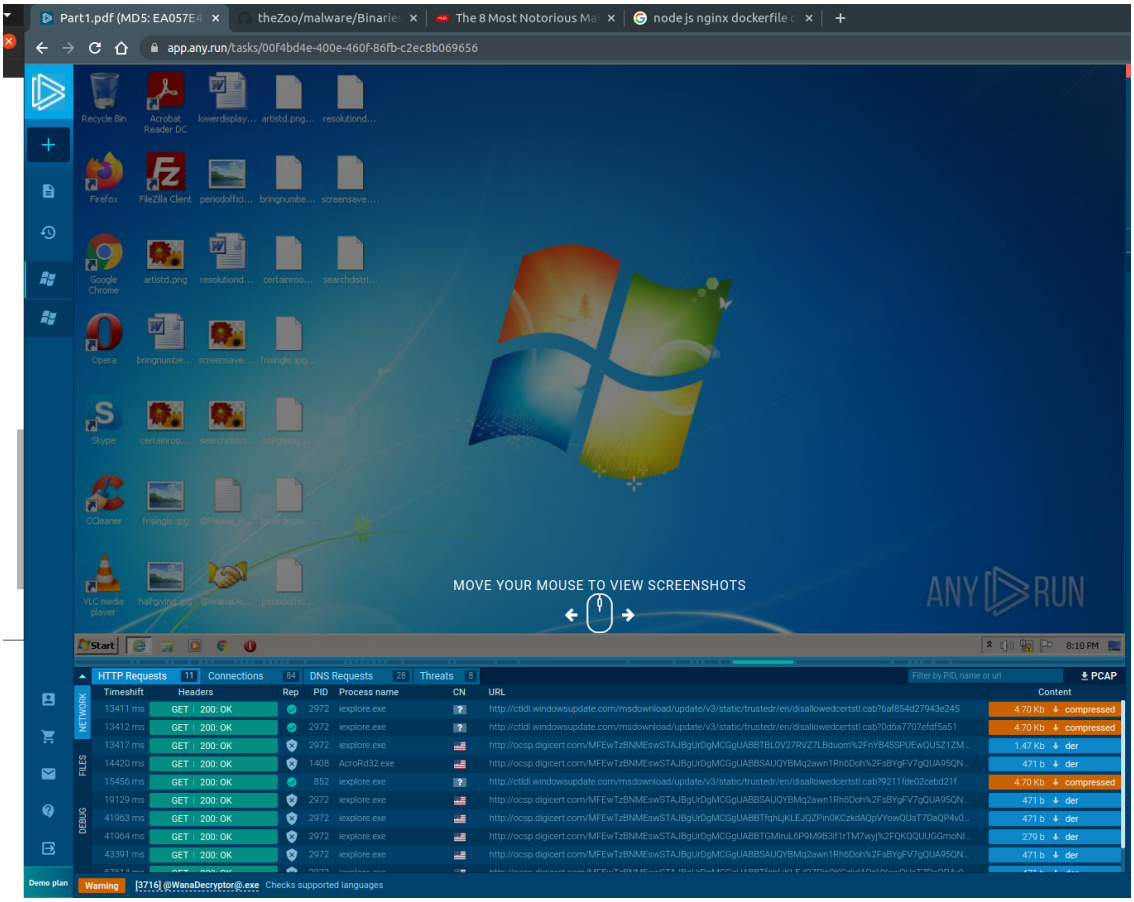
For the sake of safety, I used an online tool for Malware analysis as stated above called [any.run]. I created an account and then started a new task. Since I didn't want to even download this malware on my laptop, I uploaded a random file to ANYRUN to start a VM.



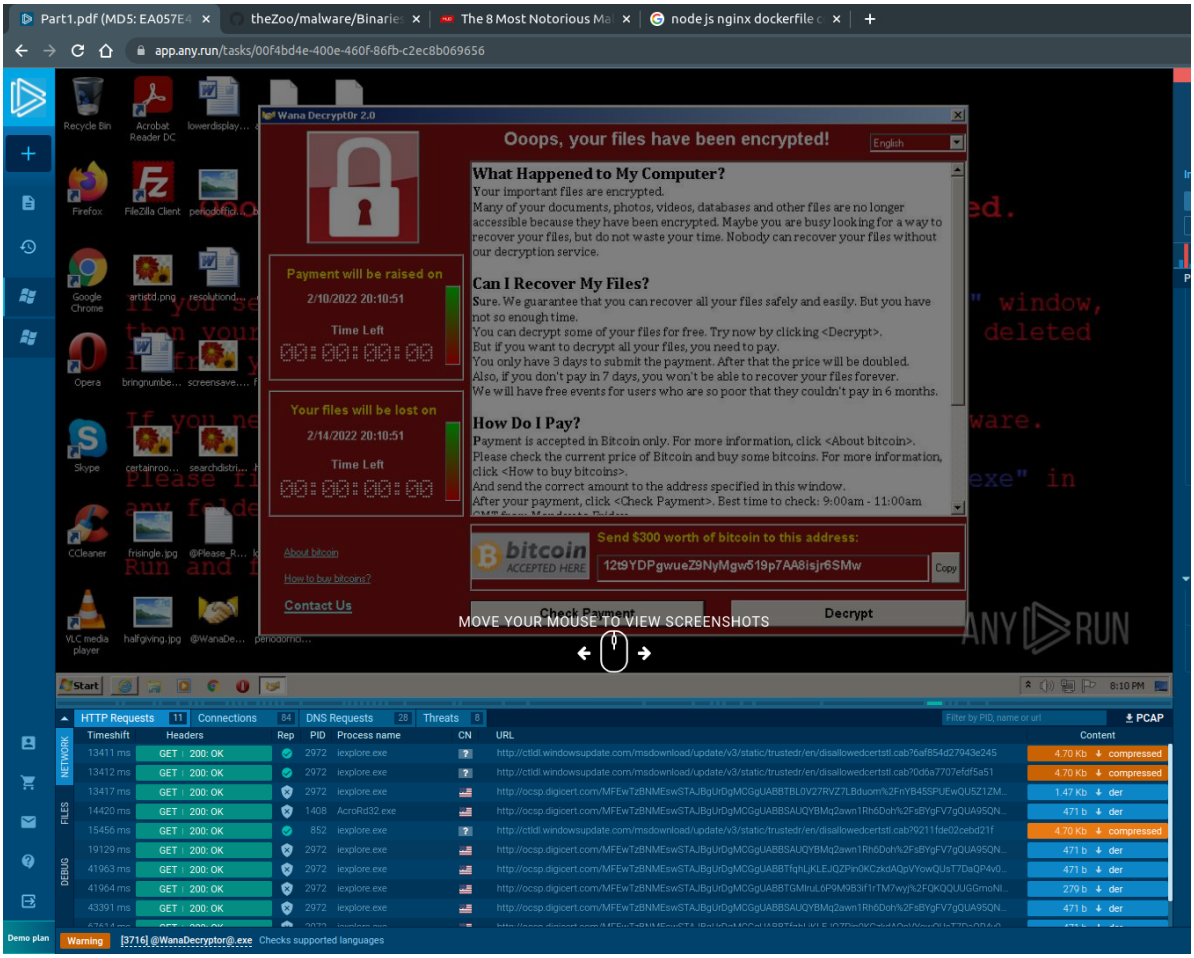


Step 2: Behavior analysis

- The Malware immediately added some images and other files on the desktop.

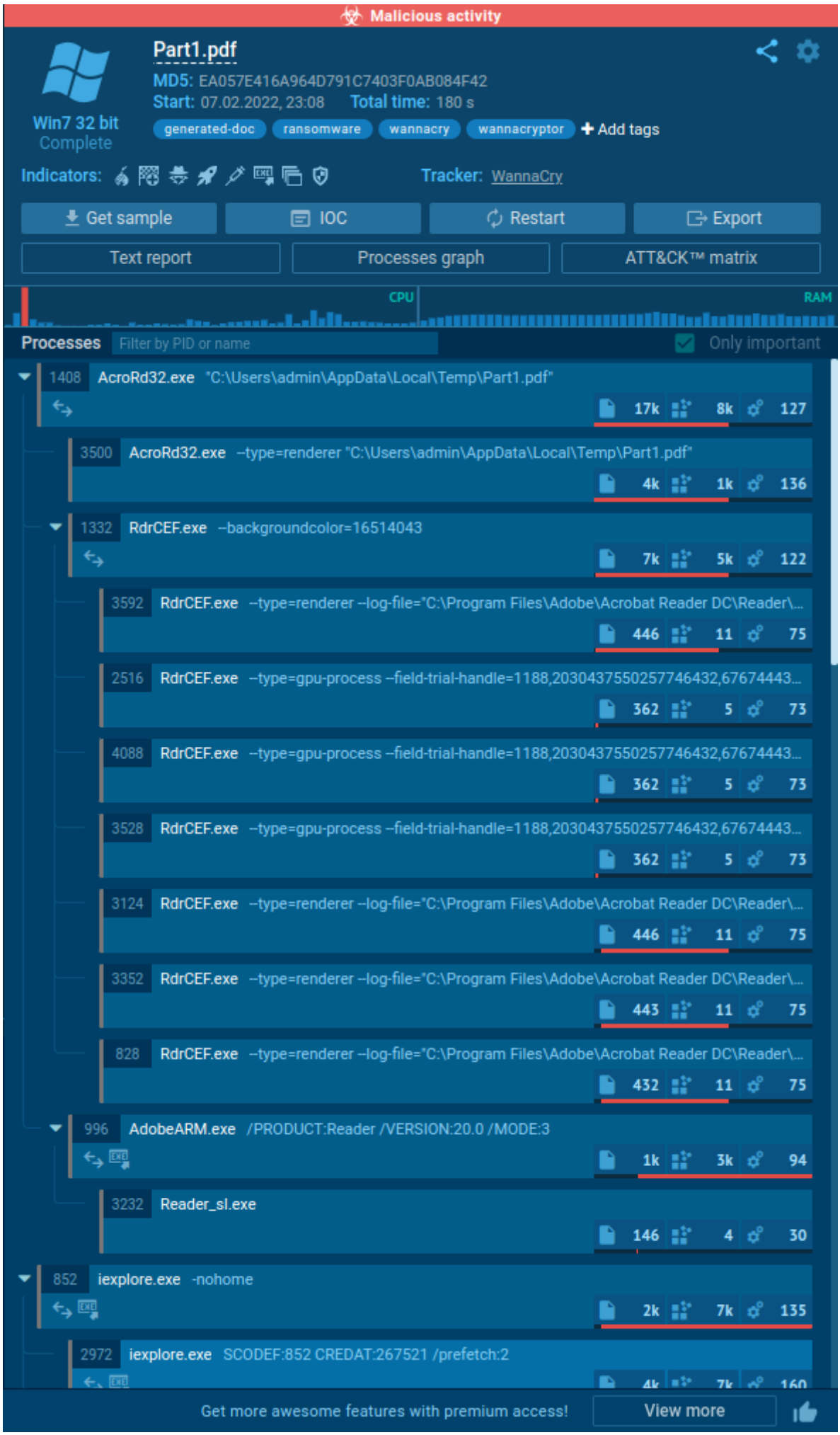


- After , the desktop changed immediately and then the Wana Decryptor launched.



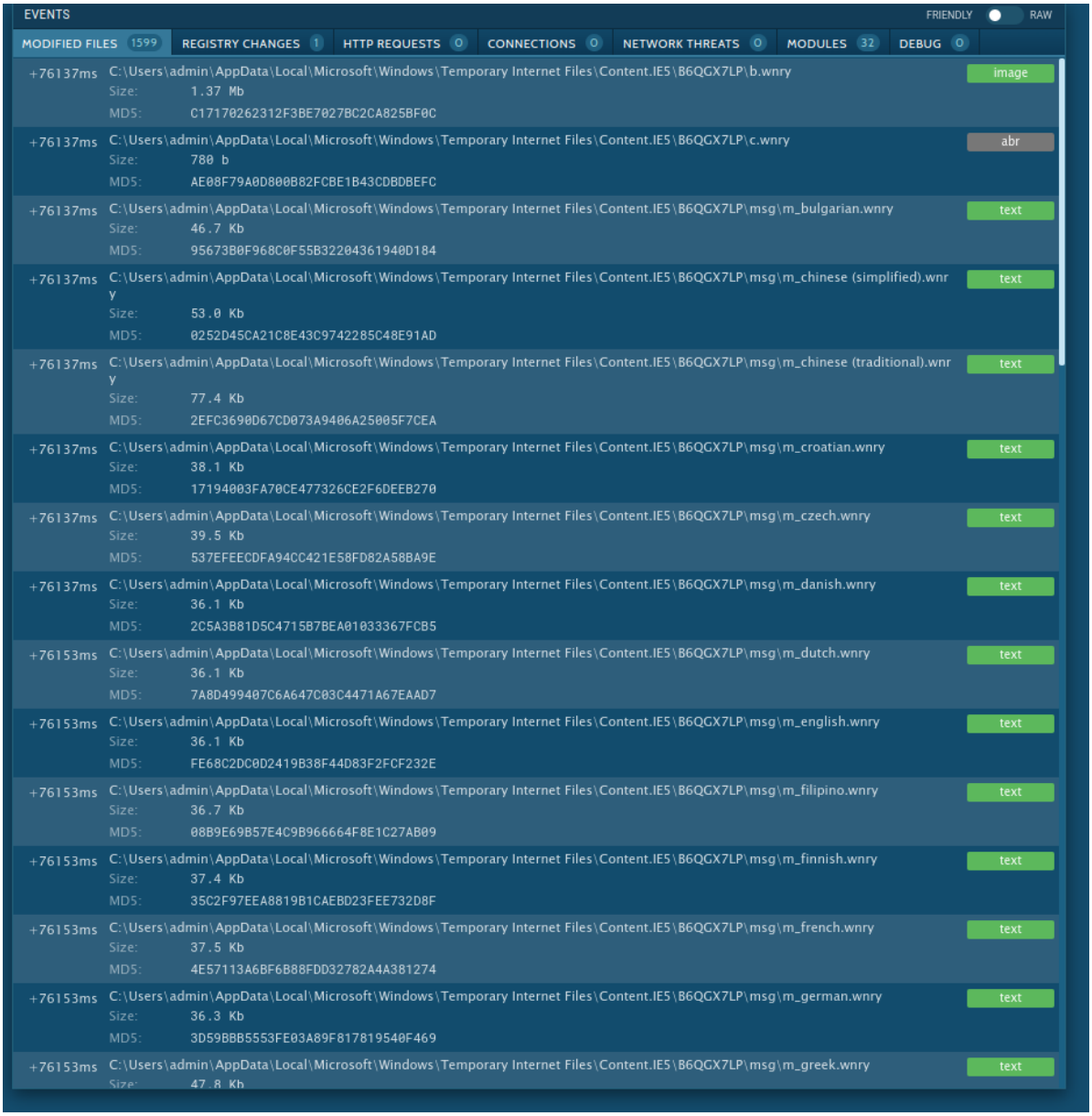
After this, I went to the browser myself and downloaded the malware and run the executable files. Now analysis was ready to be done. After the .exe was run, here is the simple report generated:

Here is also a list of processes that took place after the analysis:


Malicious activity
Part1.pdf
MD5: EA057E416A964D791C7403F0AB084F42
Start: 07.02.2022, 23:08 Total time: 180 s
Win7 32 bit
Complete
generated-doc
ransomware
wannacry
wannacryptor
+ Add tags
Indicators:
Tracker: WannaCry
Get sample
IOC
Restart
Export
Text report
Processes graph
ATT&CK™ matrix
CPU
RAM
Processes
Filter by PID or name
Only important
1408 AcroRd32.exe "C:\Users\admin\AppData\Local\Temp\Part1.pdf"
17k 8k 127
3500 AcroRd32.exe --type=renderer "C:\Users\admin\AppData\Local\Temp\Part1.pdf"
4k 1k 136
1332 RdrCEF.exe --backgroundcolor=16514043
7k 5k 122
3592 RdrCEF.exe --type=renderer --log-file="C:\Program Files\Adobe\Acrobat Reader DC\Reader\...
446 11 75
2516 RdrCEF.exe --type=gpu-process --field-trial-handle=1188,2030437550257746432,67674443...
362 5 73
4088 RdrCEF.exe --type=gpu-process --field-trial-handle=1188,2030437550257746432,67674443...
362 5 73
3528 RdrCEF.exe --type=gpu-process --field-trial-handle=1188,2030437550257746432,67674443...
362 5 73
3124 RdrCEF.exe --type=renderer --log-file="C:\Program Files\Adobe\Acrobat Reader DC\Reader\...
446 11 75
3352 RdrCEF.exe --type=renderer --log-file="C:\Program Files\Adobe\Acrobat Reader DC\Reader\...
443 11 75
828 RdrCEF.exe --type=renderer --log-file="C:\Program Files\Adobe\Acrobat Reader DC\Reader\...
432 11 75
996 AdobeARM.exe /PRODUCT:Reader /VERSION:20.0 /MODE:3
1k 3k 94
3232 Reader_sl.exe
146 4 30
852 iexplore.exe -nohome
2k 7k 135
2972 iexplore.exe SCODEF:852 CREDAT:267521 /prefetch:2
Get more awesome features with premium access!
View more

Step 3: Targeted files

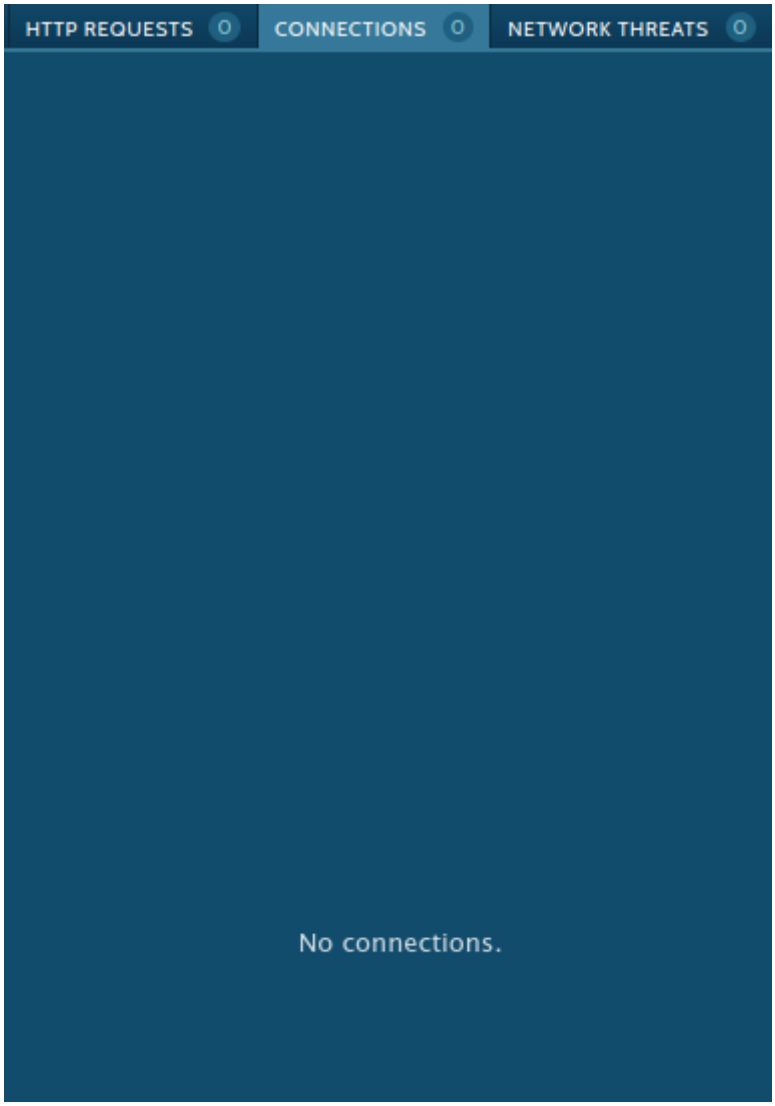
We can see that **1599 files** were modified and **1 registry**.



I went through some files including binary files, executables and some txt files and I went through to see if they contained some important information. Couldn't paste all the screen shoots here but they also contained important information.

Step 4: Remote Addresses

This malware doesn't access any remote addresses during it's execution as shown in the report.


HTTP REQUESTS 0
CONNECTIONS 0
NETWORK THREATS 0
No connections.