

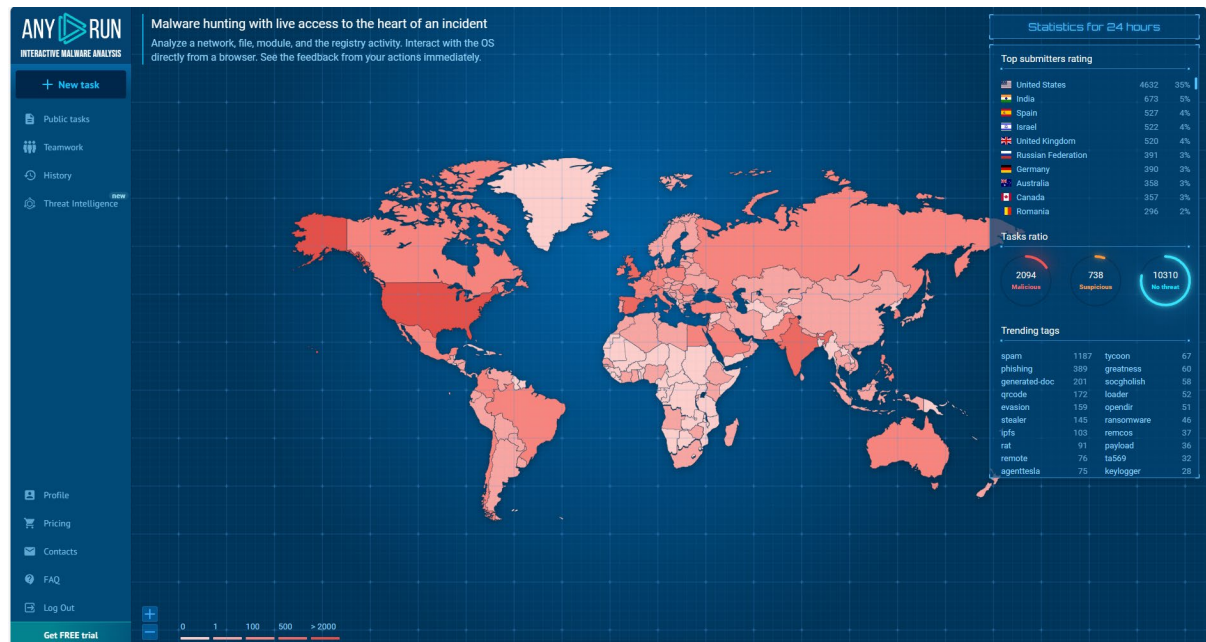
## Lab 3: Malware Analysis

Mohamad Syafiq Syazwan Bin Mohamad Salim

B032110149

### Sandbox Environment


1) Open the any run to analysis the malware.




2) Click the new task to put the URL and upload file to detect the malware.

**Create a new task** Pro mode ×

**1. Type URL or upload a file**


 type or copy URL


or

 **Upload**  
drag and drop a file here

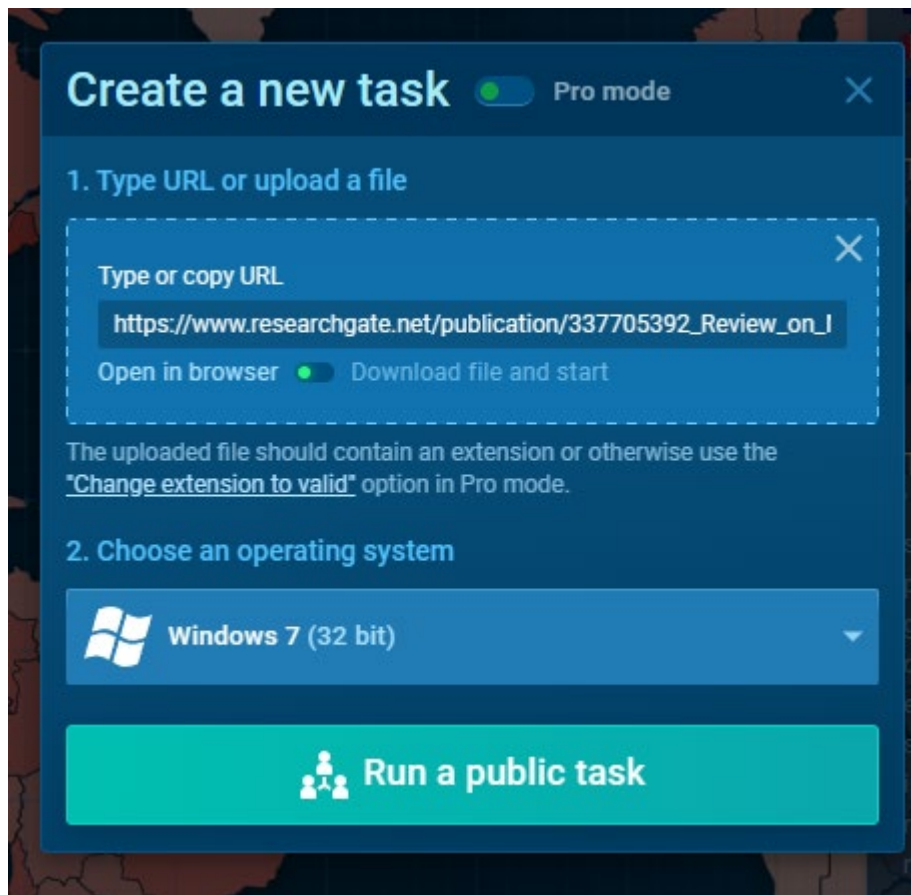
The uploaded file should contain an extension or otherwise use the "Change extension to valid" option in Pro mode.

**2. Choose an operating system**

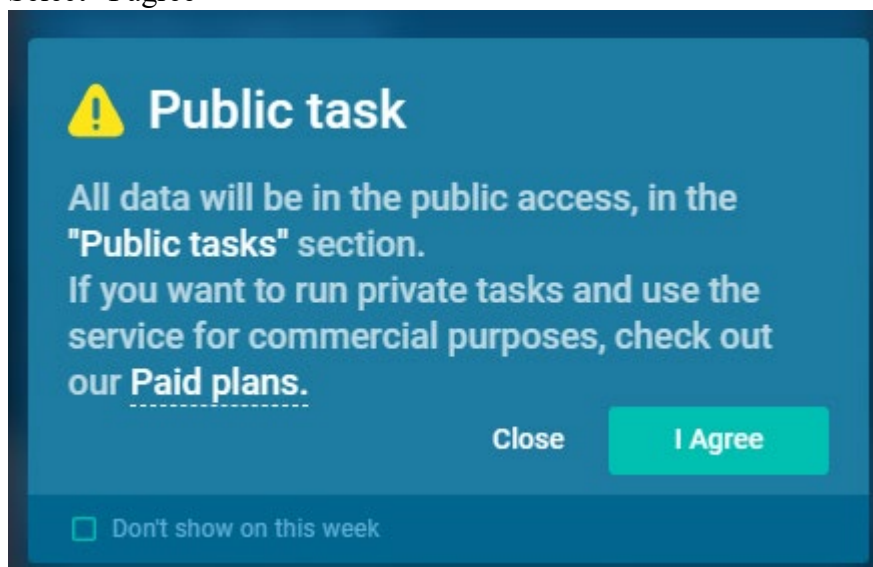
 Windows 7 (32 bit) ▼

 **Run a public task**

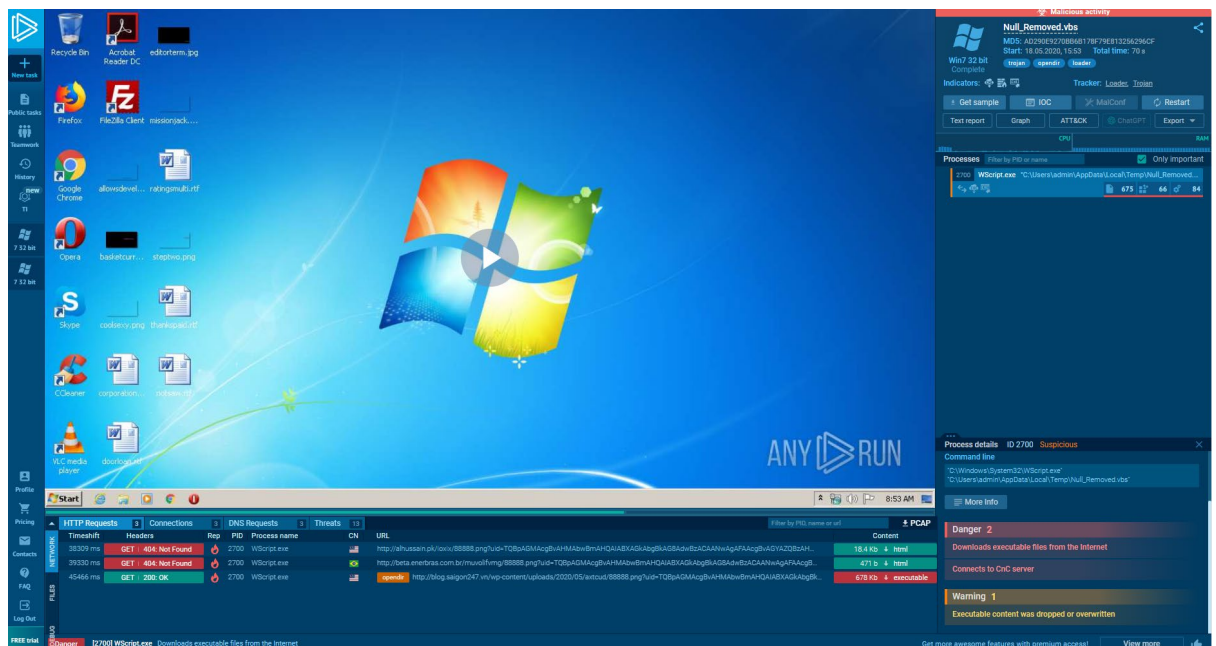
3) For this time, I'm use URL to detect the malware.



4) Select "I agree"



5) the result will appear after running the URL.



6) Finish the question are given.

- Is the suspicious activity is detected?

## SUSPICIOUS

Executable content was dropped or overwritten

- WScript.exe (PID: 2700)

- Is the Command & Control server is detected?

### Behavior activities

(PID: 2700) WScript.exe

▲ 1 of 3 ▼ Source: network First seen: 38524 ms

**Danger / Network Activities**  
**Connects to CnC server**

PortSrc:	49700
PortDst:	80
IpSrc:	192.168.100.151
IpDst:	45.61.147.136
Process:	C:\Windows\System32\WScript.exe

### Behavior activities

(PID: 2700) WScript.exe

▲ 2 of 3 ▼ Source: network First seen: 38524 ms

**Danger / Network Activities**  
**Connects to CnC server**

PortSrc:	49721
PortDst:	80
IpSrc:	192.168.100.151
IpDst:	186.233.148.134
Process:	C:\Windows\System32\WScript.exe



- What is the IP address involved in this activity?

PID	Process	Method	HTTP Code	IP	URL	CN
2700	WScript.exe	GET	404	45.61.147.136:80	http://alhussain.pk/ioxix/88888.png?uid=TQBpAGMAcgBvAHMAbwBmAHQAIABXAGkAbgBkAG8AdwBzACAANwAgAFAAcgBvAGYAZQBzAHMAaQBvAG4AYQBsACAA	US
2700	WScript.exe	GET	200	104.28.21.40:80	http://blog.saigon247.vn/wp-content/uploads/2020/05/axtcud/88888.png?uid=TQBpAGMAcgBvAHMAbwBmAHQAIABXAGkAbgBkAG8AdwBzACAANwAgAFAAcgBvAGYAZQBzAHMAaQBvAG4AYQBsACAA	US
2700	WScript.exe	GET	404	186.233.148.134:80	http://beta.enerbras.com.br/muvolifvmg/88888.png?uid=TQBpAGMAcgBvAHMAbwBmAHQAIABXAGkAbgBkAG8AdwBzACAANwAgAFAAcgBvAGYAZQBzAHMAaQBvAG4AYQBsACAA	BR

Download PCAP, analyze network streams, HTTP content and a lot more at the [full report](#)

## Connections

PID	Process	IP	Domain	ASN
—	—	186.233.148.134:80	beta.enerbras.com.br	Central Server Informática Ltda
—	—	104.28.21.40:80	blog.saigon247.vn	Cloudflare Inc
2700	WScript.exe	45.61.147.136:80	alhussain.pk	—

## DNS requests

Domain	IP	Reputation
alhussain.pk	45.61.147.136	malicious
beta.enerbras.com.br	186.233.148.134	malicious
blog.saigon247.vn	104.28.21.40 104.28.20.40	malicious



- What is the malware types involved in this activity?

## Threats

PID	Process	Class	Message
2700	WScript.exe	A Network Trojan was detected	ET TROJAN Unk.VBSLoader Retrieving Payload
2700	WScript.exe	A Network Trojan was detected	ET USER_AGENTS Possible QBot User-Agent
2700	WScript.exe	A Network Trojan was detected	ET TROJAN Possible Win32/Qbot/Quakbot Checkin via HTTP GET
2700	WScript.exe	A Network Trojan was detected	ET TROJAN Unk.VBSLoader Retrieving Payload
2700	WScript.exe	A Network Trojan was detected	ET USER_AGENTS Possible QBot User-Agent
2700	WScript.exe	A Network Trojan was detected	ET TROJAN Possible Win32/Qbot/Quakbot Checkin via HTTP GET
2700	WScript.exe	A Network Trojan was detected	ET TROJAN Unk.VBSLoader Retrieving Payload
2700	WScript.exe	A Network Trojan was detected	ET USER_AGENTS Possible QBot User-Agent
2700	WScript.exe	A Network Trojan was detected	ET TROJAN Possible Win32/Qbot/Quakbot Checkin via HTTP GET
2700	WScript.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
2700	WScript.exe	A Network Trojan was detected	AV POLICY EXE or DLL in HTTP Image Content Inbound - Likely Malicious
2700	WScript.exe	Misc activity	ET INFO EXE - Served Attached HTTP
2700	WScript.exe	Misc activity	SUSPICIOUS [PTsecurity] PE as Image Content type mismatch

Previous
1
Next
20



## VirusTotal

7) First open the GitHub to download the malware sample.

The screenshot shows the GitHub repository page for 'malware-samples' by user 'fabrimagic72'. The repository is public and has 102 watchers, 398 forks, and 1.5k stars. The main content area displays a list of files and folders, each with a description and a timestamp. The files include Adylkuzz, Allapple, Bitcoin miners, Downloader-CUZ, EternalRocks, Generic Trojan, Muldrop, Pepex, Ransomware, Rbot, SdBot, Shodi, Spam/Paypal, Virut, Wannacry, and Wisdomeyes. The right sidebar contains the 'About' section, which describes the repository as a collection of malware samples caught by several honeypots, and lists various tags like botnet, honeypot, malware, malwareanalysis, ransomware, malware-analysis, malware-samples, wannacry, eternalblue, uiwix, eternalrocks, and trickbot. Below the 'About' section are links to the README, Activity, and Stars, and a 'Report repository' link. The 'Releases' section shows 'No releases published', and the 'Packages' section shows 'No packages published'.

fabrimagic72 / malware-samples

<> Code Issues 9 Pull requests 2 Actions Projects Security Insights

malware-samples Public

Watch 102 Fork 398 Star 1.5k

master Go to file + Code

fabrimagic72 Delete readme.txt 79d5342 · 4 years ago 84 Commits

Adylkuzz	Adylkuzz	7 years ago
Allapple	new sample added	7 years ago
Bitcoin miners	possible Locky	7 years ago
Downloader-CUZ	ne entry	7 years ago
EternalRocks	EternalRocks Malware	7 years ago
Generic Trojan	Add files via upload	7 years ago
Muldrop	new malware added	7 years ago
Pepex	new malware added	7 years ago
Ransomware	Create grandcab.bin	6 years ago
Rbot	New malware added	7 years ago
SdBot	new sample added	7 years ago
Shodi	New Malware added	7 years ago
Spam/Paypal	zipfile added	7 years ago
Virut	new malware added	7 years ago
Wannacry	info	7 years ago
Wisdomeyes	New malware added	7 years ago
Emotet attack	Comparison between Emotet and...	4 years ago

https://github.com

About

A collection of malware samples caught by several honeypots i manage

botnet honeypot malware malwareanalysis ransomware malware-analysis malware-samples wannacry eternalblue uiwix eternalrocks trickbot

Readme Activity 1.5k stars 102 watching 398 forks Report repository

Releases

No releases published

Packages








No packages published

8) Second download the malware sample


Free Download Manager

✚ ⏮ ⏭ ⏴ ⏵ ⏶ 🔍 ☰

All (218) Missing Files (3) Active (1) Completed (217) Uncompleted (1) Torrent Video (7) Music (20) +

<input type="checkbox"/>	Name ▾	Status	Speed	Size	Added
<input type="checkbox"/>	 malware-samples-master.zip	Unknown file size	▼ 918 KB/s	629 MB / —	8:47 PM
<input type="checkbox"/>	 malware-samples-master.zip			50.8 MB	8:49 PM
<input type="checkbox"/>	 main.dart.pdf			645 KB	17/10/2023
<input type="checkbox"/>	 link for Assignment 2 Task 1 (1).txt			60 B	31/12/2023
<input type="checkbox"/>	 get-pip.py			2.51 MB	16/12/2023
<input type="checkbox"/>	 flutter_windows_3.13.6-stable.zip			856 MB	10/10/2023
<input type="checkbox"/>	 fashion video.mp4			409 KB	6/1/2024

General Progress Connections



**malware-samples-master.zip**

Unknown file size

Speed: ▼ 918 KB/s      Downloaded: 629 MB

Added at: 8:47 PM

📁 C:\Users\Syafiq\OneDrive\Desktop\sem 6\INFORMATION TECHNOLOGY SECURITY

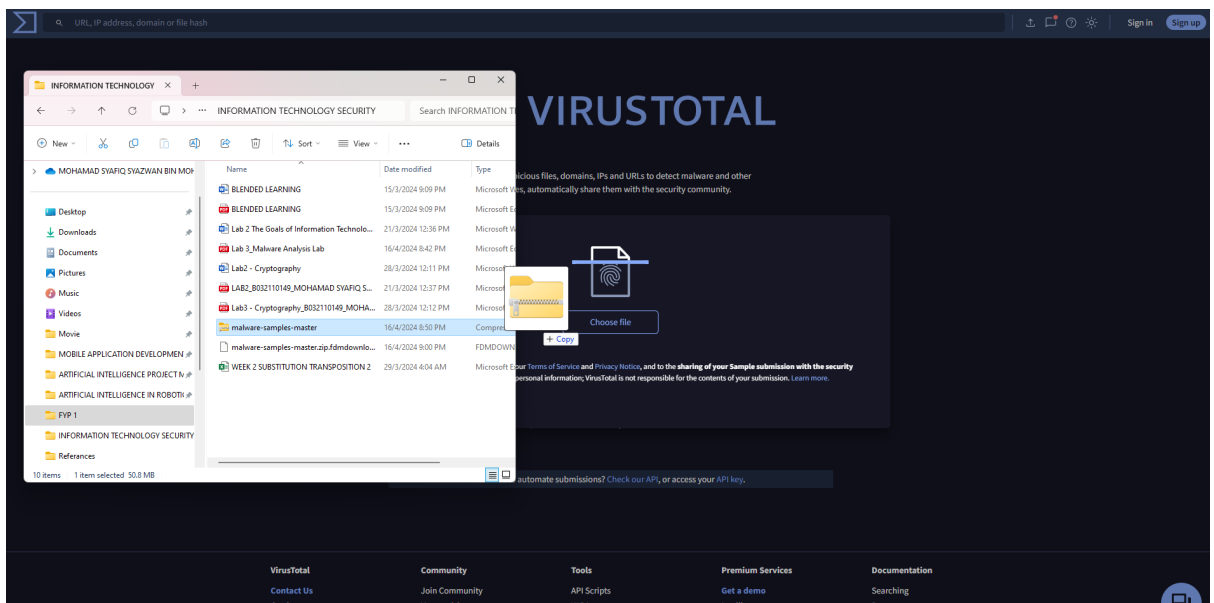
🌐 Web page: <https://github.com/jstrosch/malware-samples>

🌀 ▼ 918 KB/s ▲ 0 B/s malware-samples-master.zip

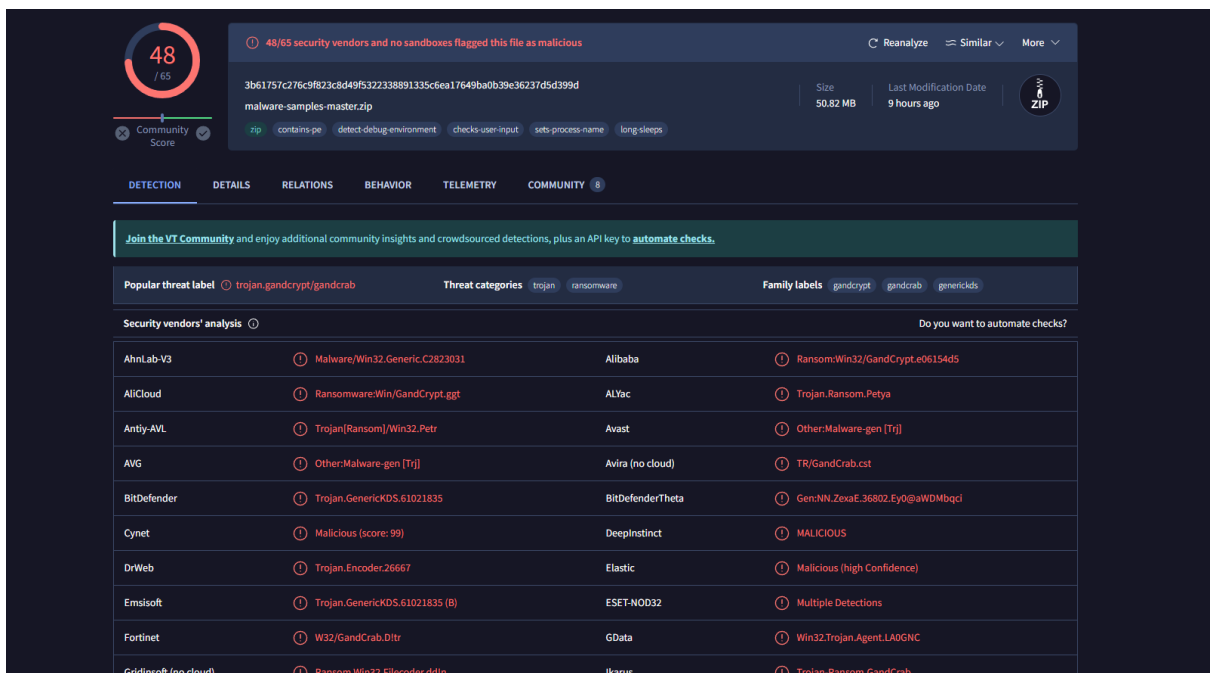
9) After download the malware into VirusTotal.com to make the analysis the malware.



10) Upload the malware file in VirusTotal.



11) Then, the result will appear.



12) Finish the question are given.

- What is the malware type involved in this activity?

**Threat categories** trojan ransomware

- Threat categories
  - 1) trojan
  - 2) ransomware

- What is the size of malware?

**File size** 50.82 MB (53285180 bytes)

- File size = 50.82 MB (53285180 bytes)

- What is the MD5 for this malware?

**MD5** 04ff5205025adf73e9ce2d5284a7c816

- MD5 = 04ff5205025adf73e9ce2d5284a7c816

- What is the date and year of malware for first submission?

**First Submission** 2020-10-13 07:26:31 UTC

- First Submission = 2020-10-13 07:26:31 UTC

- What is the date and year of malware for latest modification?

**Latest Contents Modification** 2020-09-30 06:02:56

- Latest Contents Modification = 2020-09-30 06:02:56

- Is the malware file is encrypted? Obfuscated?

**UNKNOWN** 54

- UNKNOWN = 54 files

- How many security vendors or engines are detected this file? Please listed here.

47/65 security vendors and no sandboxes flagged this file as malicious

- 48/65 security vendors and no sandboxes flagged this file as malicious.

- Illustrate the analysis by VirusTotal Graph

