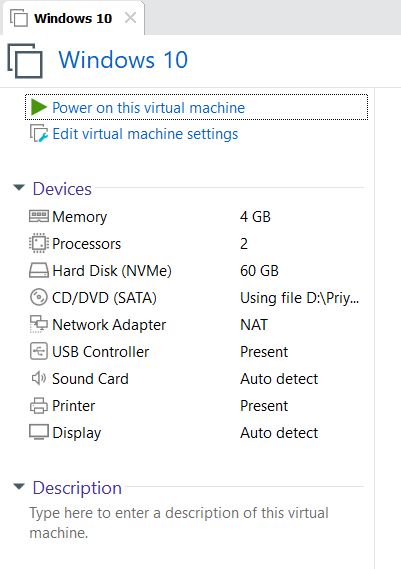
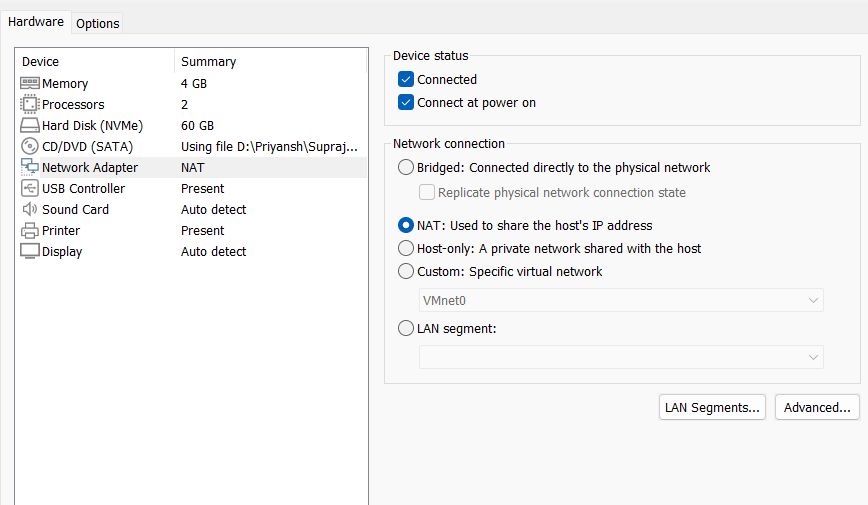
**Malware Analysis**

**Set up a virtualized environment using VMware Player for Win-10 32 bit:**

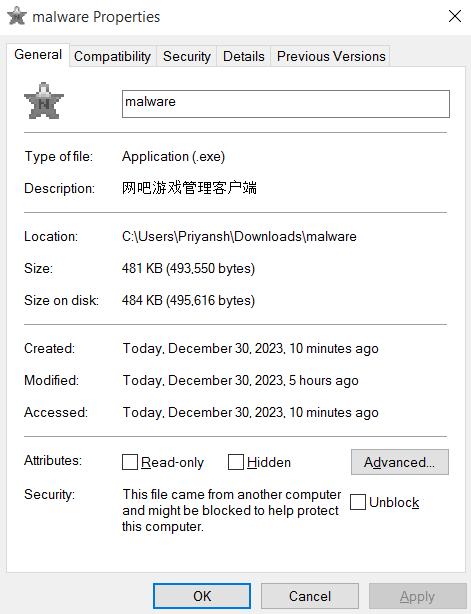
**Windows 10:**

* Modern architecture for analysing current malware.
* Enhanced security with regular



Using **NAT** in the VM for malware analysis provides a **secure and efficient setup**. It allows the VM to access the internet while safeguarding its internal structure, ensuring anonymity. NAT's mapping of private to public IP addresses enhances security and resource utilization in the analysis environment.

**Search the malware in malware bazar and download it in your VM Machine**



**Name: Malware**

**Type of File:** Application (.exe)

**Description:** 网吧游戏管理客户端

**Location:** C:\Users\Priyansh\Downloads\malware

**Size:** 481 KB (493,550 bytes)

**Size on Disk:** 484 KB (495,616 bytes)

**Created:** **‎**December ‎30, ‎2023

**Modified:** ‎December ‎30, ‎2023

**Accessed:** ‎December ‎30, ‎2023

**This file, named "malware," is identified as an application with a size of 481 KB. Located on the Downloads\malware folder.**

**Static Malware Analysis**

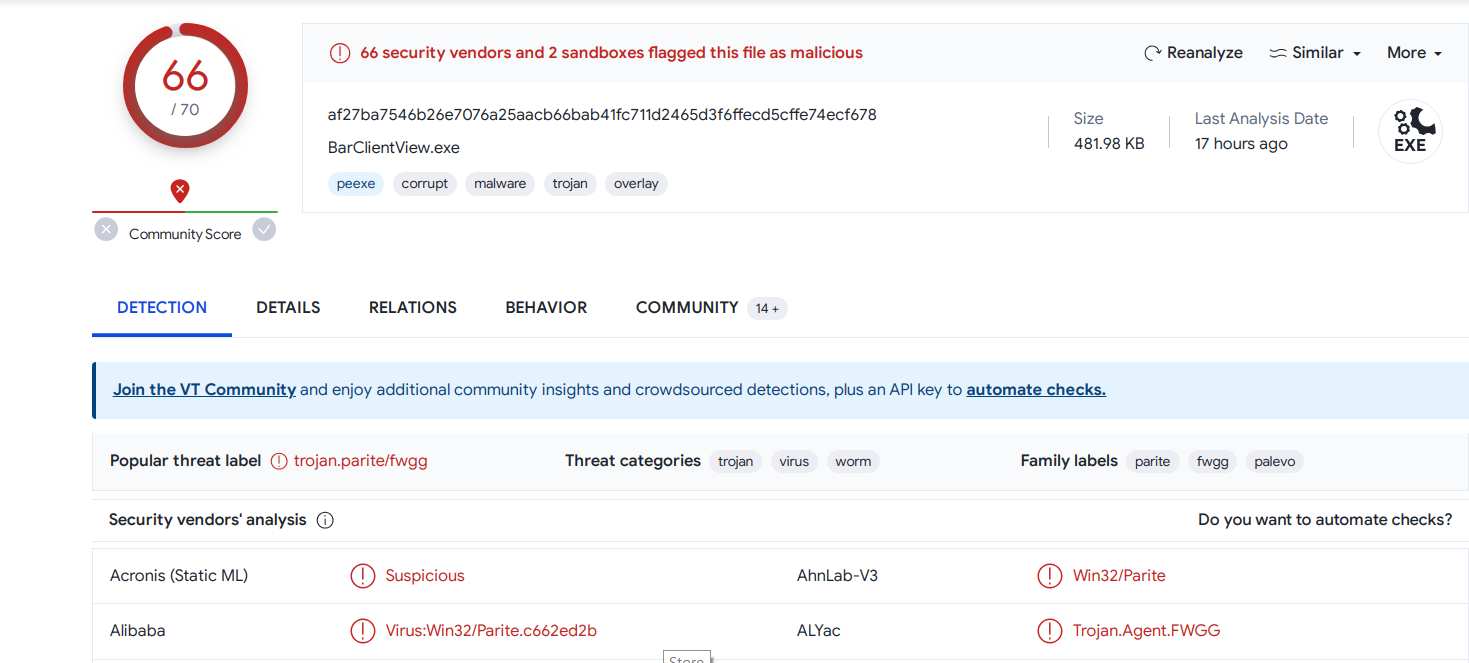
**Virus total:**

**Steps:**

* Calculate Hash of the Malware file
* Upload the hash value into virus total website and let in analyse for you.

The analysis on **Virus Total** for **"Malware.exe"** by **66 security vendors**, including **2 sandbox detections** flagged this file as Malicious.

* **File Name:**Malware.exe
* **File Hash (SHA256):** af27ba7546b26e7076a25aacb66bab41fc711d2465d3f6ffecd5cffe74ecf678

****

**Popular threat level:** trojan.parite/fwgg

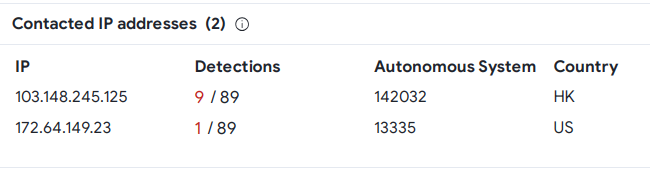
**Threat Categories:**

* Trojan
* Virus
* Worm

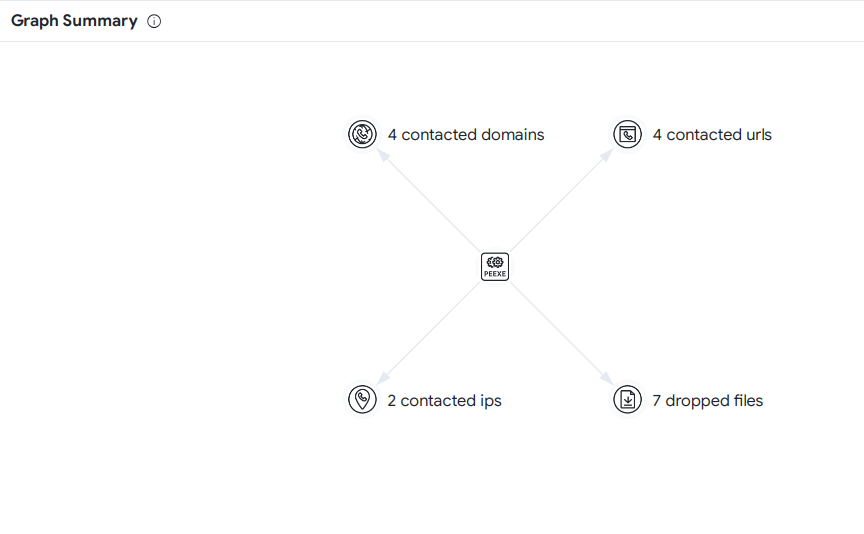
**Family Labels:**

* parite
* fwgg
* palevo

**Contacted IP Address’s by the Malware**



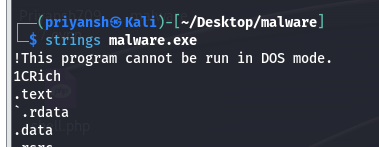
Graph View



**Strings:**

String command in Linux will return each string type of characters that are printable in the file. It is mainly used in determining the file's contents and extracting the text from binary-type files.

**Sample:**

****

Look for:

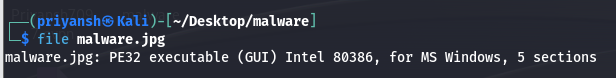
* IP Addresses
* URL's
* Windows API or files (anything)
* Base64 or any encoded text

**Strings of Interest:**

* MZ 4D 5A - That Represents Executable File
* This Program Cannot be run in DOS MODE.

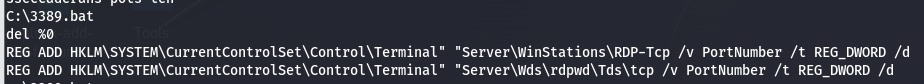
**Check File type of the malware:**

This step is crucial as sometimes the hackers can change the extension of the malware such as jpg or png etc.



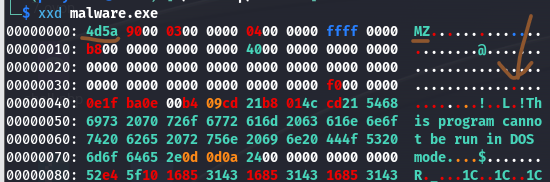
The file command clearly shows that the file malware.jpg is an executable file.

**Registries changes made by the malware:**

****

**Hex Values**

**Tool :** Hxd / xxd / hexeditor

****

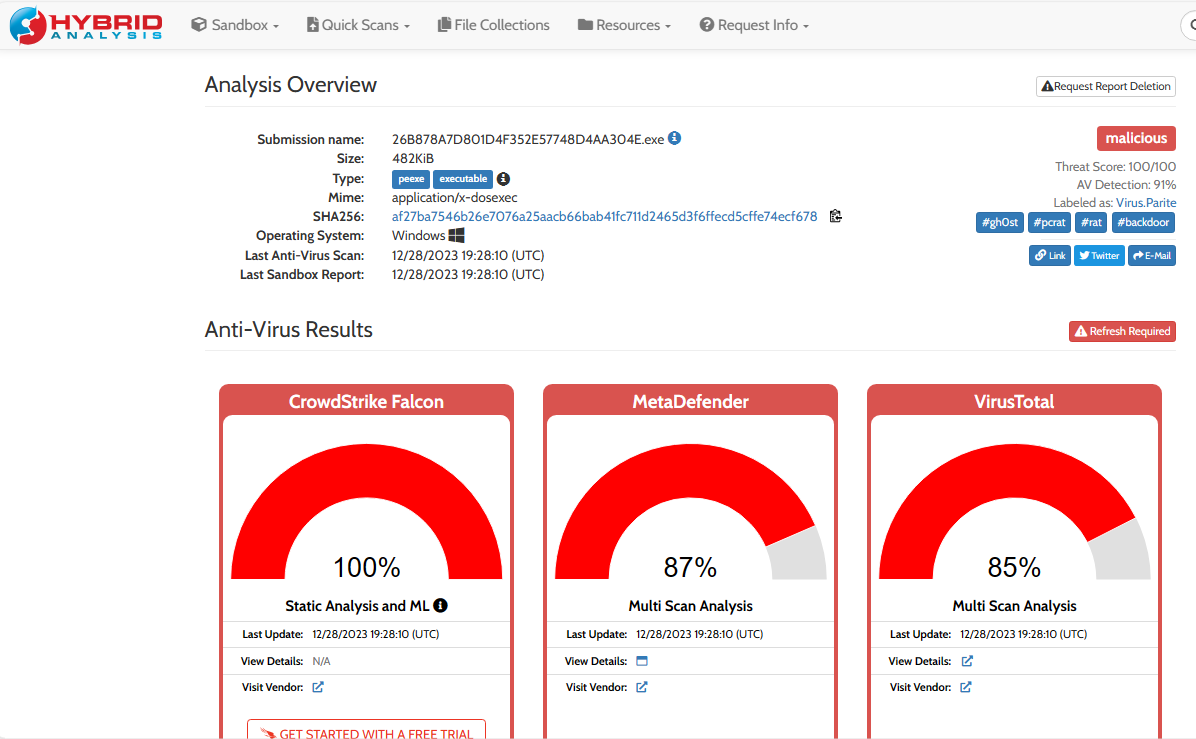
Known Signatures:

* **MZ 4D 5A** - That Represents Executable File
* **Malware** - This Program Cannot run in DOS MODE

**Note : All in One Tool for Static Malware Analysis is PEStudio**

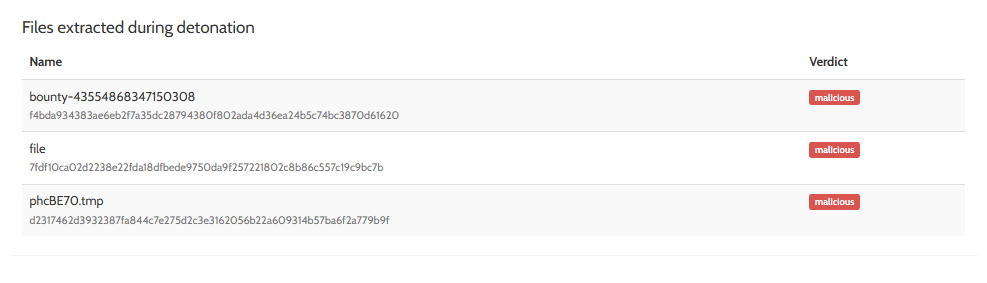
**Dynamic Analysis**

**Hybrid-Analysis.com:**

****

The Executable file (sha-256 : af27ba7546b26e7076a25aacb66bab41fc711d2465d3f6ffecd5cffe74ecf678) has been identified as malware

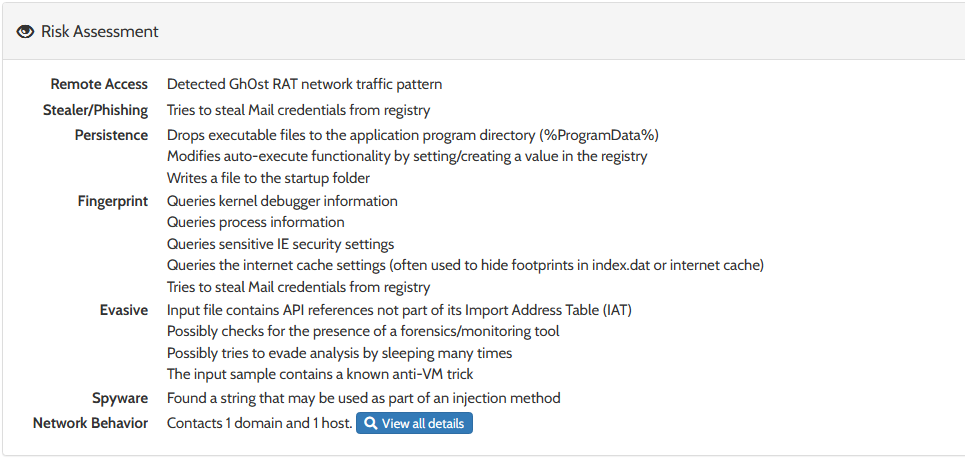
**File’s extracted during execution:**

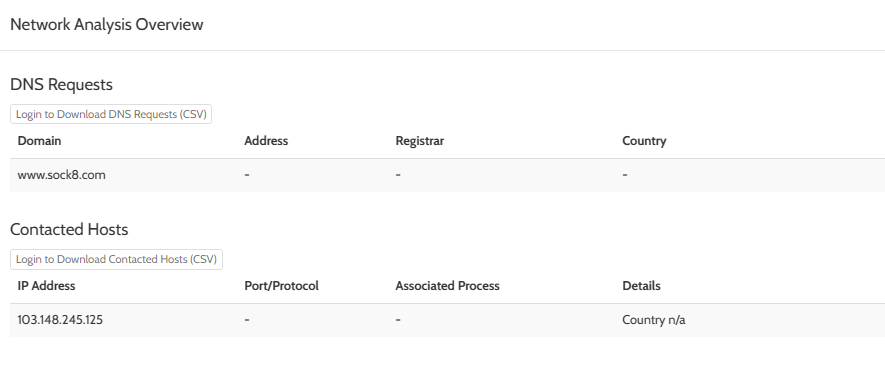


**Incident Response**

**Risk Assessment:**

Detected Gh0st Rat (Remote Access Trojan)



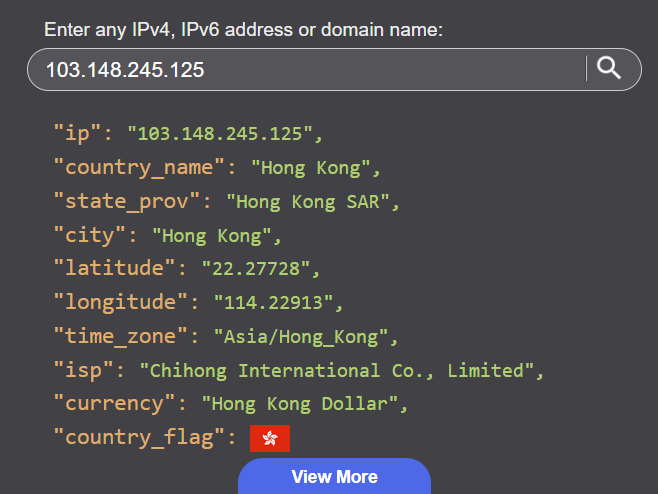
**DNS Request’s and Contacted Host’s By Malware**

**DNS Request**

Domain: www.sock18.com

**Contacted Hosts:**

IP: 103.148.245.125

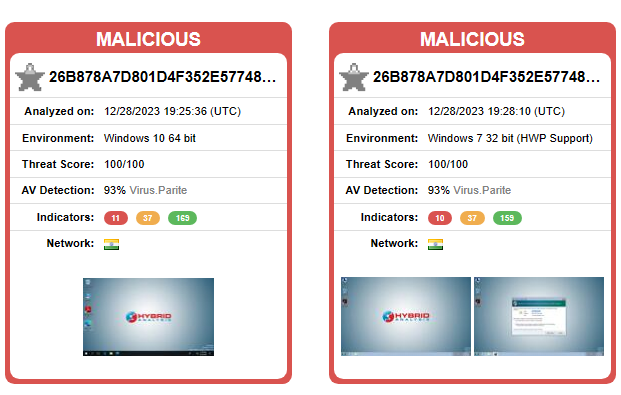
**IP Geolocator:**

IP Geolocator Reveals that the IP Address

To which malware tried to contact/connect

Belongs to IP Address of **Hong Kong.**

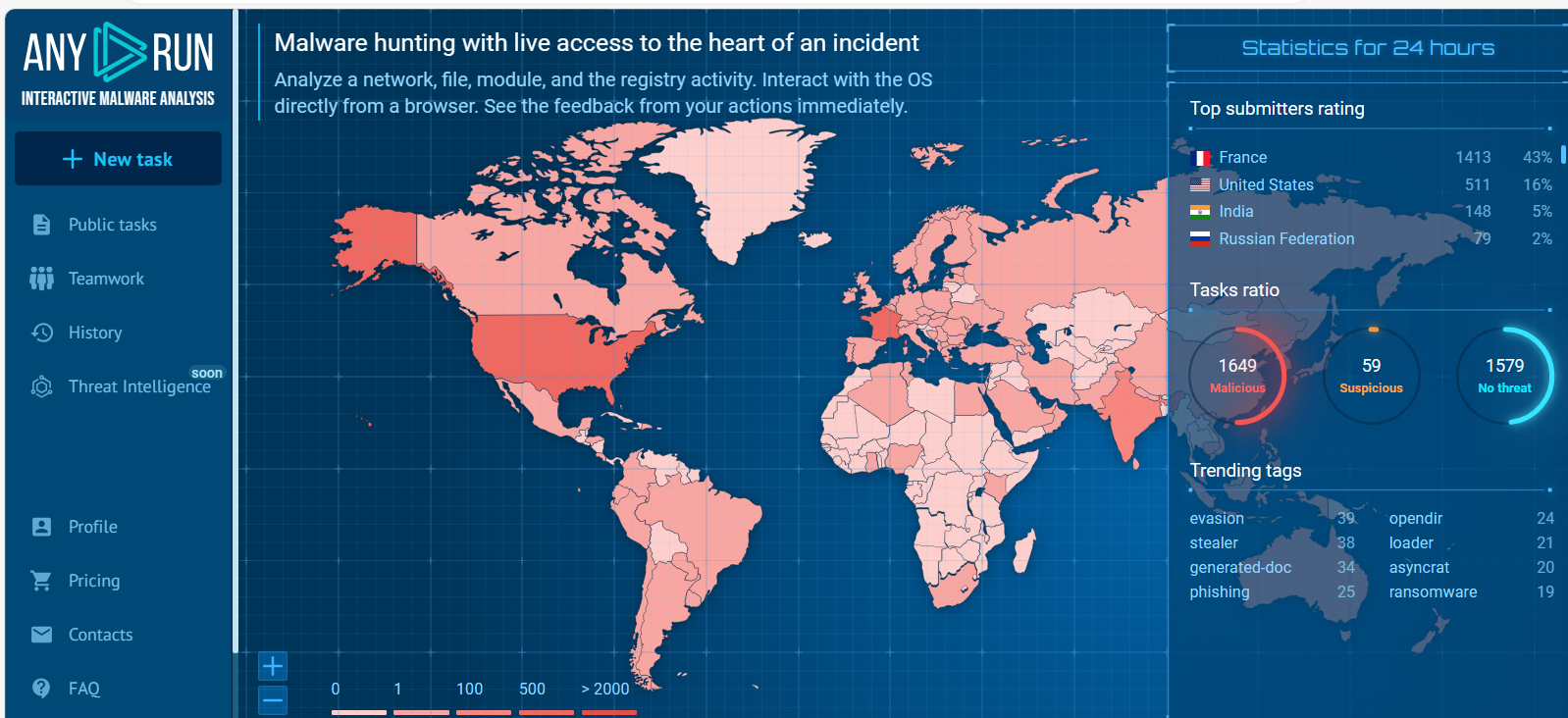
**Flacon Sandbox Report**

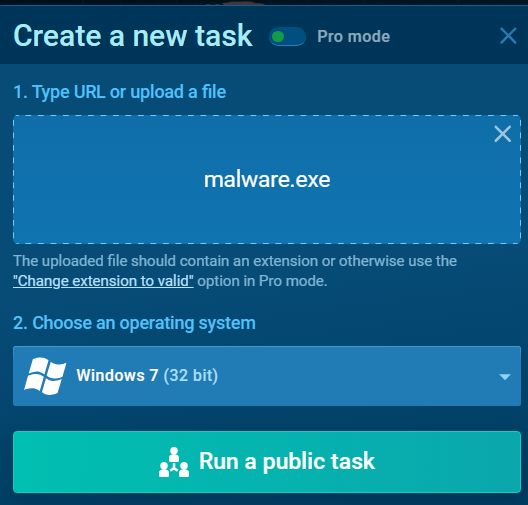


The analysis of Malware on Windows 10 (64-bit) conducted on 12/28/2023 revealed an alarming threat score of 100/100, indicating a highly malicious nature. Notably, 93% of antivirus engines flagged the file as **“Virus, Parite”**.

**AnyRun.com:**

Overview Of Dashboard



**Create a New Task**

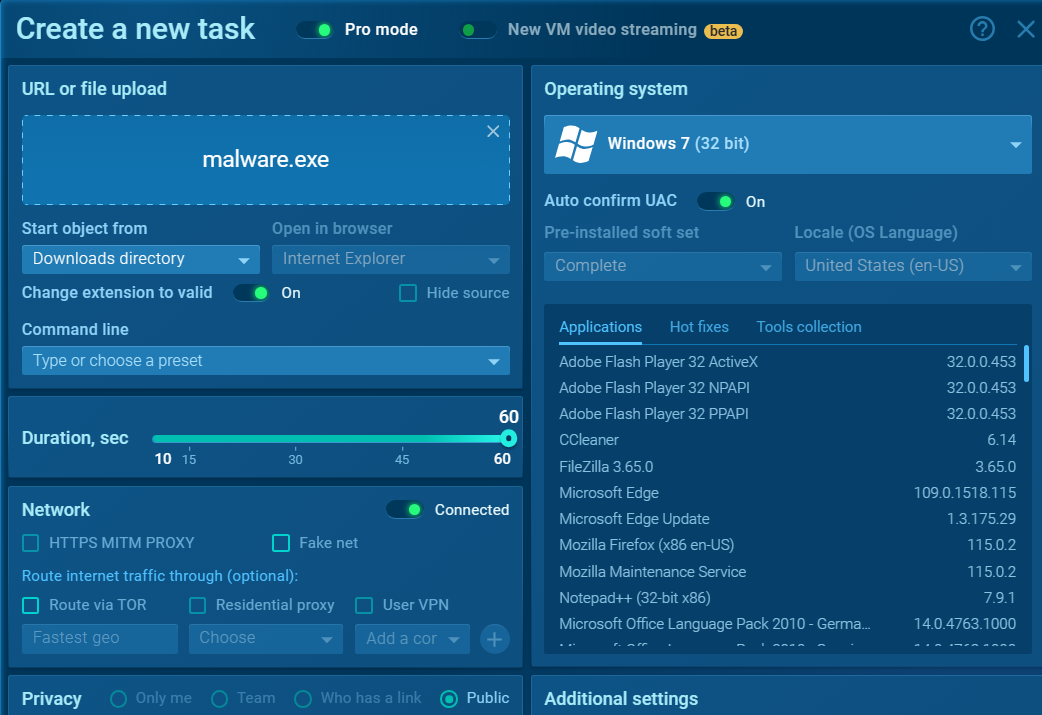
**Upload the file and**

**Choose the OS. (For free**

**Version only windows 7**

**Is available).**

**Creating task using PRO Mode:**

****

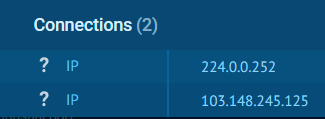
**Connections Made by Malware:**



**Mitre Attack Matrix:**

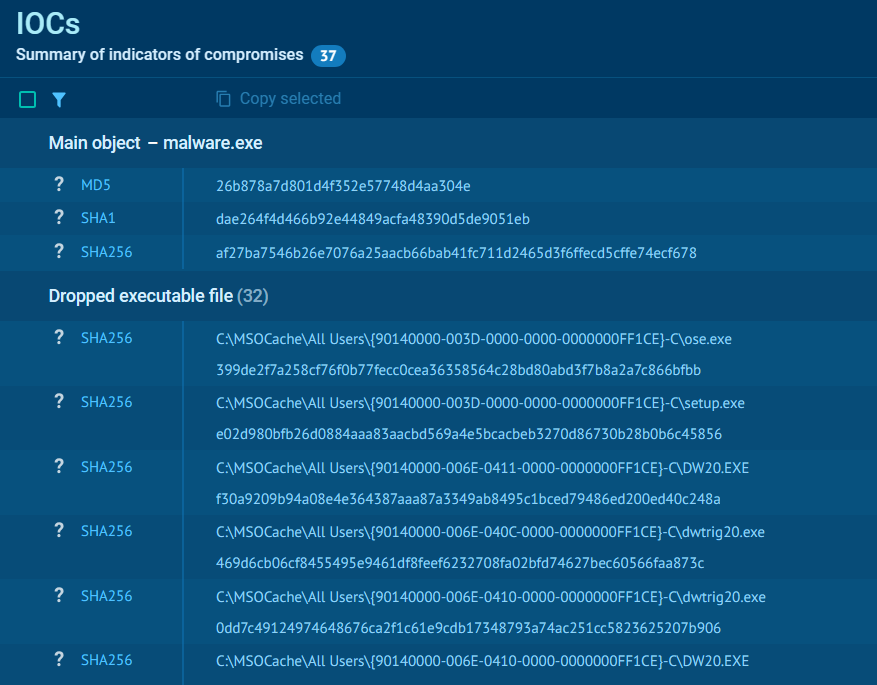


**Connection’s Made:**

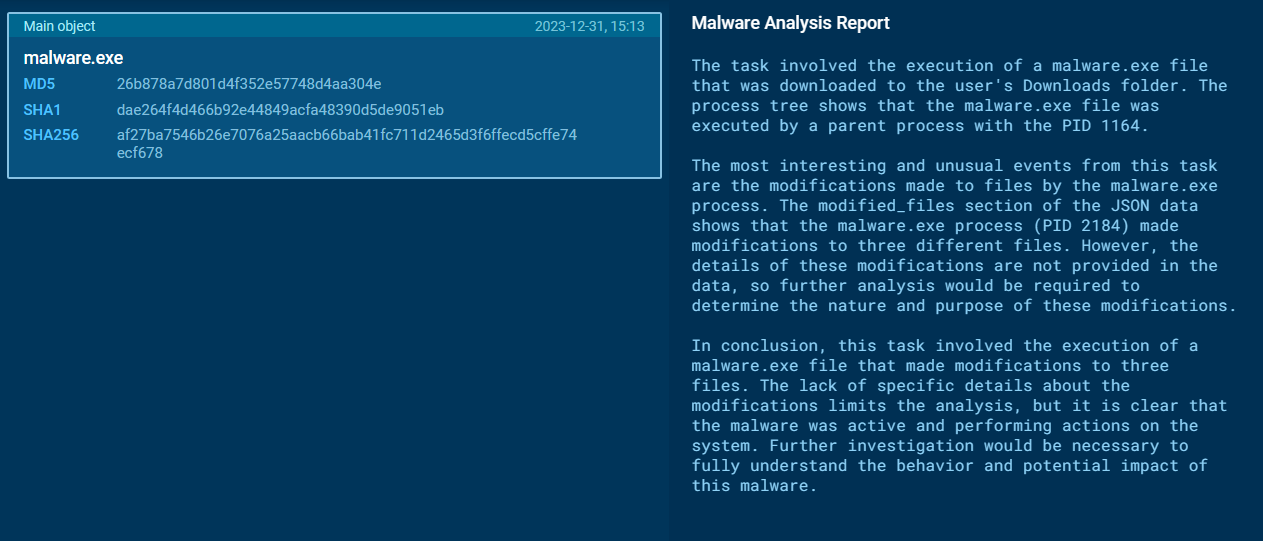
****

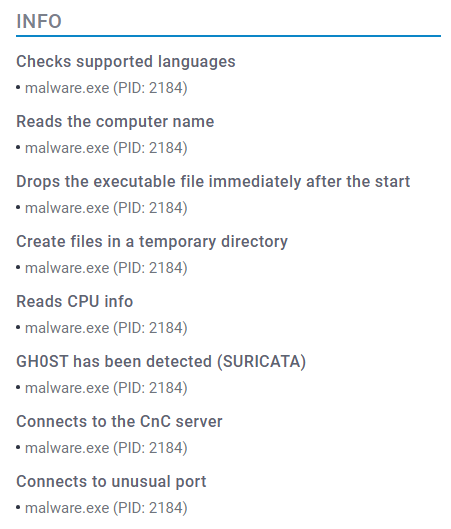
**IOC’s (Indicators of Compromise):**

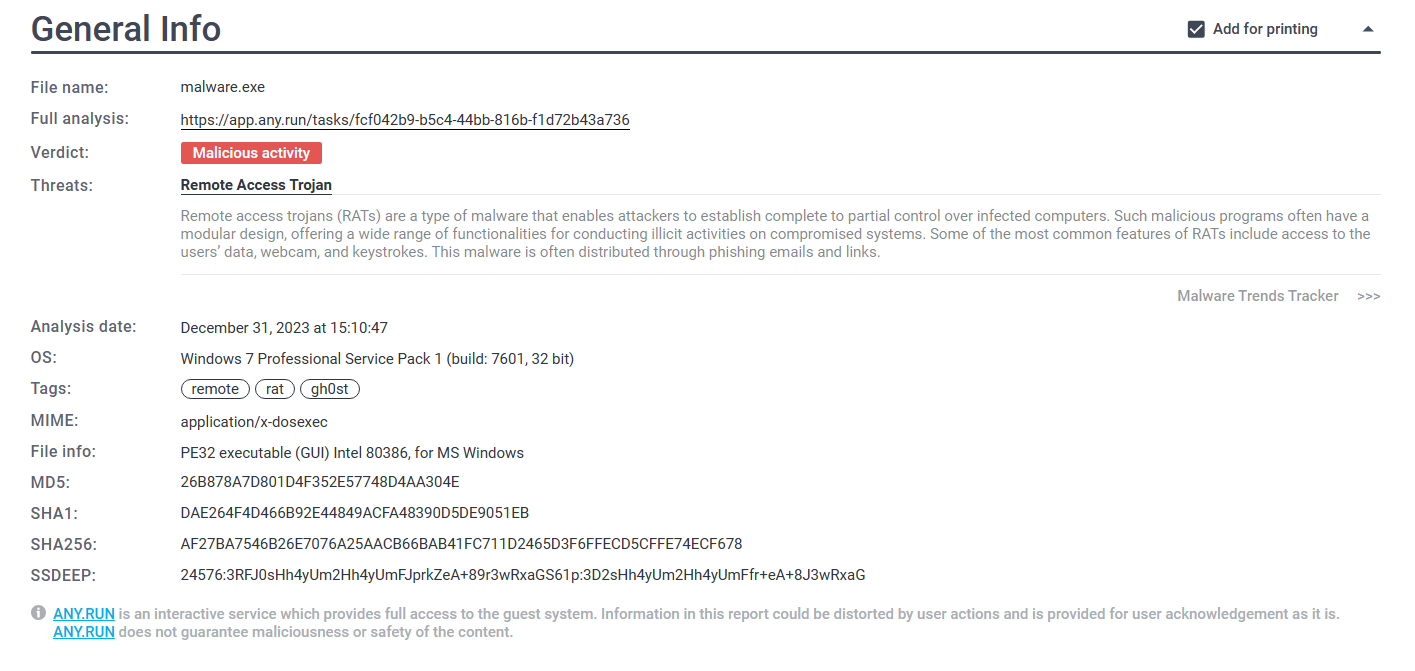
* IOC Report shows the indicator of compromise and show’s what files did malware create and where did it tried to make connections to.

****

**Quick Summary of Malware Analysis by ChatGPT**

****

**Text Report for Malware**

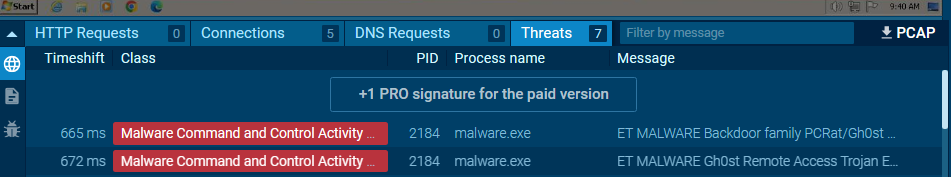


Text Report contains General info for the malware,

Behaviour activities, Video’s and screenshots, Process, Dropped Files, Malware Configuration, Static Information, Network Activity, DNS Requests, Threats.

This Text report can serve as a documented report that can be submitted to upper authorities for further analysis.

You can Even Download the malware activity as PCAP File for further analysis of malware.

****

Download PCAP File for further analysis.

**Additional Tool’s and Techniques for Dynamic Malware Analysis:**

* **Process Monitor –** To Monitor all the processes.
* **Regshot –** To Take Snapshot of machine (processes, services, registries etc) before and after execution of malware.
* **FakeNet-NG –** To Make malware think that it is being executed in actual network and send and receive requests which we can monitor.
* **ProcDOT –** For Visual Representation (Graph view) what malware is doing.

**Conclusion:**

The amalgamation of static and dynamic analysis methodologies proved to be instrumental in gaining a comprehensive understanding of the malware's attributes and potential threats. The static analysis provided crucial insights into the malware's inner workings and potential IOCs, while dynamic analysis offered real-time behavioural patterns and confirmed its malicious nature.

It's imperative to note that while these analyses shed light on the malware's current capabilities and behaviour, the threat landscape is constantly evolving. Continuous monitoring, proactive security measures, and regular updates to detection mechanisms are crucial to mitigate the risks posed by such malware and safeguard against future variants or similar threats.

In conclusion, the findings obtained through static and dynamic malware analysis serve as a foundation for developing robust security measures, enhancing threat intelligence, and fortifying defenses against similar cyber threats, thereby bolstering the resilience of systems and networks in the face of evolving cyber risks.

This report aims to aid in the formulation of proactive strategies, facilitating better threat detection, and enabling swift response protocols to counter potential malware attacks effectively.