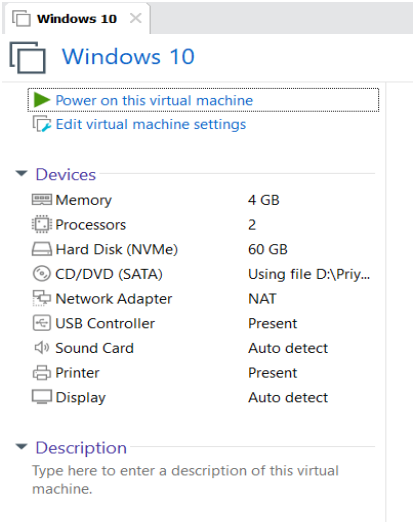
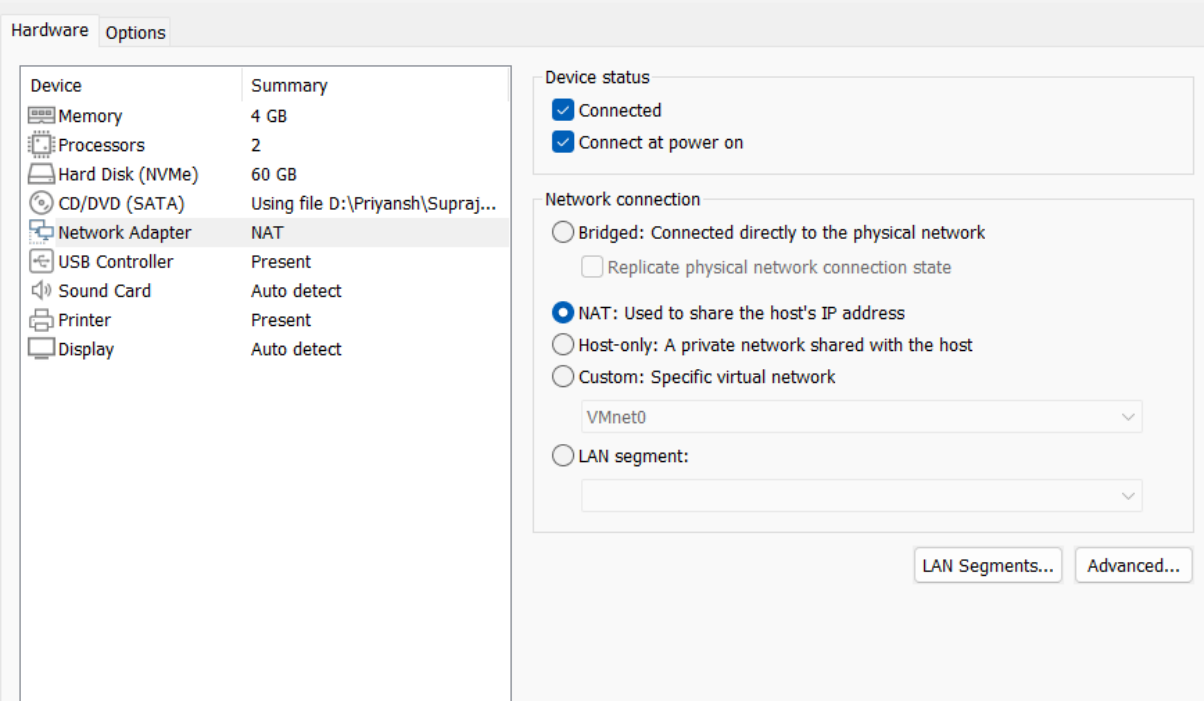
Malware Analysis

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.

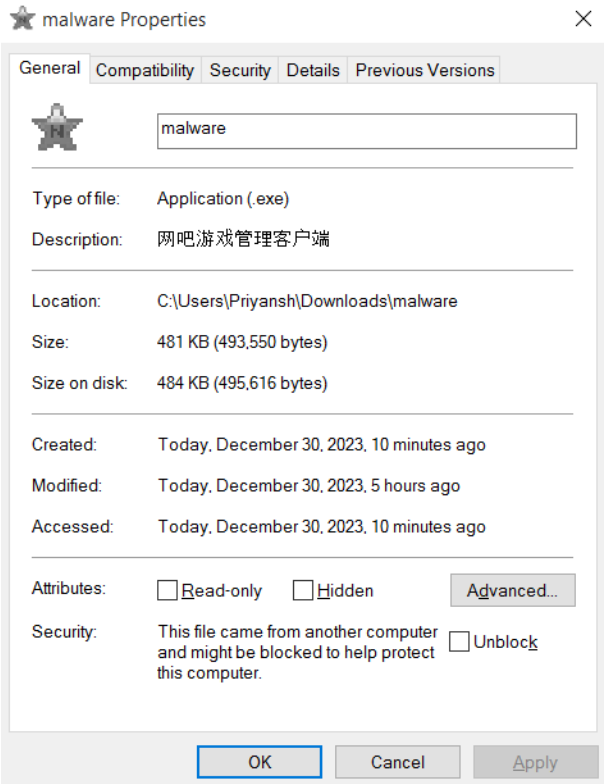
Search the malware in malware bazar and download it in your VM Machine

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

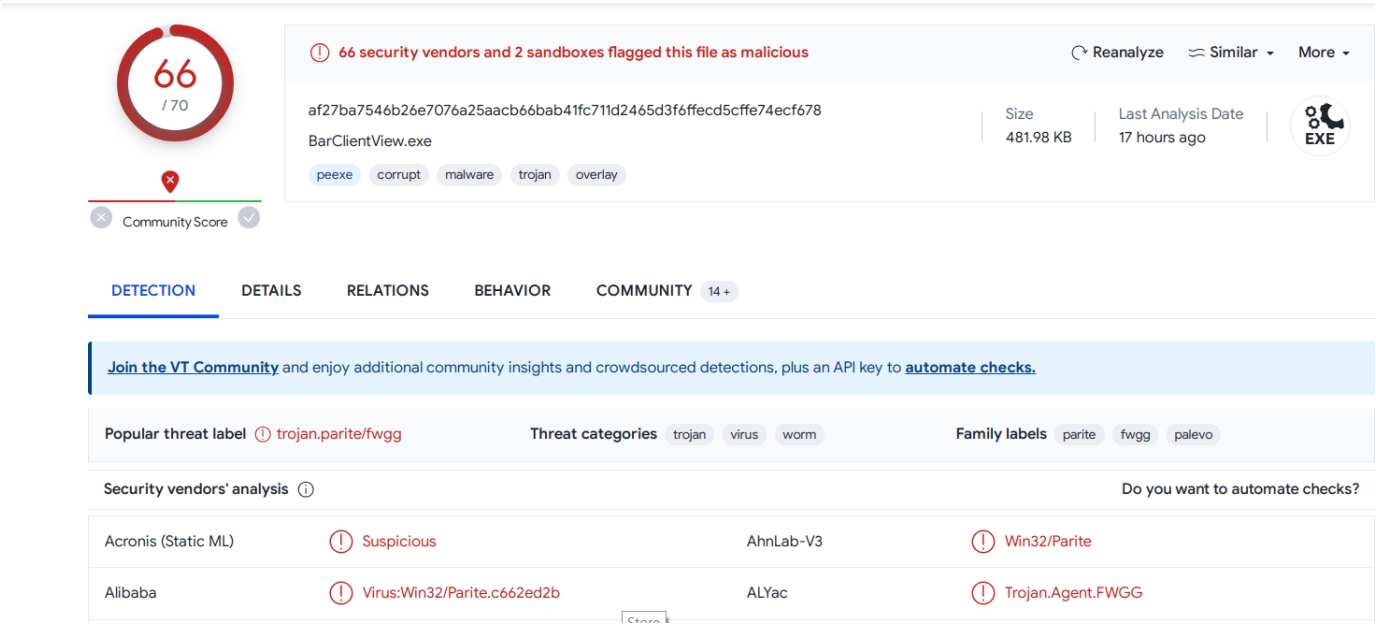
Virus total:

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

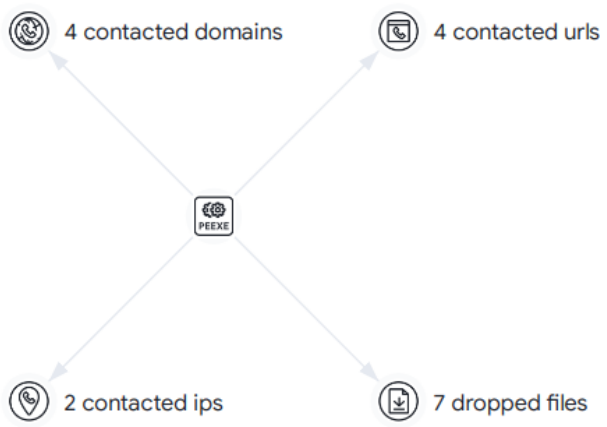
Contacted IP Address's by the Malware

Contacted IP addresses (2)

IP	Detections	Autonomous System	Country
103.148.245.125	9 / 89	142032	HK
172.64.149.23	1 / 89	13335	US

Graph View

Graph Summary



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:

```
┌──(priyansh㉿Kali)-[~/Desktop/malware]
└─$ strings malware.exe
!This program cannot be run in DOS mode.
1CRich
.text
`.rdata
.data
```

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.

```
┌──(priyansh㉿Kali)-[~/Desktop/malware]
└─$ file malware.jpg
malware.jpg: PE32 executable (GUI) Intel 80386, for MS Windows, 5 sections
```

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

Registries changes made by the malware:

```
C:\3389.bat
del %0
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\WinStations\RDP-Tcp /v PortNumber /t REG_DWORD /d
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\Wds\rdpwd\Tds\tcp /v PortNumber /t REG_DWORD /d
```

Hex Values

Tool : Hxd / xxd / hexeditor

```
└$ xxd malware.exe
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 f000 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS 
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: 52e4 5f10 1685 3143 1685 3143 1685 3143  R._...1C..1C..1C
```

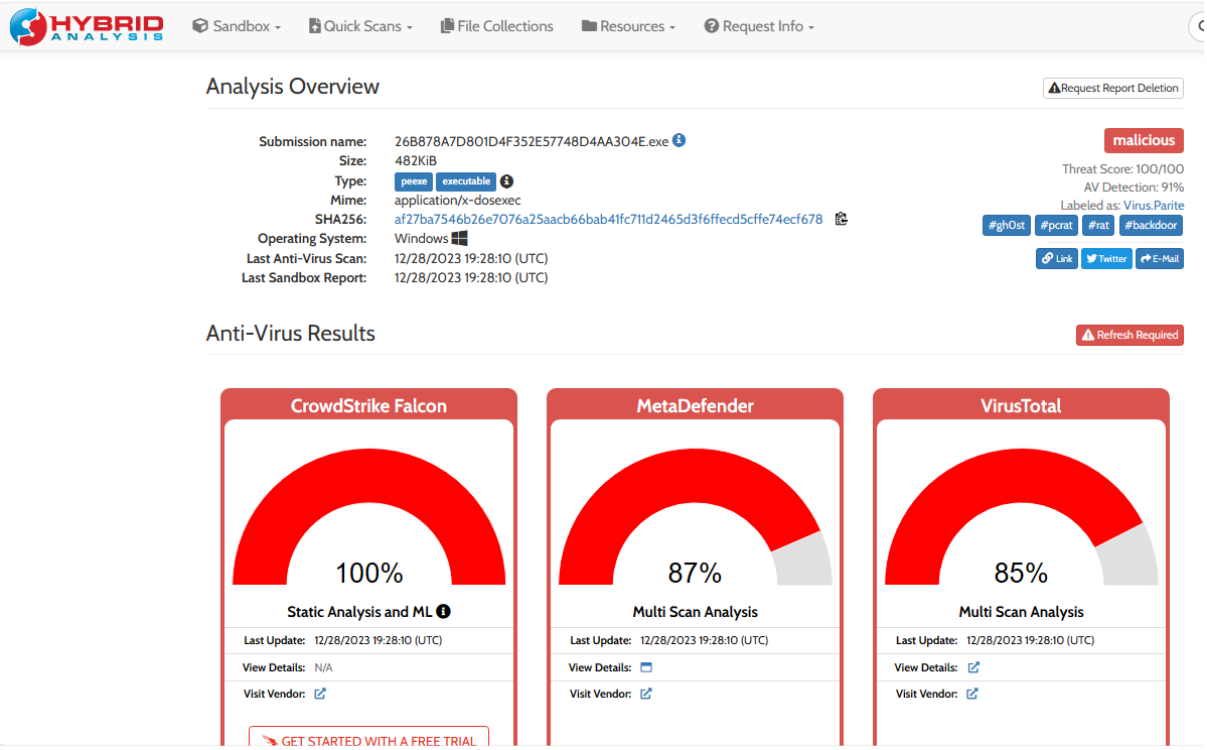
Known Signatures:

- **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:

Files extracted during detonation

Name	Verdict
bounty-4355486834715030 8 f4bda934383ae6eb2f7a35dc28794380f802ada4d36ea24b5c74bc3870d61620	malicious
file 7fdf10ca02d2238e22fda18dfbede9750da9f2572218 02c8b86c557c19c9bc7b	malicious
phcBE70.tmp d2317462d3932387fa844c7e275d2c3e3162056b22a609314b57ba6f2a779b9f	malicious

Incident Response

Risk Assessment:

Detected Gh0st Rat (Remote Access Trojan)

Risk Assessment

Remote Access	Detected GhOst RAT network traffic pattern
Stealer/Phishing	Tries to steal Mail credentials from registry
Persistence	Drops executable files to the application program directory (%ProgramData%) Modifies auto-execute functionality by setting/creating a value in the registry Writes a file to the startup folder
Fingerprint	Queries kernel debugger information Queries process information Queries sensitive IE security settings Queries the internet cache settings (often used to hide footprints in index.dat or internet cache) Tries to steal Mail credentials from registry
Evasive	Input file contains API references not part of its Import Address Table (IAT) Possibly checks for the presence of a forensics/monitoring tool Possibly tries to evade analysis by sleeping many times The input sample contains a known anti-VM trick
Spyware	Found a string that may be used as part of an injection method
Network Behavior	Contacts 1 domain and 1 host. View all details

DNS Request's and Contacted Host's By Malware

DNS Request

Domain: www.sock18.com

Contacted Hosts:

IP: 103.148.245.125

Network Analysis Overview

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
www.sock8.com	-	-	-

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
103.148.245.125	-	-	Country n/a

IP Geolocator:

IP Geolocator Reveals that the IP Address

To which malware tried to contact/connect

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

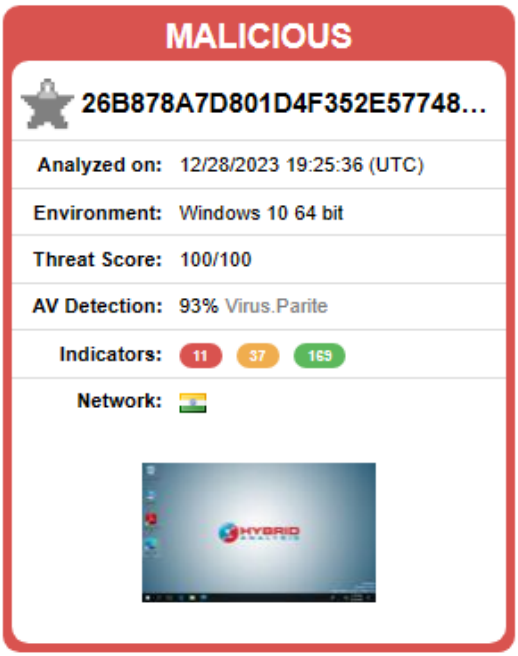
Enter any IPv4, IPv6 address or domain name:

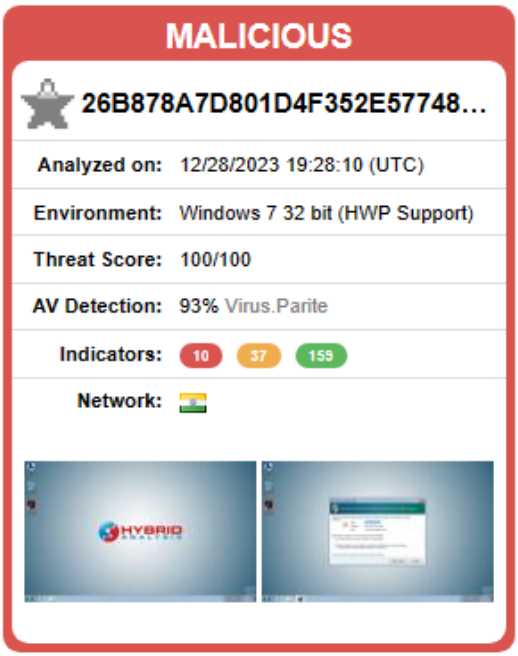
103.148.245.125


```
"ip": "103.148.245.125",
"country_name": "Hong Kong",
"state_prov": "Hong Kong SAR",
"city": "Hong Kong",
"latitude": "22.27728",
"longitude": "114.22913",
"time_zone": "Asia/Hong_Kong",
"isp": "Chihong International Co., Limited",
"currency": "Hong Kong Dollar",
"country_flag":
```


View More

Flacon Sandbox Report

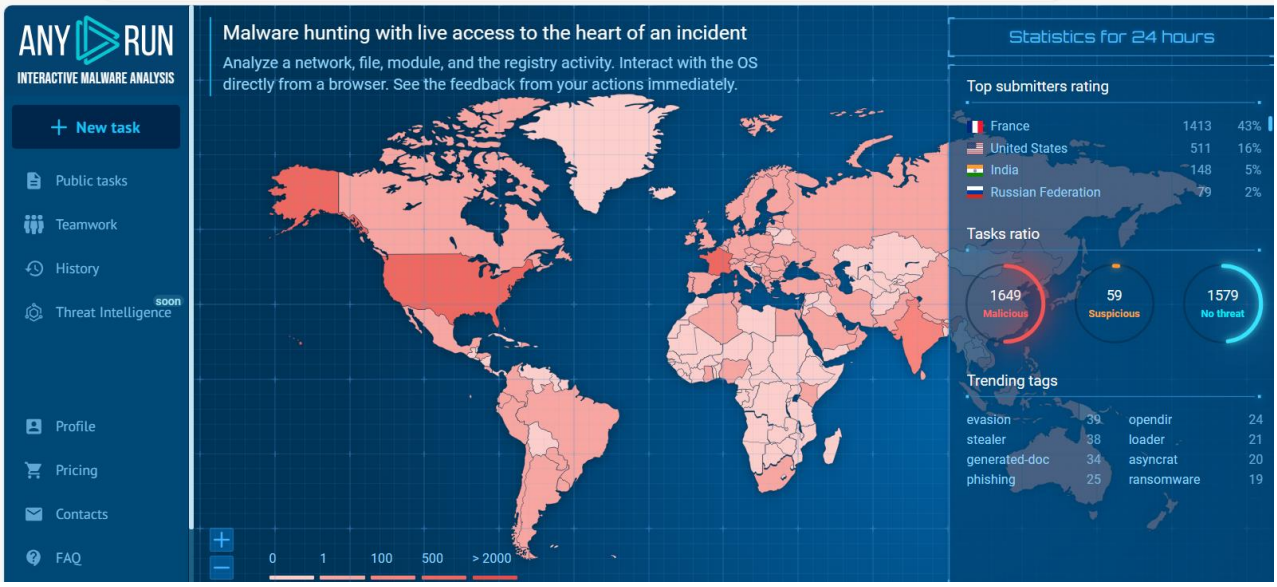




The analysis of Malware on Windows 10 (64-bit) conducted on 12/28/2023 revealed an alarming threat score of 100/100, indicating a highly malicious nature. Notably, 93% of antivirus engines flagged the file as **“Virus, Parite”**.

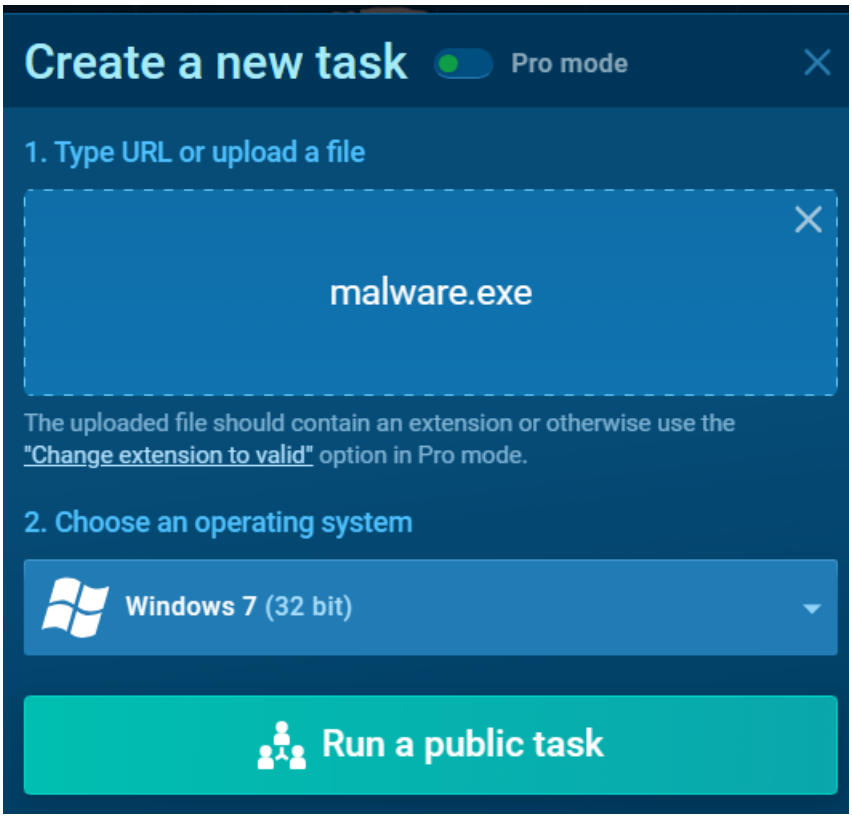
AnyRun.com:

Overview Of Dashboard

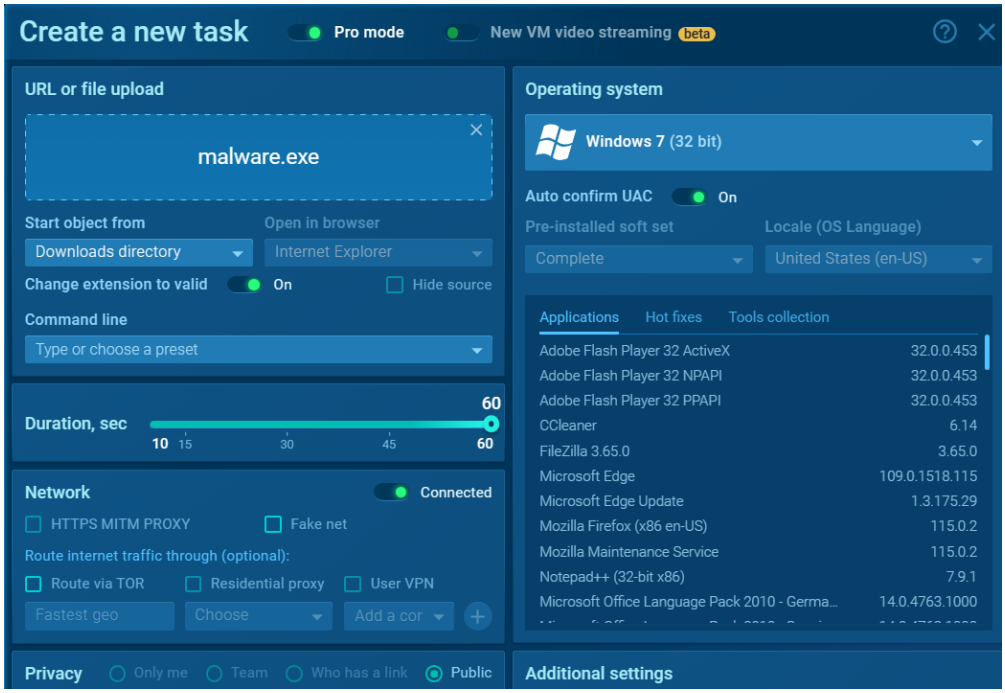


Create a New Task

Upload the file and Choose the OS. (For free Version only windows 7 Is available).



Creating task using PRO Mode:



Connections Made by Malware:

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN
469 ms	UDP	✓	4	System	?	192.168.100.255	138	–	–
474 ms	TCP	?	2184	malware.exe	☆	103.148.245.125	999	–	High Family T...
475 ms	UDP	✓	4	System	?	192.168.100.255	137	–	–
2467 ms	UDP	?	1080	svchost.exe	?	224.0.0.252	5355	–	–

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.

IOCs

Summary of indicators of compromises 37

Copy selected

Main object – malware.exe

MD5	26b878a7d801d4f352e57748d4aa304e
SHA1	dae264f4d466b92e44849acfa48390d5de9051eb
SHA256	af27ba7546b26e7076a25aacb66bab41fc711d2465d3f6ffecd5cffe74ecf678

Dropped executable file (32)

SHA256	C:\MSOCache\All Users\{90140000-003D-0000-0000-0000000FF1CE}-C\ose.exe 399de2f7a258cf76f0b77fecc0cea36358564c28bd80abd3f7b8a2a7c866bfbb
SHA256	C:\MSOCache\All Users\{90140000-003D-0000-0000-0000000FF1CE}-C\setup.exe e02d980bfb26d0884aaa83aacbd569a4e5bcacbeb3270d86730b28b0b6c45856
SHA256	C:\MSOCache\All Users\{90140000-006E-0411-0000-0000000FF1CE}-C\DW20.EXE f30a9209b94a08e4e364387aaa87a3349ab8495c1bced79486ed200ed40c248a
SHA256	C:\MSOCache\All Users\{90140000-006E-040C-0000-0000000FF1CE}-C\dwtrig20.exe 469d6cb06cf8455495e9461df8feef6232708fa02bfd74627bec60566faa873c
SHA256	C:\MSOCache\All Users\{90140000-006E-0410-0000-0000000FF1CE}-C\dwtrig20.exe 0dd7c49124974648676ca2f1c61e9cdb17348793a74ac251cc5823625207b906
SHA256	C:\MSOCache\All Users\{90140000-006E-0410-0000-0000000FF1CE}-C\DW20.EXE

Quick Summary of Malware Analysis by ChatGPT

Main object 2023-12-31, 15:13

malware.exe

MD5	26b878a7d801d4f352e57748d4aa304e
SHA1	dae264f4d466b92e44849acfa48390d5de9051eb
SHA256	af27ba7546b26e7076a25aacb66bab41fc711d2465d3f6ffecd5cffe74 ecf678

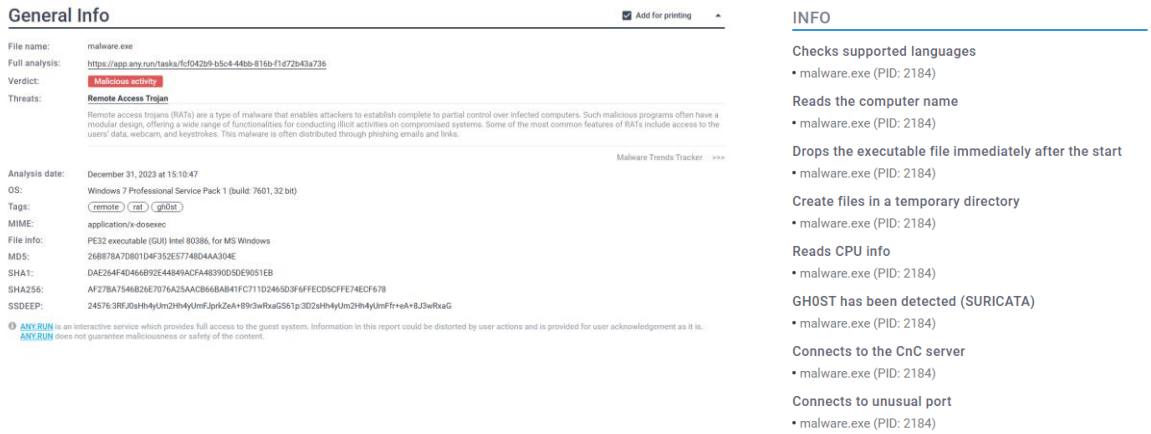
Malware Analysis Report

The task involved the execution of a malware.exe file that was downloaded to the user's Downloads folder. The process tree shows that the malware.exe file was executed by a parent process with the PID 1164.

The most interesting and unusual events from this task are the modifications made to files by the malware.exe process. The modified_files section of the JSON data shows that the malware.exe process (PID 2184) made modifications to three different files. However, the details of these modifications are not provided in the data, so further analysis would be required to determine the nature and purpose of these modifications.

In conclusion, this task involved the execution of a malware.exe file that made modifications to three files. The lack of specific details about the modifications limits the analysis, but it is clear that the malware was active and performing actions on the system. Further investigation would be necessary to fully understand the behavior and potential impact of this malware.

Text Report for Malware

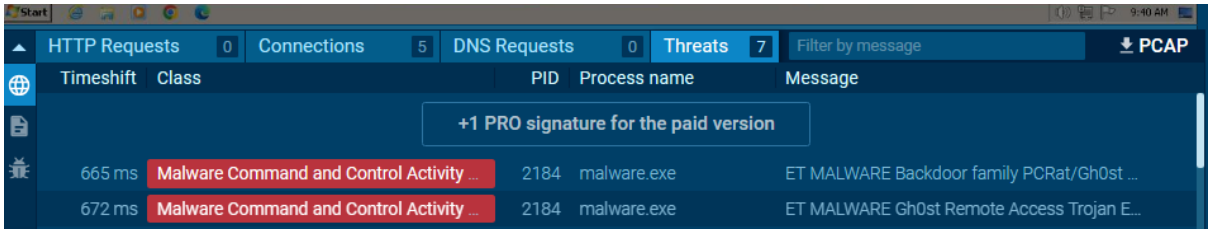


Text Report contains General info for the malware,

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.