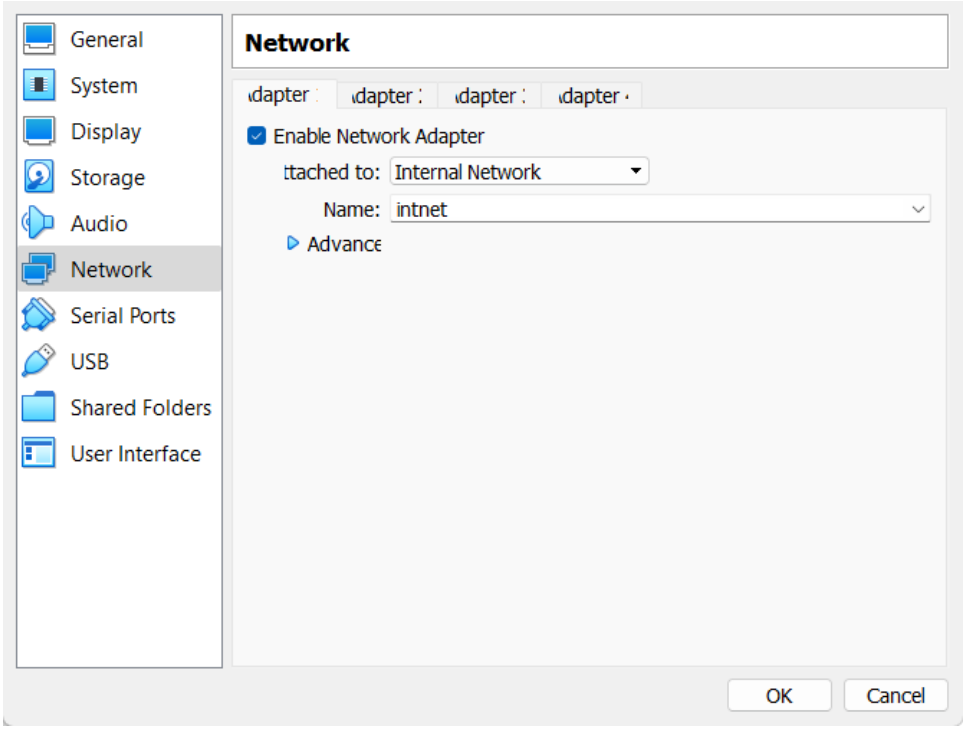
Malware Analysis Laboratory

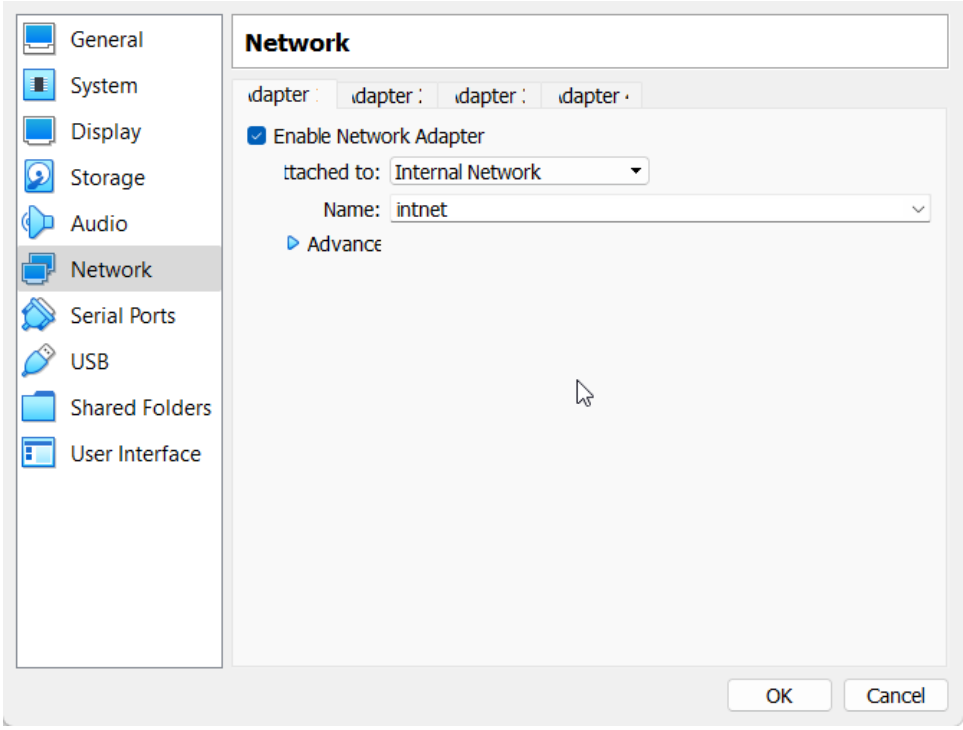
Network setup :

Changing to internal network for both of the virtual machines .

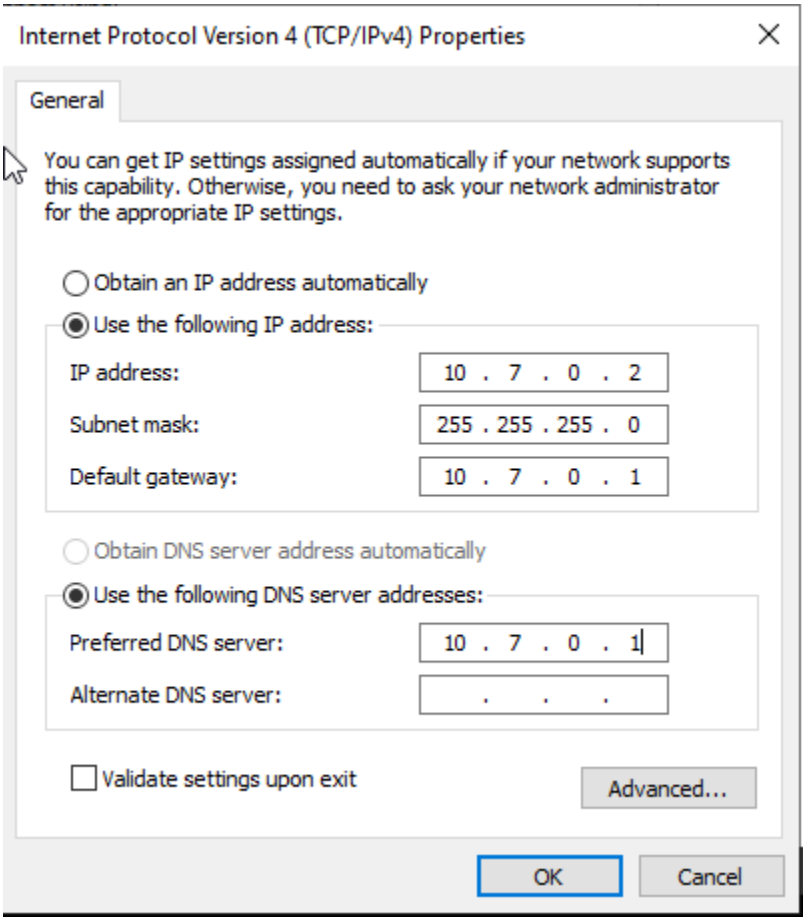
FlareVM



Remnux

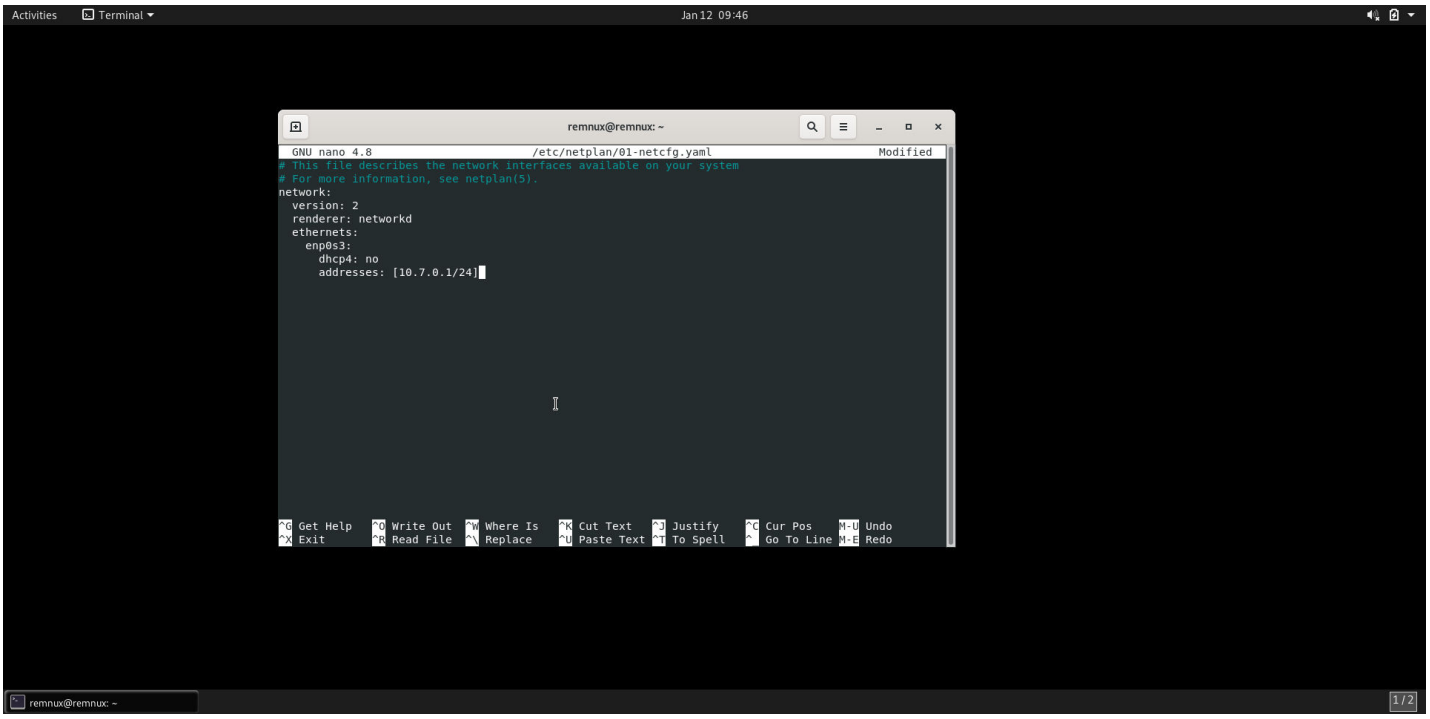

General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Enable Network Adapter
Internal Network
Name:
intnet
OK
Cancel

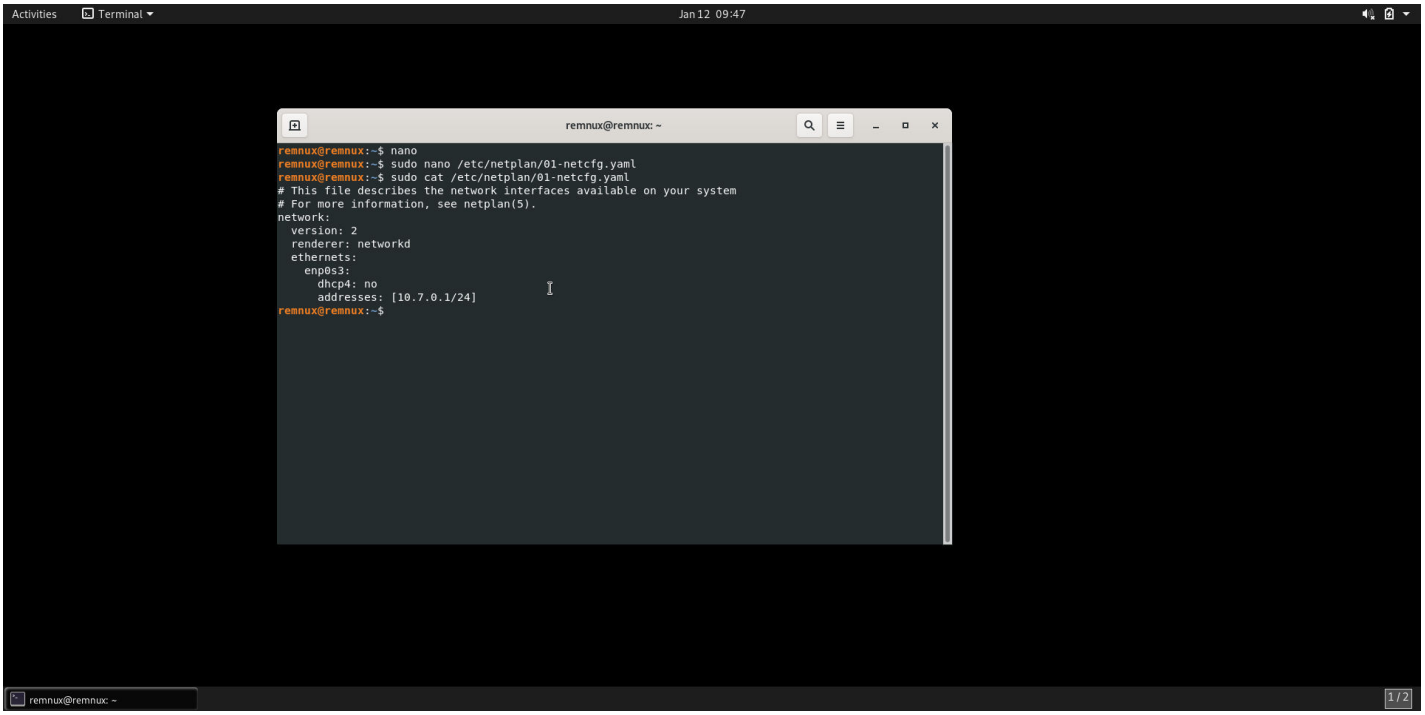
Ipv4 address change on flare virtual machine:



Inetsim configuration on remnux virtual machine :

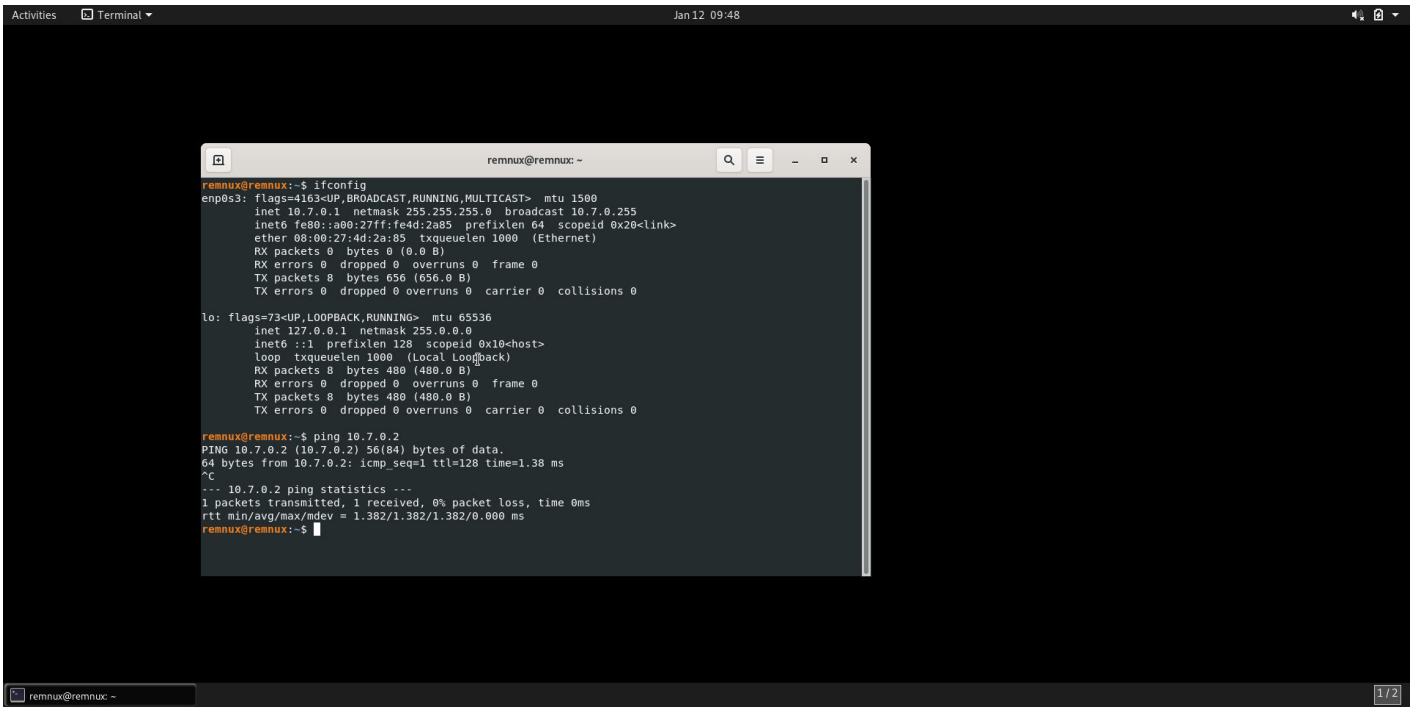
Network adapter ip address changing in configuration file :



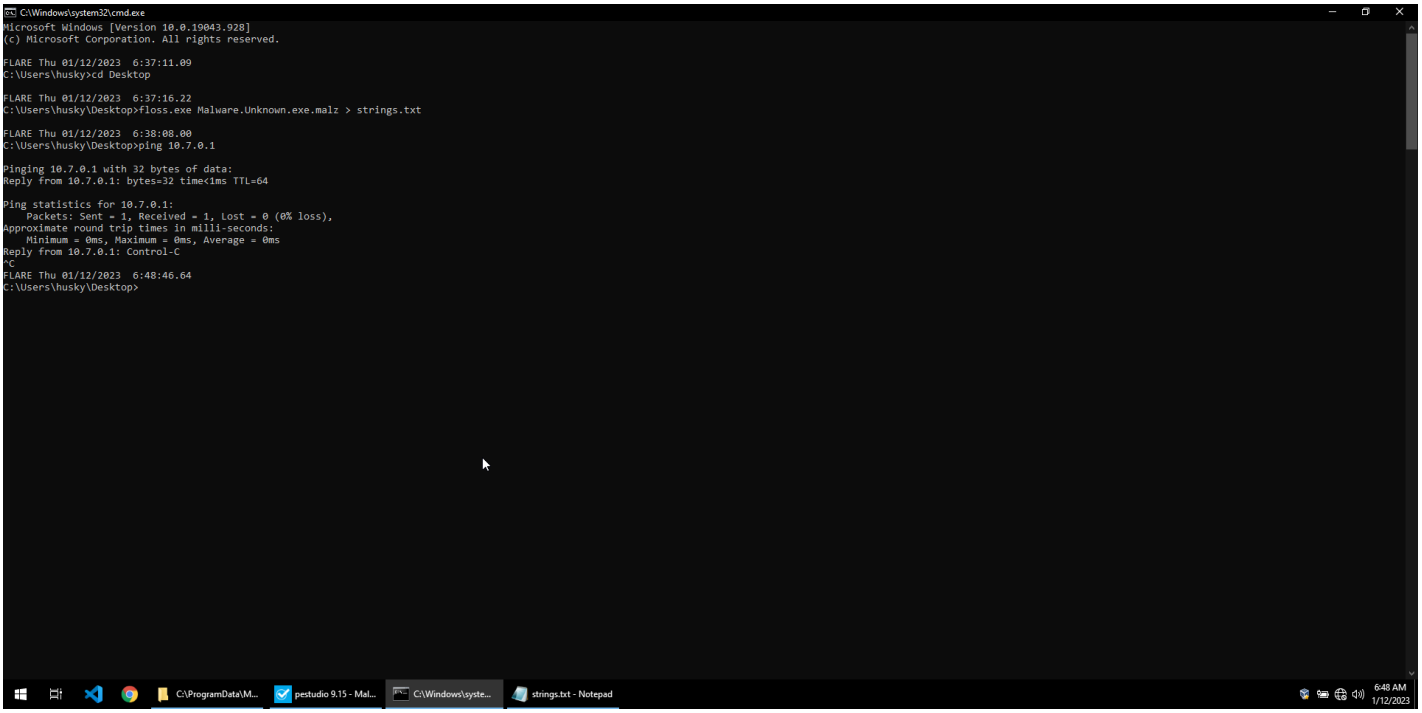


Connectivity check through ping tool :

Remnux

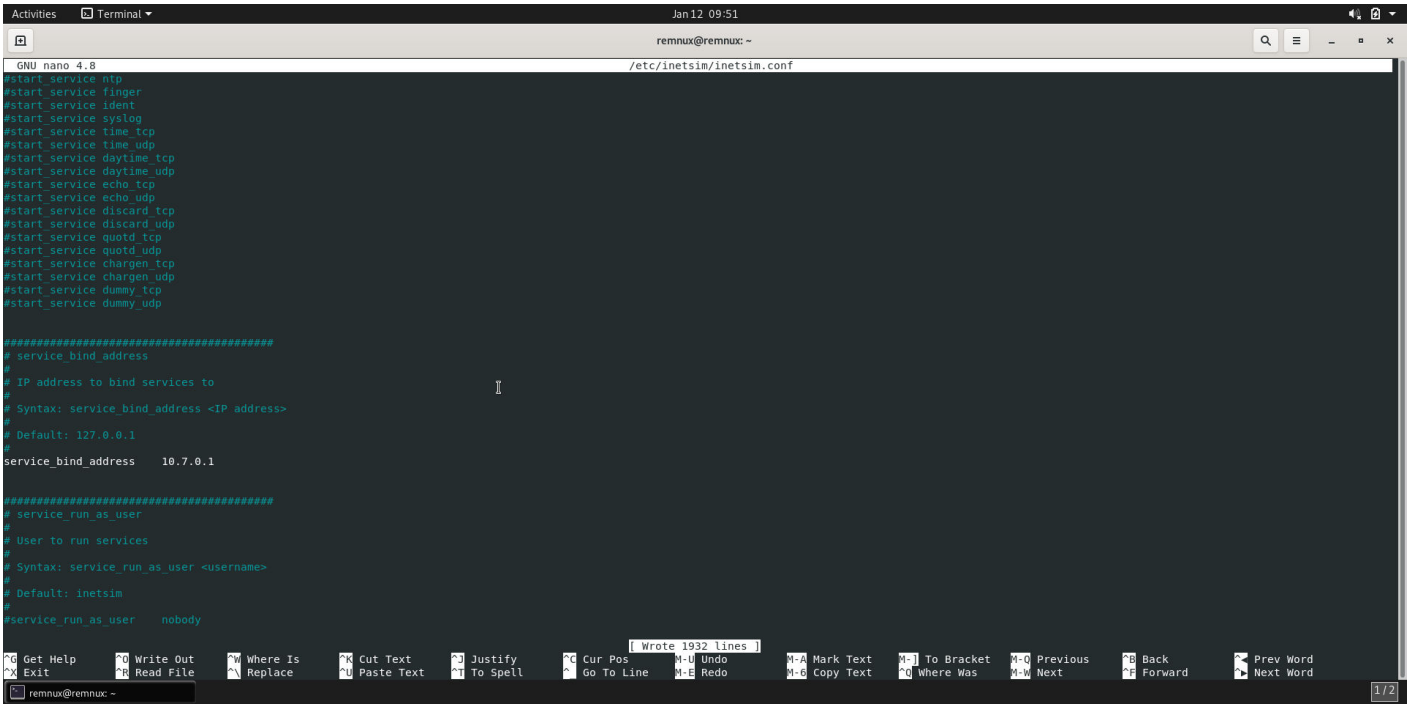


FlareVM


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.
FLARE Thu 01/12/2023 6:37:11.09
C:\Users\husky>cd Desktop
FLARE Thu 01/12/2023 6:37:16.22
C:\Users\husky\Desktop>floss.exe Malware.Unknown.exe.malz > strings.txt
FLARE Thu 01/12/2023 6:38:08.00
C:\Users\husky\Desktop>ping 10.7.0.1
Pinging 10.7.0.1 with 32 bytes of data:
Reply from 10.7.0.1: bytes=32 time<1ms TTL=64
Ping statistics for 10.7.0.1:
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Reply from 10.7.0.1: Control-C
^C
FLARE Thu 01/12/2023 6:48:46.64
C:\Users\husky\Desktop>
C:\ProgramData\M...
pestudio 9.15 - Mal...
C:\Windows\syste...
strings.txt - Notepad
6:48 AM
1/12/2023

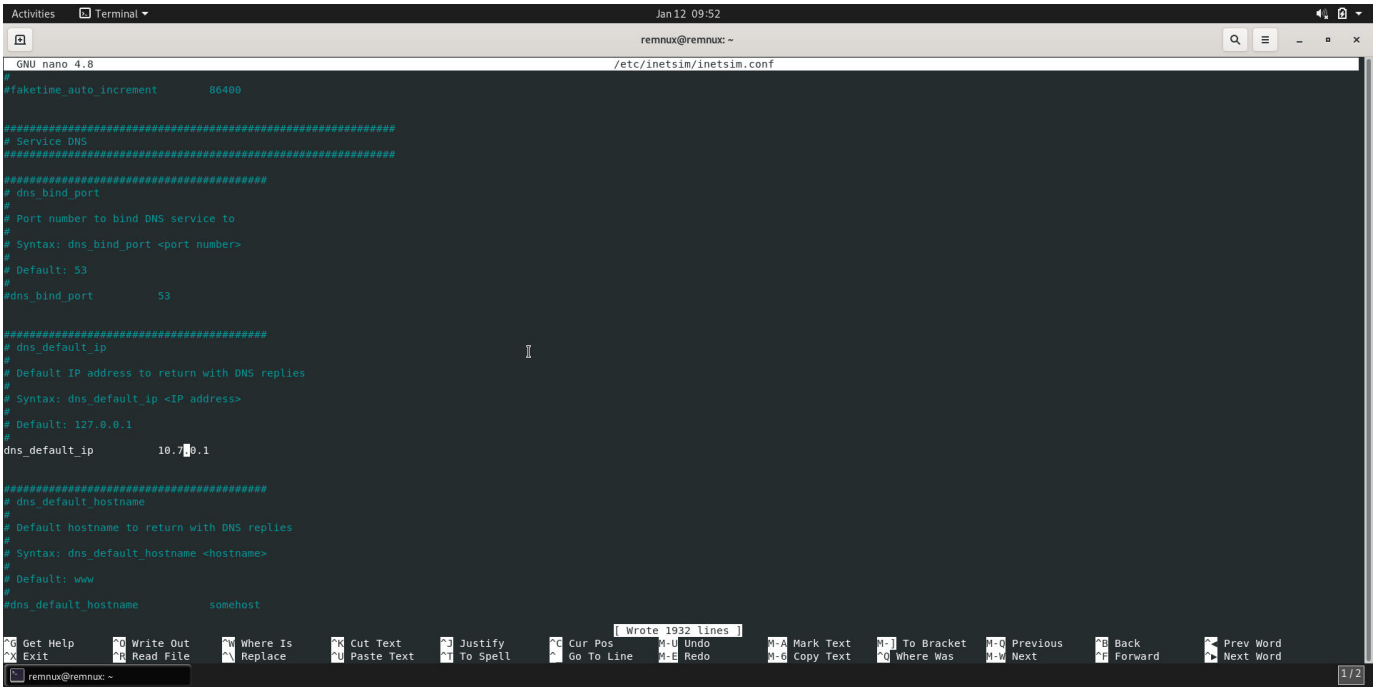
Inetsim configuration on remnux virtualmachine :

Service_bind_address 10.7.0.1



Changing dns ip:

Dns_default_ip 10.7.0.1



Start the DNS service :

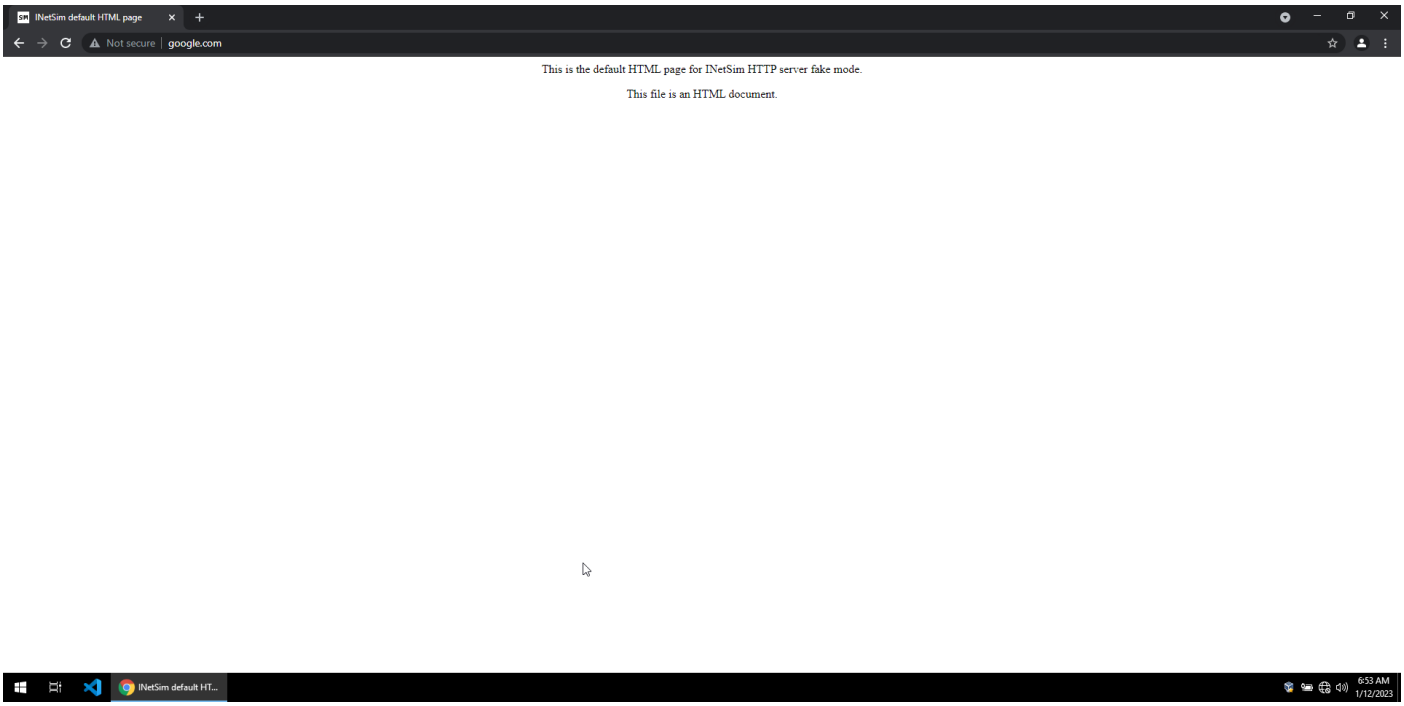
Start_service dns

```
Activities  Terminal  Jan 12 09:52
remnux@remnux: ~
 GNU nano 4.8                    /etc/inetsim/inetsim.conf                    Modified
##################################################################
#
# INetSim configuration file
#
##################################################################


##################################################################
# Main configuration
##################################################################

#########################################
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
                                        [ Search Wrapped ]
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text   M-] To Bracket   M-Q Previous   ^B Back   ^◀ Prev Word
^X Exit       ^R Read File   ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo   M-6 Copy Text   ^Q Where Was   M-W Next   ^F Forward   ^▶ Next Word
remnux@remnux: ~                                                                                                                                   1 / 2
```

Start the FakeNet network simulation:

```
Activities  Terminal  Jan 12 09:53
remnux@remnux: ~
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1441) ===
Session ID:     1441
Listening on:   10.7.0.1
Real Date/Time: 2023-01-12 09:53:06
Fake Date/Time: 2023-01-12 09:53:06 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 1445)
  * smtp_25_tcp - started (PID 1448)
  * http_80_tcp - started (PID 1446)
  * pop3_110_tcp - started (PID 1450)
  * https_443_tcp - started (PID 1447)
  * pop3s_995_tcp - started (PID 1451)
  * ftps_990_tcp - started (PID 1453)
  * smtps_465_tcp - started (PID 1449)
  * ftp_21_tcp - started (PID 1452)
 done.
Simulation running.
remnux@remnux: ~                                                                   1 / 2
```

On flareVM , accessing www.google.com , it is working :

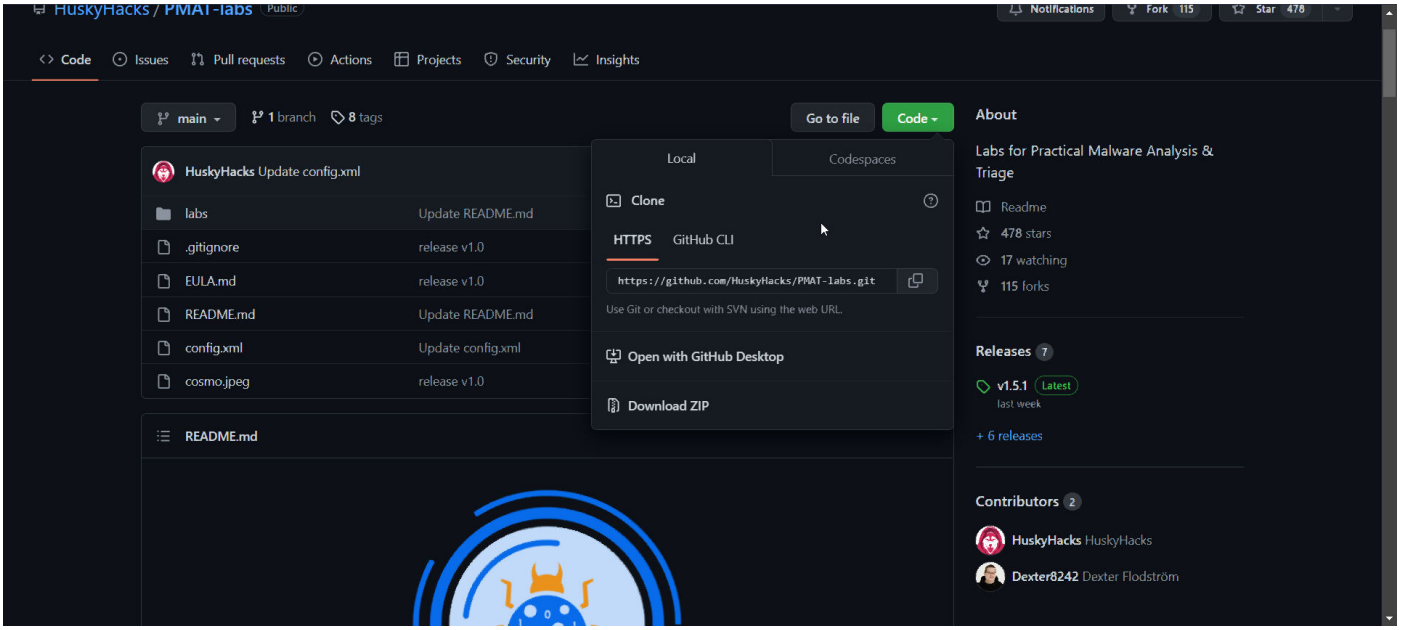


Static Analysis

I will do basic static malware analysis . I used laboratories from this github repository :

https://github.com/HuskyHacks/PMAT-labs

I downloaded it and dragged it to the flare vm from the host windows OS , on the desktop .



Analysis Type : Basic Static Malware Analysis

Malware:

- PMAT-labs-main\labs\1-1.BasicStaticAnalysis\Malware.Unknown.exe.malz

Hashes:

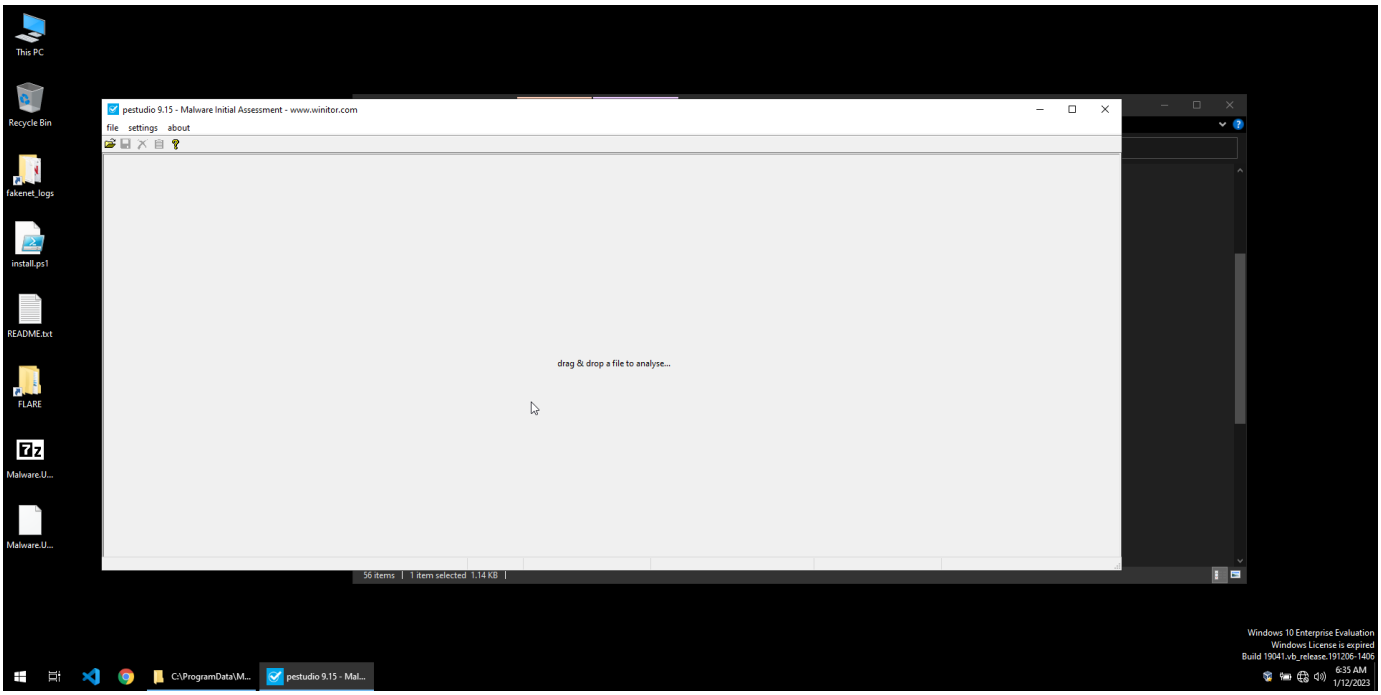
- Md5: 1D8562C0ADCAEE734D63F7BAACA02F7C
- Sha256: 92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A

Prepare malware to be analyzed

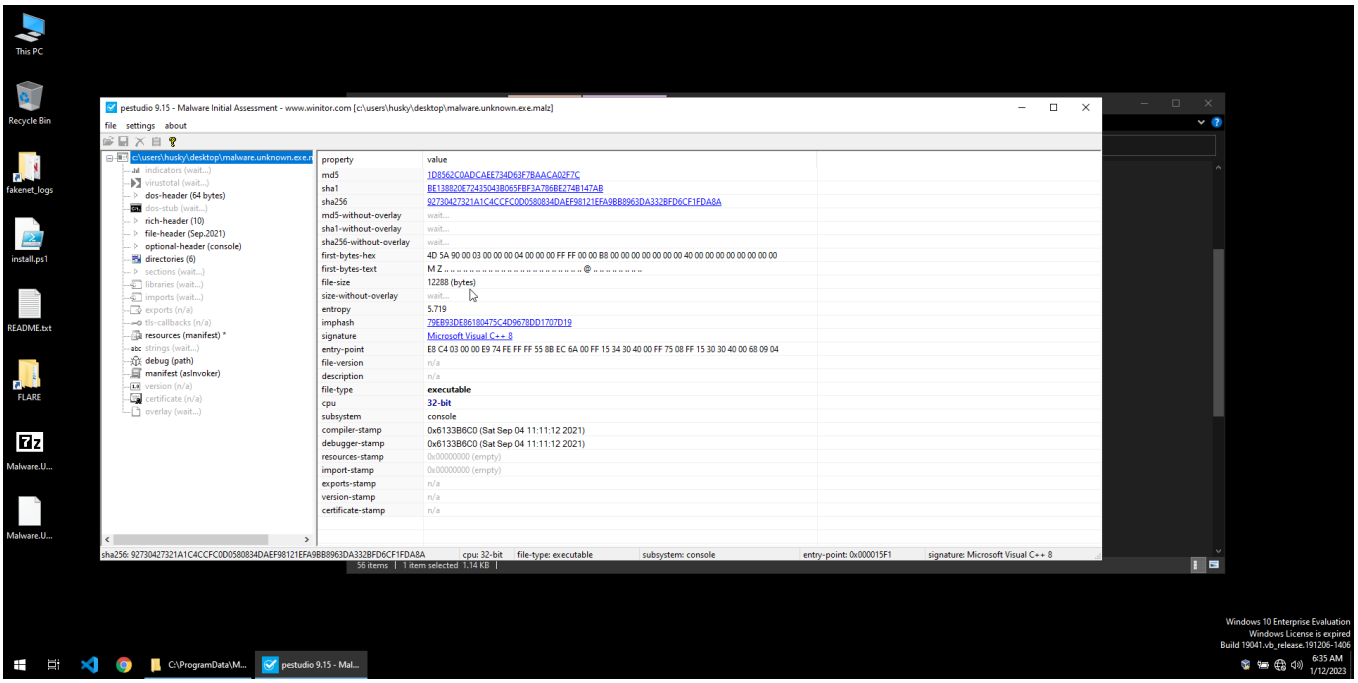
I dragged the malware , unarchive it and put it on desktop.

Check with pestudio

I used pestudio for static analysis of the malware.

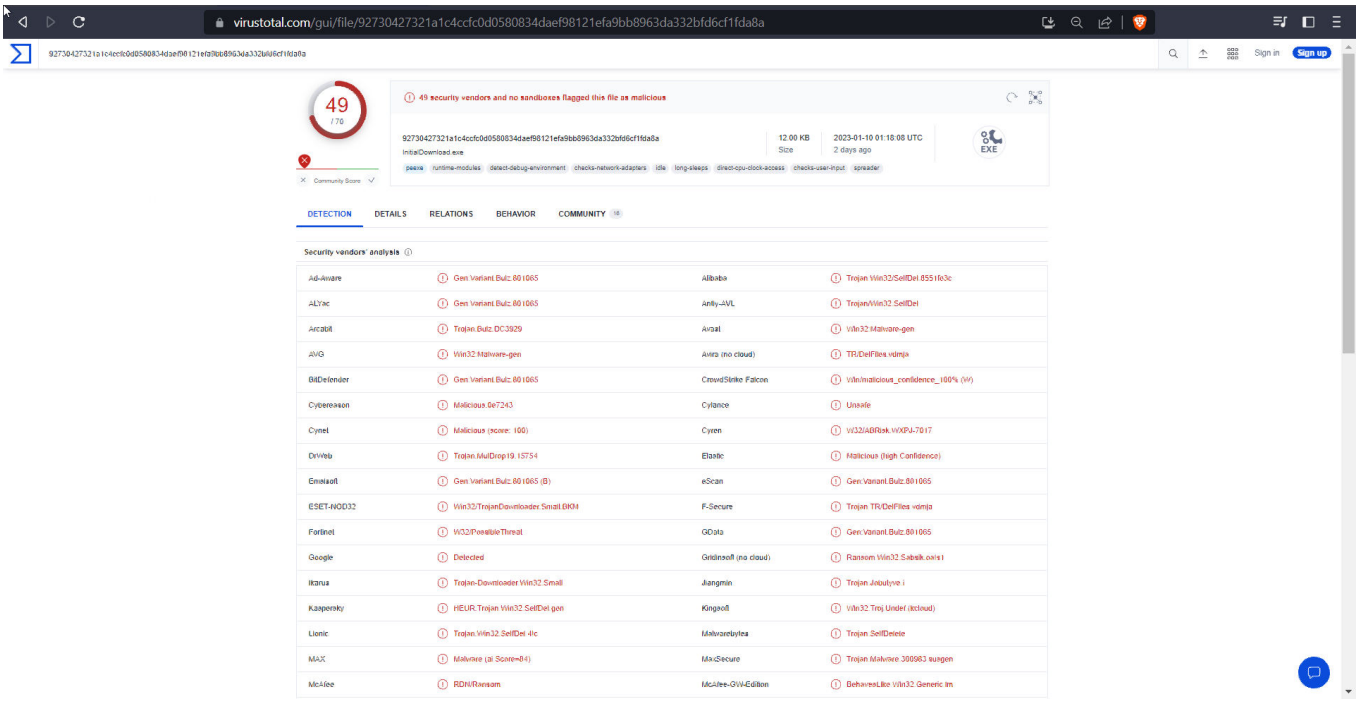


Getting the SHA256 and MD5 of the binary file .



Check signature on virustotal.com

I entered virustotal website and I found out more information about this malware based on SHA256 hash .

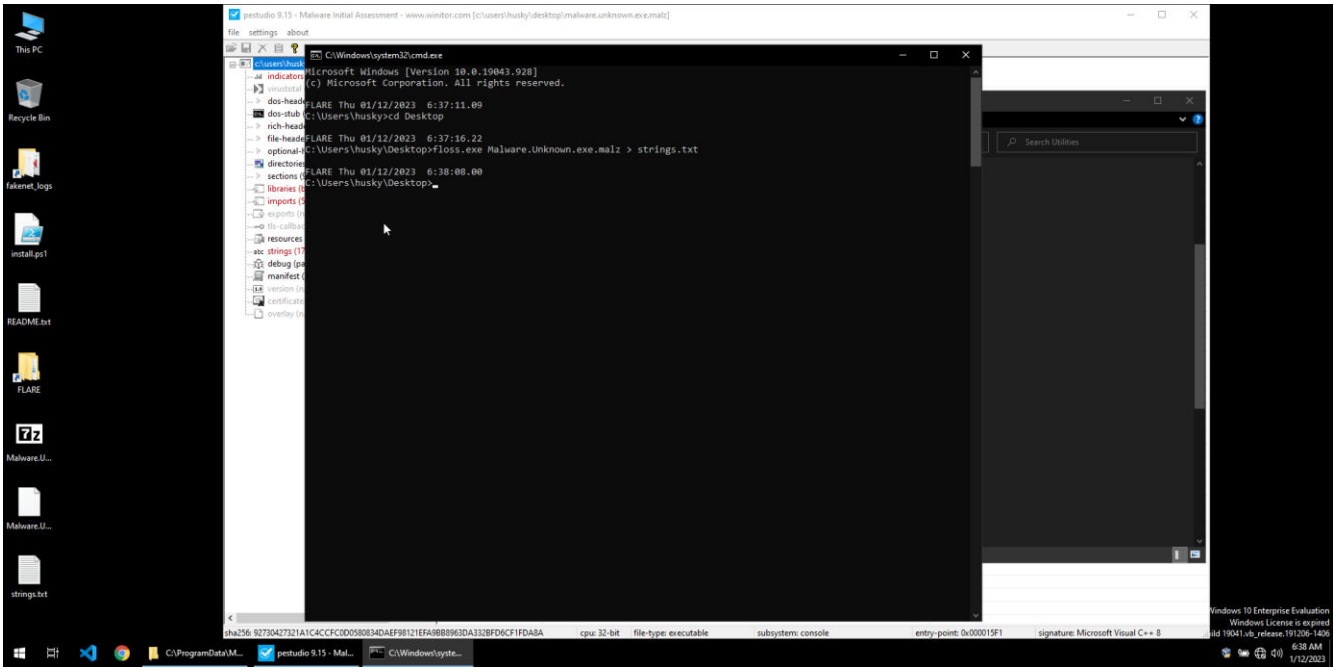


From the screenshot above , it is scanned and reported as a Trojan .

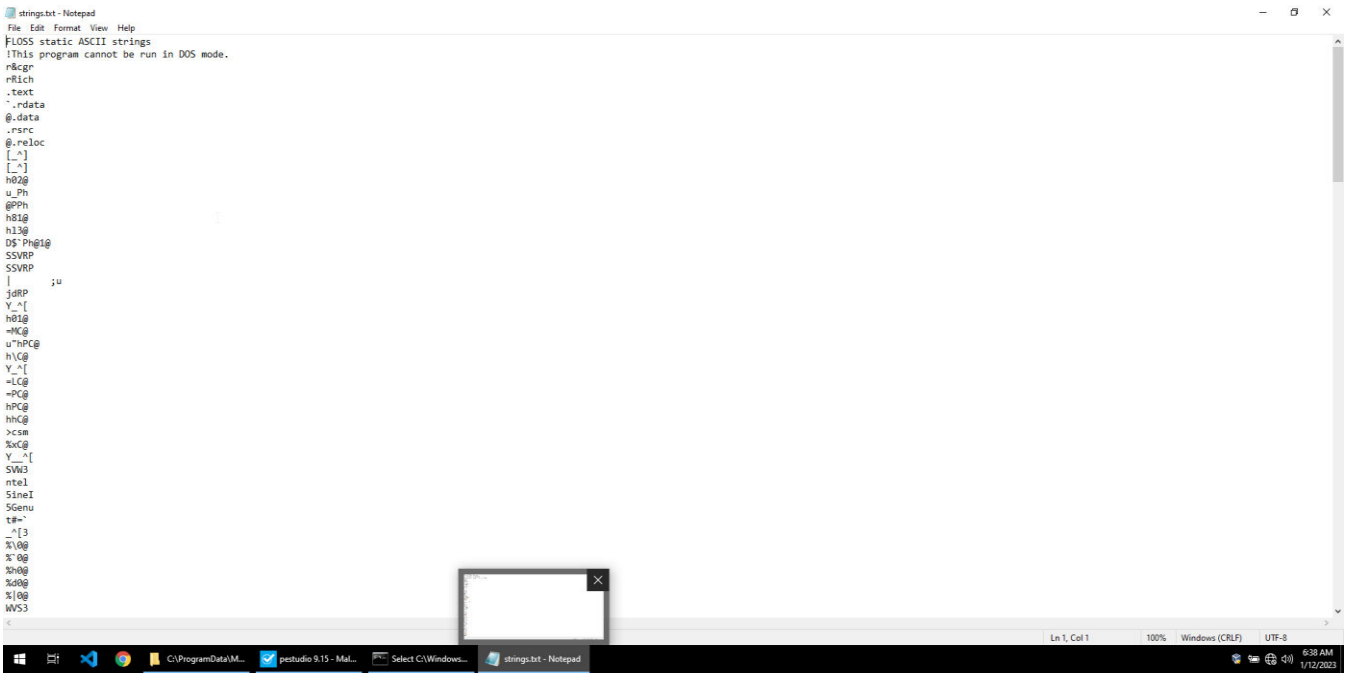
A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

Extract Strings

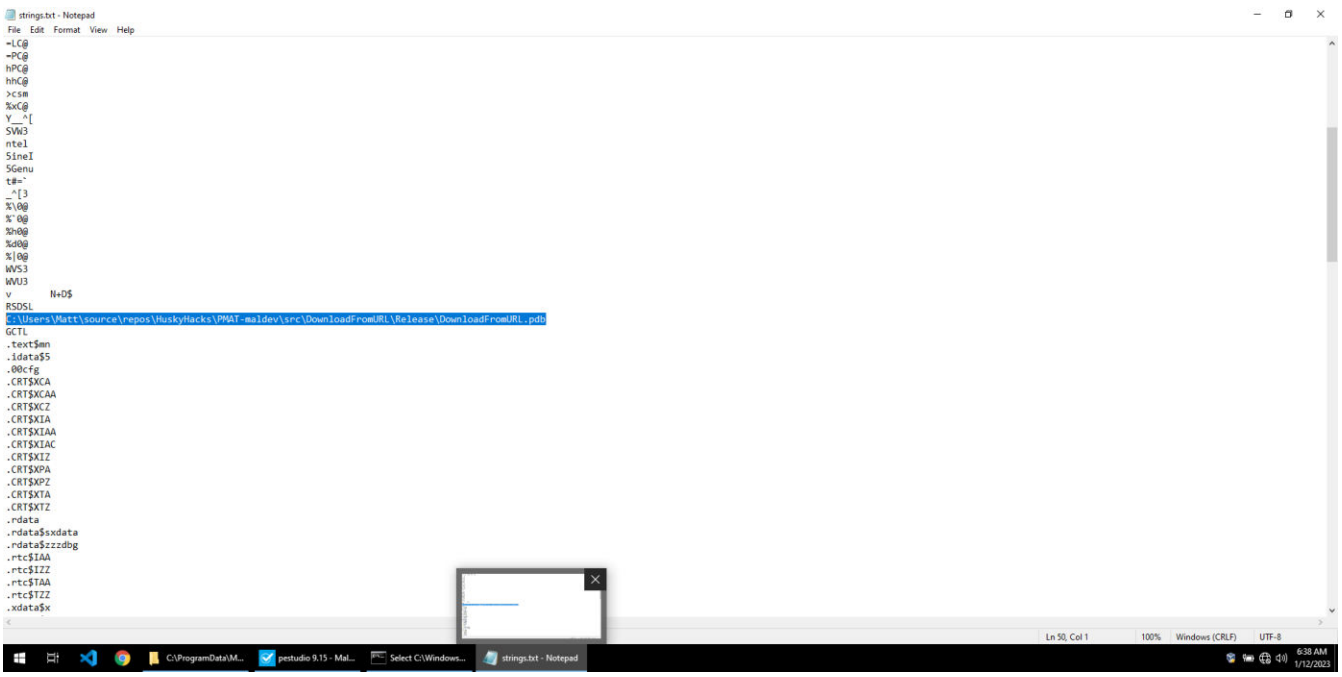
Now , strings will be extracted from the binary file trough floss.exe command and put in a text file .



The text file owned after the command execution :

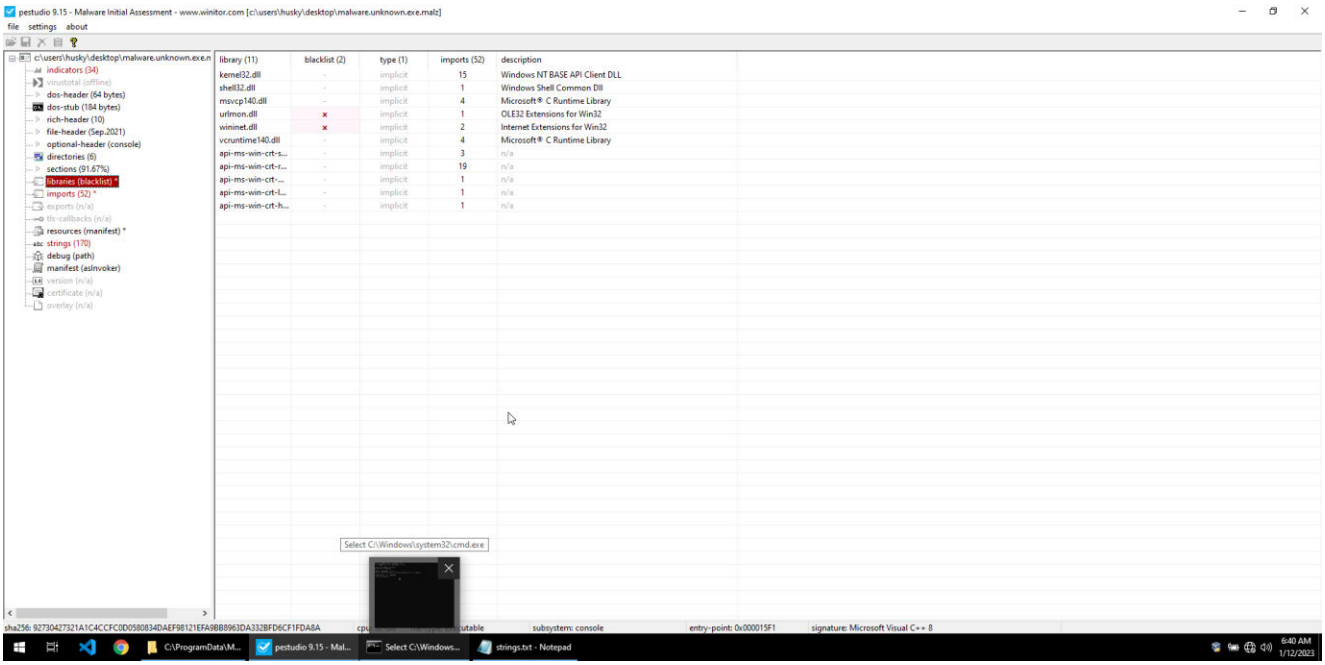


A program database is seen in the strings , the malware could work with this database , or dragged in to the computer from it .

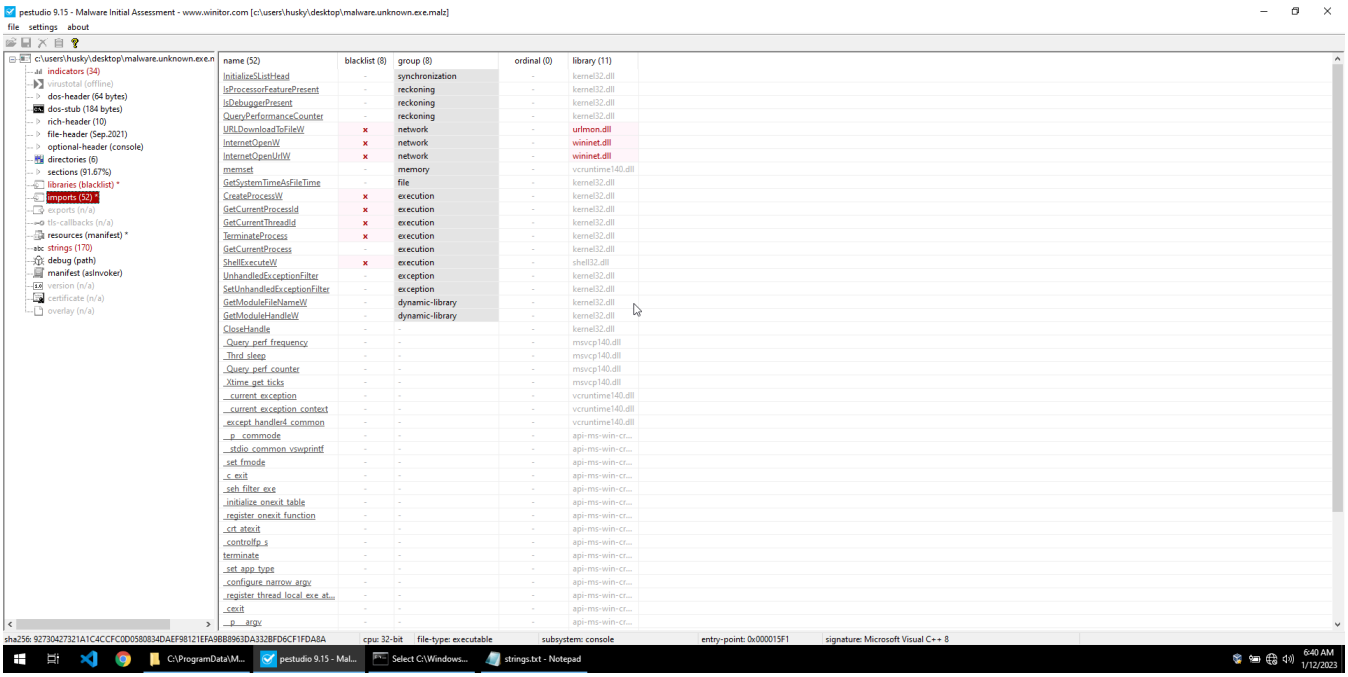


In the strings below , it can be seen that the malware checks internet connectivity and then downloads an executable file that is CR433101.dat.exe . This could be the malicious code executed from the trojan .

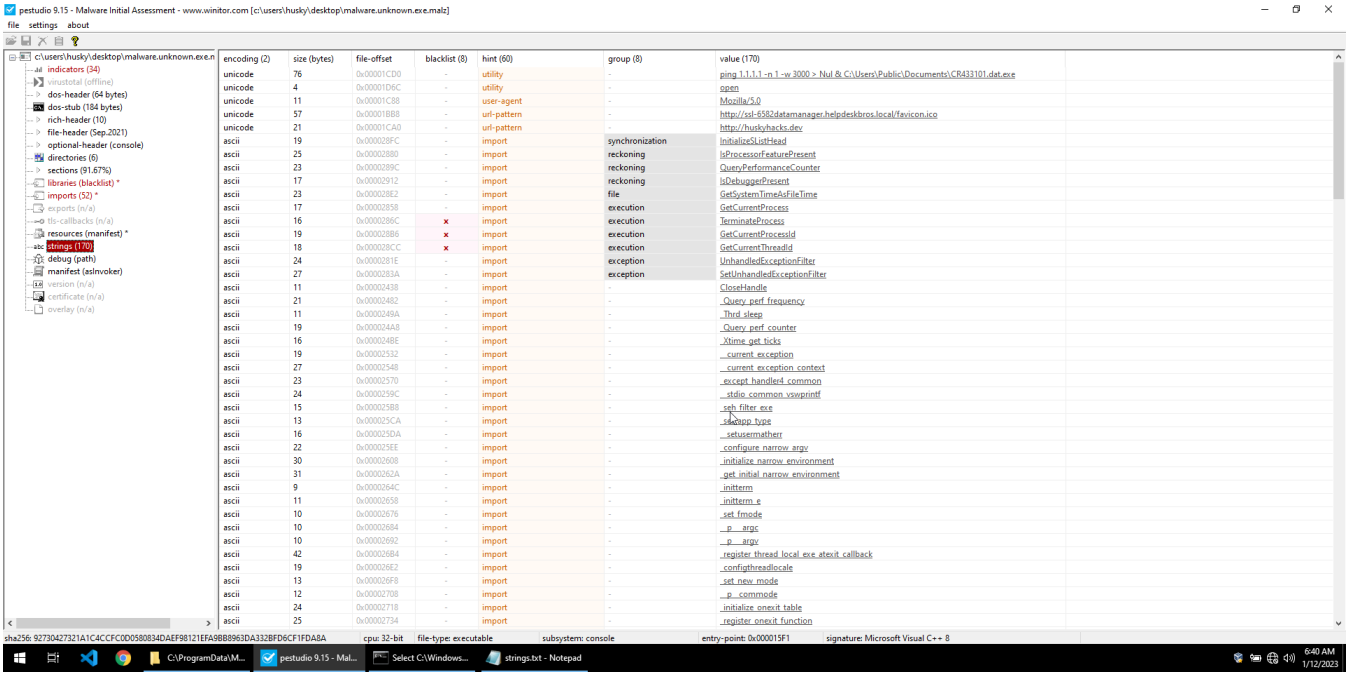
Libraries used by the malware:



Imports used by the malware :



Strings from the malware , as seen above , but in an ordered manner :



Details from virustotal :

Filetype : Win32 EXE

92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

Sign in | Sign up

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 16

Basic properties

MD5	1d8562c0adcaee734d63f7baaca02f7c
SHA-1	be138820e72435043b065fbf3a786be274b147ab
SHA-256	92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
Vhash	014056651d15555bzfhz11z13z23z45z
Authentihash	5f18327b29c76da006f05240022cbde921e78fa2472b537d903008caeef64365
Imphash	f2d1b81b70adf3f2dccc6d462ae64dc4
Rich PE header hash	fa59319837c5c2d12d4271dacda97ad2
SSDEEP	192:BR5KeZxKpjjHo3ugzjOkRKbyWkU7gwDR2FGV7E5pz67VSNI:BjqVH8uejrkbhkP5FGV78N
TLSH	T1DF428D03F6D00FB1DF240579303796A5C0BBB2516EE197236BD214850E762E2F43316E
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (generic) (9.9%) | Win16 NE executable (generic) (7.6%) | Win32 Executable (generic) (6.8%)
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (2017 v.15.5-6) [EXE32] | Compiler: Microsoft Visual C++ (2019 v.16.8 or 16.9) | Linker: Microsoft Linker (14.28, Visual Studio 2019 16.8 or 16.9*) [Console32,console]
File size	12.00 KB (12288 bytes)

History

Creation Time	2021-09-04 18:11:12 UTC
First Seen In The Wild	2021-09-04 11:11:12 UTC
First Submission	2021-10-08 06:53:51 UTC
Last Submission	2023-01-03 06:46:00 UTC
Last Analysis	2023-01-10 01:18:08 UTC

The virus is a trojan , it has been scanned by companies with great name in cybersecurity as BitDefender , and Fortinet for example .

92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a

Sign in | Sign up

92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
InitialDownload.exe

12.00 KB
Size

2023-01-10 01:18:08 UTC
2 days ago

EXE

peexe | runtime-modules | detect-debug-environment | checks-network-adapters | idle | long-sleeps | direct-cpu-clock-access | checks-user-input | spreader

Community Score

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 16

Security vendors' analysis

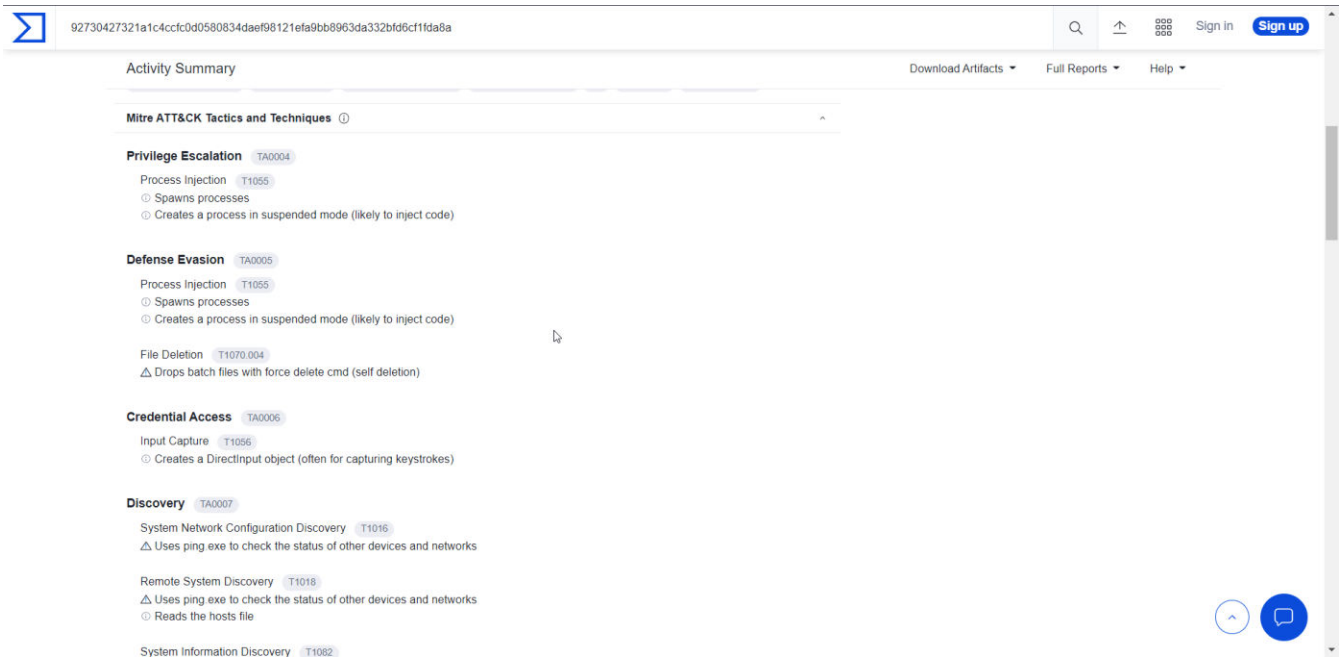
Ad-Aware	Gen:Variant.Bulz.801065	Alibaba	Trojan:Win32/SelfDel.8551fe3c
ALYac	Gen:Variant.Bulz.801065	Antiy-AVL	Trojan/Win32.SelfDel
Arcabit	Trojan.Bulz.DC3929	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/DelFiles.vdmja
BitDefender	Gen:Variant.Bulz.801065	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.0e7243	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/ABRisk.WXPJ-7017
DrWeb	Trojan.MulDrop19.15754	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Bulz.801065 (B)	eScan	Gen:Variant.Bulz.801065
ESET-NOD32	Win32/TrojanDownloader.Small.BKM	F-Secure	Trojan.TR/DelFiles.vdmja
Fortinet	W32/PossibleThreat	GData	Gen:Variant.Bulz.801065

The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target.

Below it can be seen some Mitre ATT&CK Tactics and Techniques :

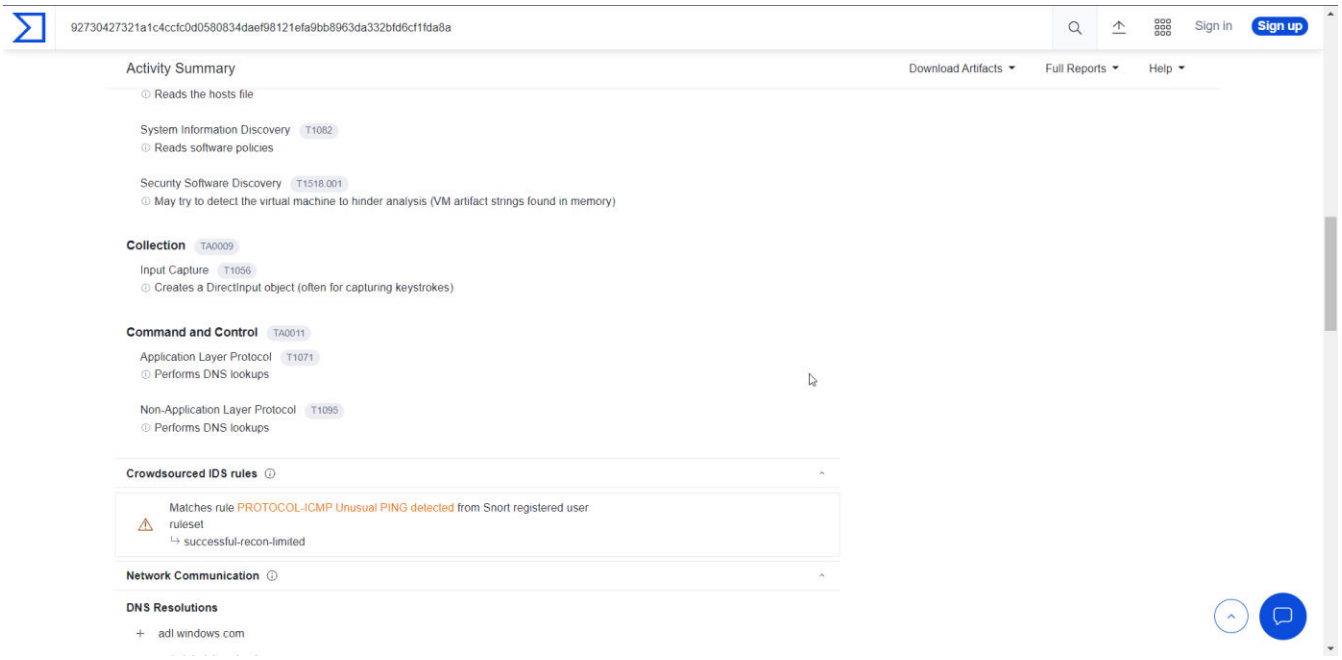
- Privilege Escalation trought process injection that spawns processes , creates a process in suspended mode that is likely to inject code .

- Defense Evasion trought process injection as well that is the same with above , privilege escalation .



It can be seen what DNS resolutions , the malware uses :

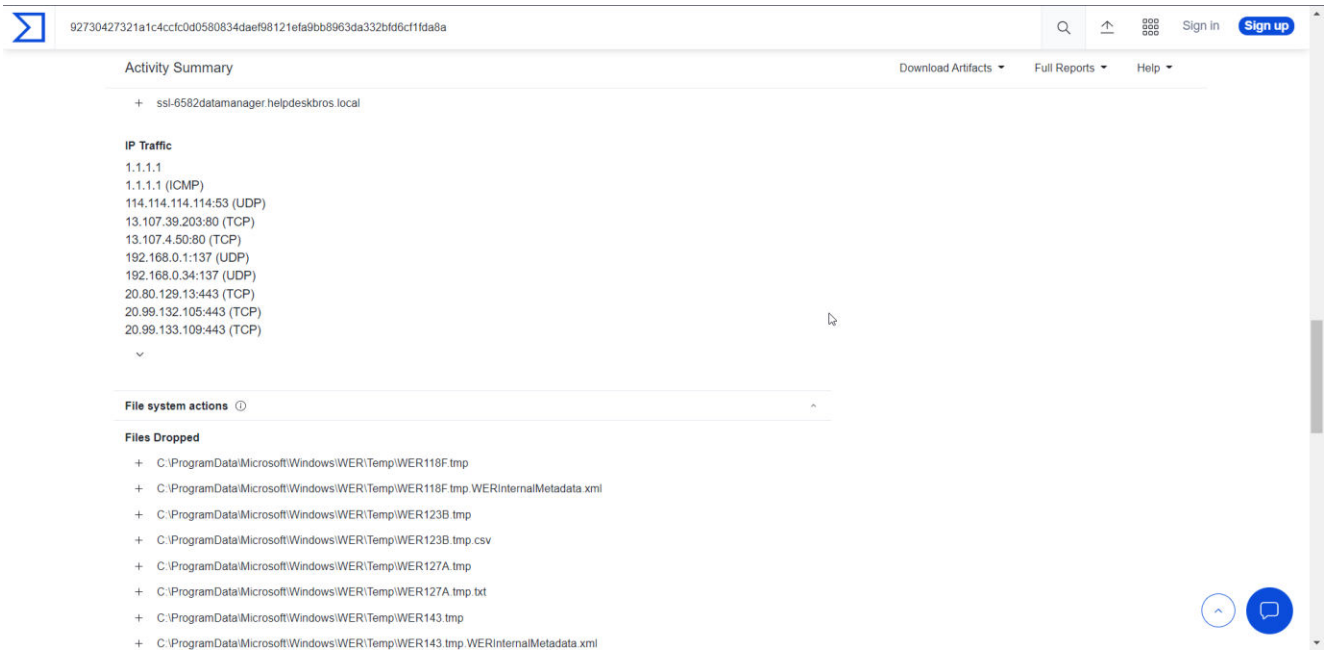
- Adl.windows.com



- Ssl-6582datamanager.helpdeskbros.local

And the IP Traffic :

- It pings 1.1.1.1
- And transfers data trough TCP and UDP at different IP addresses , for example 13.107.39.203 at the port 80 , and 114.114.114.114 at the port 53 .



File system actions

Files that are dropped on the computer :

File system actions

Files Dropped

- C:\ProgramData\Microsoft\Windows\WER\Temp\WER118F.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER118F.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER123B.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER123B.tmp.csv
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER127A.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER127A.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER143.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER143.tmp.WERInternalMetadata.xml
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER155.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER155.tmp.csv

Registry Keys configuration setting :

Registry Keys Set

- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix
- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix
- HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\DownloadManager
- HKLM/Software/Microsoft/Tracing/sample_RASAPI32/ConsoleTracingMask
- HKLM/Software/Microsoft/Tracing/sample_RASAPI32/EnableConsoleTracing
- HKLM/Software/Microsoft/Tracing/sample_RASAPI32/EnableFileTracing
- HKLM/Software/Microsoft/Tracing/sample_RASAPI32/FileDirectory
- HKLM/Software/Microsoft/Tracing/sample_RASAPI32/FileTracingMask
- HKLM/Software/Microsoft/Tracing/sample_RASAPI32/MaxFileSize

From the processes tree below :

- It spawns a command line shell [cmd.exe]
- Trough the shell , it pings 1.1.1.1 , it gets the output to null , so that it doesn t shows the output in the terminal and downloads an executable . The file name is a hash , malware on the internet is often described as a hash , without the .exe extension , then renamed with that extension and executed on the target computer .

Process and service actions

Processes Tree

↳ 1272 - C:\Windows\SysWOW64\cmd.exe

↳ 1956 - cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q C:\Users\<USER>\Downloads\92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a.exe

2440 - 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a.exe

2608 - %SAMPLEPATH%

2676 - %CONHOST% "-2105614999762916395970753 20-194356153149093151 7-1025176780133819798 6-1754718124

2724 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}

↳ 2752 - ping 1.1.1.1 -n 1 -w 3000

↳ 2776 - cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%SAMPLEPATH%"

2792 - %CONHOST% "-1128990772486315268-826692265167178913316035019151566929741102697678 5-1514249974

↳ 2808 - ping 1.1.1.1 -n 1 -w 3000

What malware does and with what works so that it gets to the wanted purpose. Examples:

- Checks network adapters
- Long sleeps
- Direct Cpu Clock Access
- Checks User Input

peexe runtime-modules detect-debug-environment checks-network-adapters idle long-sleeps direct-cpu-clock-access checks-user-input spreader