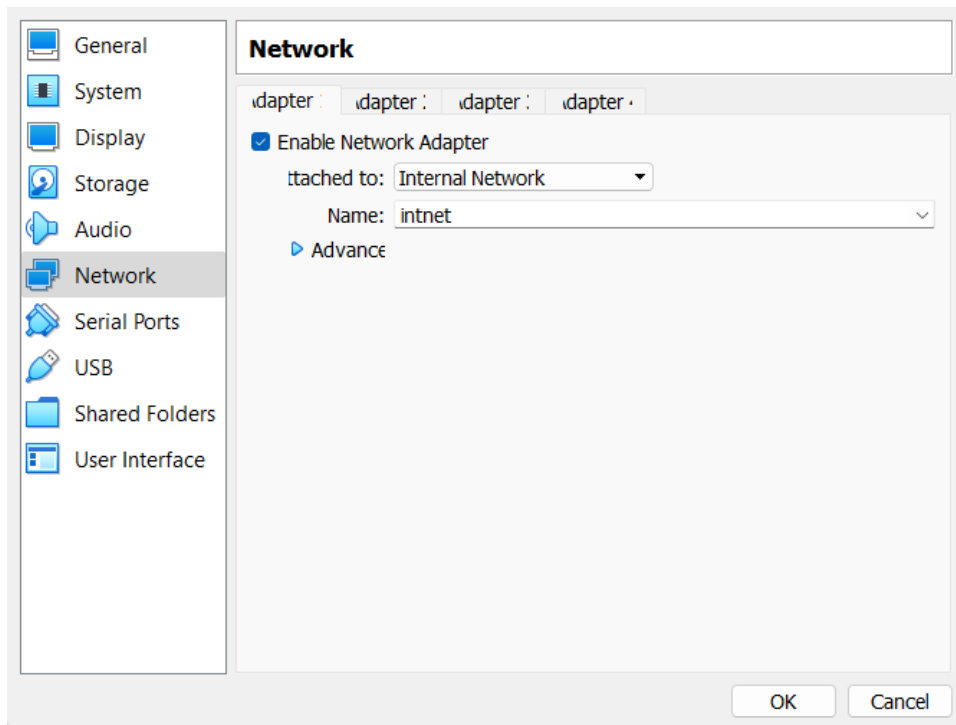


# Malware Analysis Laboratory

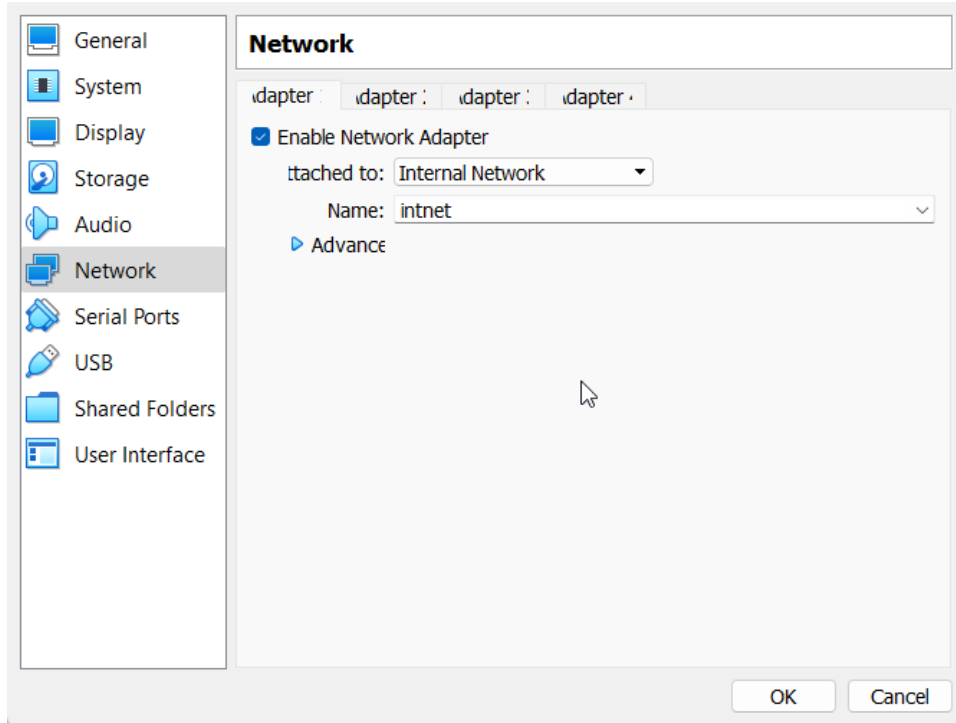
## Network setup :

Changing to internal network for both of the virtual machines .

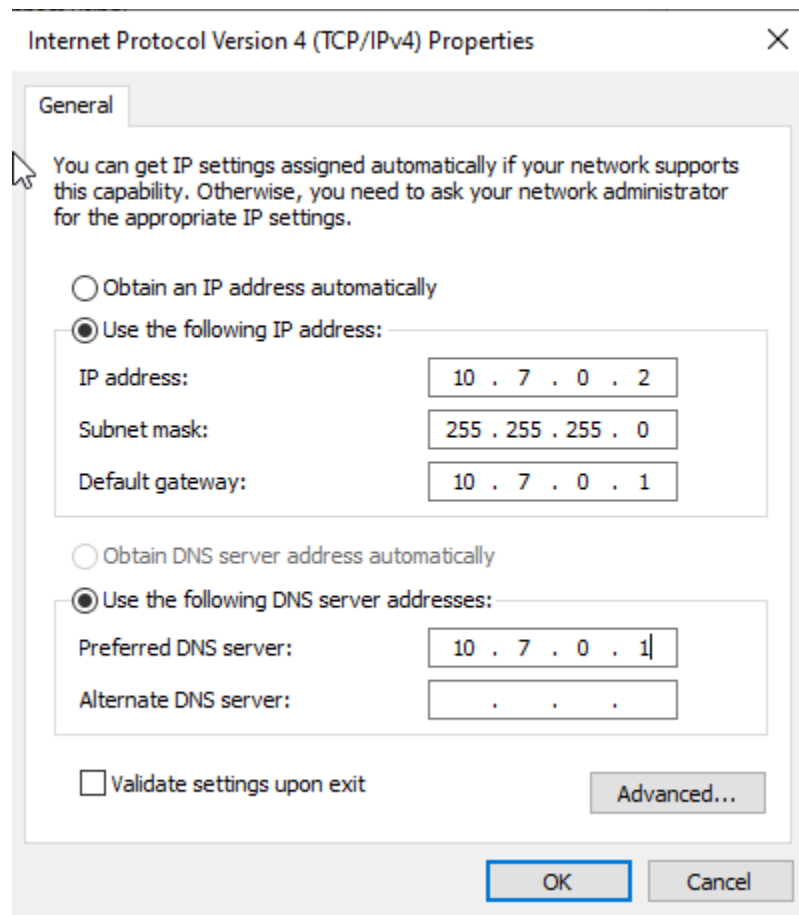
### FlareVM



# Remnux

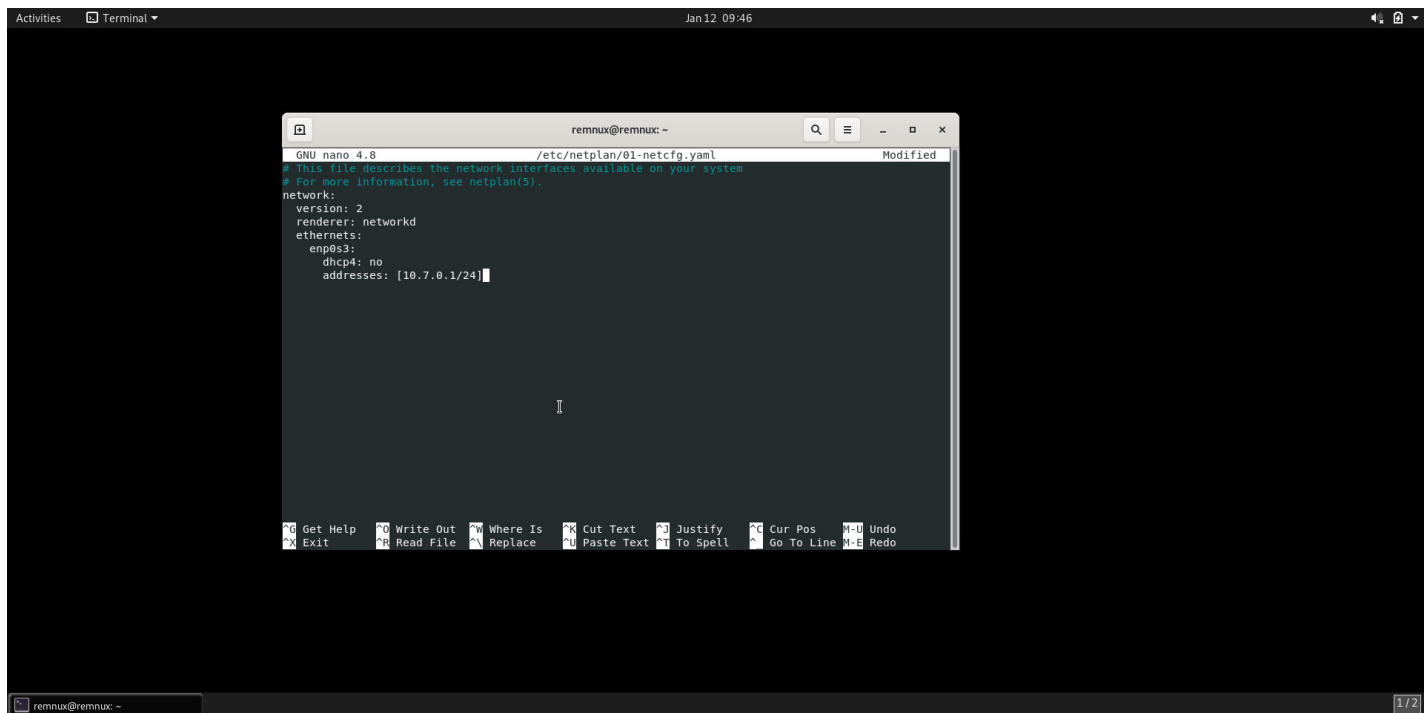


## Ipv4 address change on flare virtual machine:



# Inetsim configuration on remnux virtual machine :

Network adapter ip address changing in configuration file :



The screenshot shows a terminal window with a nano editor open, editing the file `/etc/netplan/01-netcfg.yaml`. The file content is as follows:

```
GNU nano 4.8 /etc/netplan/01-netcfg.yaml Modified
# This file describes the network interfaces available on your system
# For more information, see netplan(5).

network:
  version: 2
  renderer: networkd
  ethernet:
    enp0s3:
      dhcp4: no
      addresses: [10.7.0.1/24]
```

The cursor is positioned at the end of the `addresses: [10.7.0.1/24]` line. The terminal window title is `remnux@remnux: ~` and the date/time is `Jan12 09:46`. The bottom status bar shows the nano editor's command shortcuts and the file path `remnux@remnux: ~`.

```
Activities Terminal Jan 12 09:47

remnux@remnux:~$ nano
remnux@remnux:~$ sudo nano /etc/netplan/01-netcfg.yaml
remnux@remnux:~$ sudo cat /etc/netplan/01-netcfg.yaml
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.7.0.1/24]
remnux@remnux:~$
```

## Connectivity check through ping tool :

Remnux

```
Activities Terminal Jan 12 09:48

remnux@remnux:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.7.0.1 netmask 255.255.255.0 broadcast 10.7.0.255
    inet6 fe80::a00:27ff:fe4d:2a85 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:4d:2a:85 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 656 (656.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

remnux@remnux:~$ ping 10.7.0.2
PING 10.7.0.2 (10.7.0.2): 56(84) bytes of data:
64 bytes from 10.7.0.2: icmp_seq=1 ttl=128 time=1.38 ms
^C
--- 10.7.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.382/1.382/1.382/0.000 ms
remnux@remnux:~$
```

# FlareVM

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

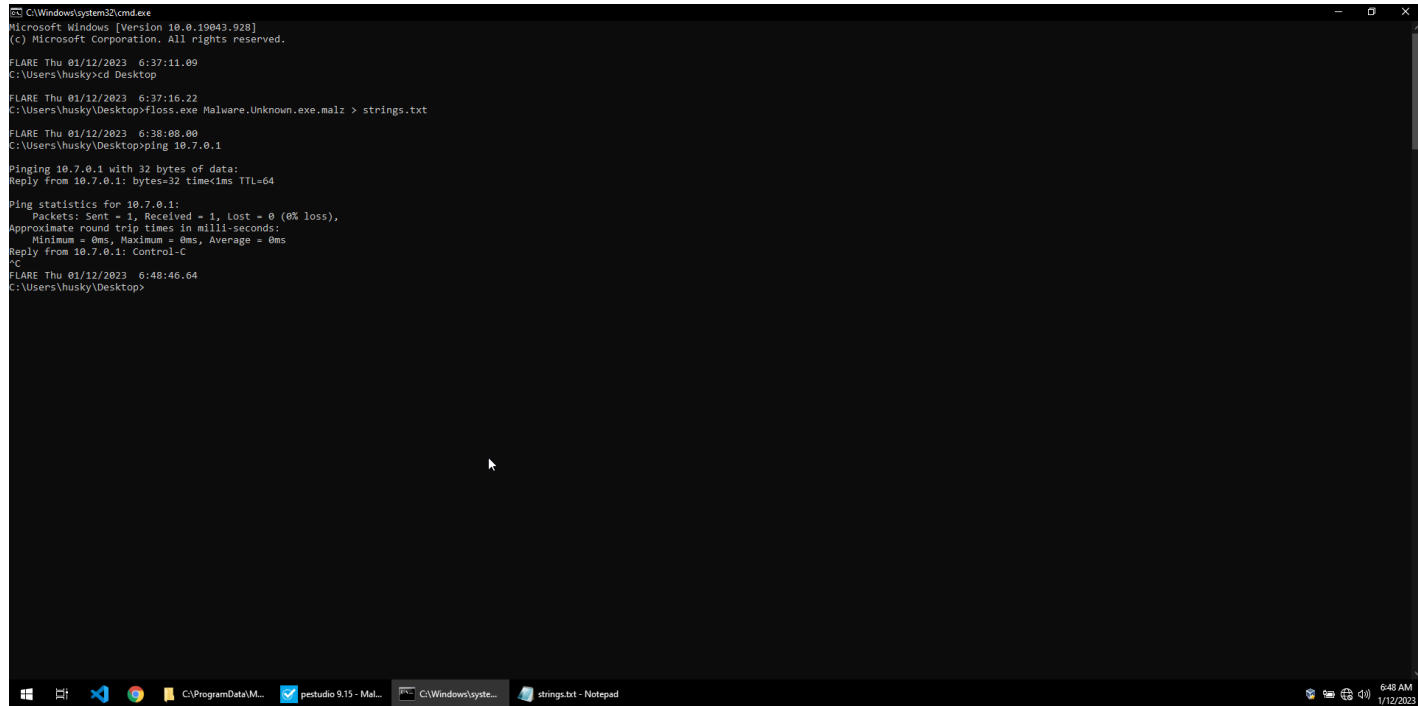
FLARE Thu 01/12/2023 6:37:11.09
C:\Users\husky>cd Desktop

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

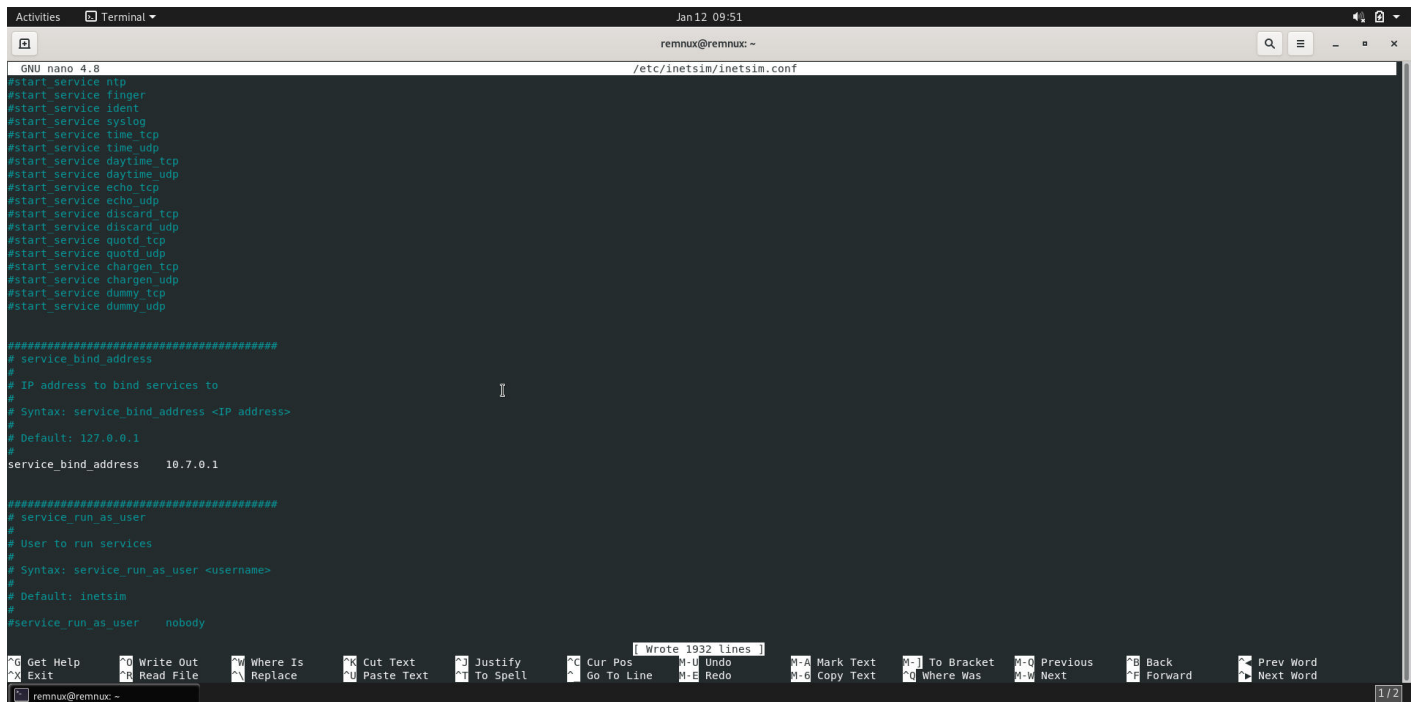
Pinging 10.7.0.1 with 32 bytes of data:
Reply from 10.7.0.1: bytes=32 time<1ms TTL=64

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>
```



# Inetsim configuration on remnux virtualmachine :

## Service\_bind\_address 10.7.0.1



```
GNU nano 4.8 /etc/inetsim/inetsim.conf
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#start_service echo_tcp
#start_service echo_udp
#start_service discard_tcp
#start_service discard_udp
#start_service quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 10.7.0.1

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
#
#service_run_as_user nobody
```

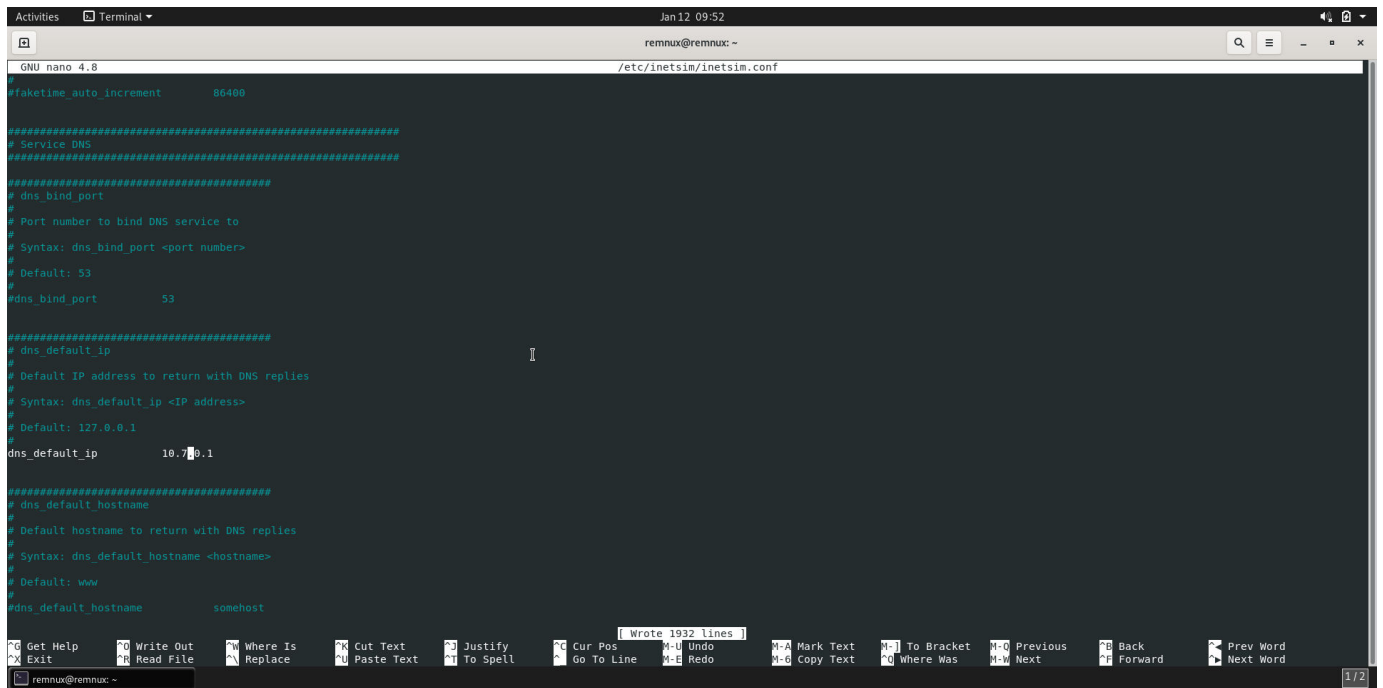
Wrote 1932 lines

Get Help Write Out Where Is Cut Text Justify Cur Pos Undo M-A Mark Text M-] To Bracket M-; Previous PG Back Prev Word  
Exit Read File Replace Paste Text To Spell Go To Line M-E Redo M-C Copy Text M-? Where Was M-W Next PG Forward Next Word

remnux@remnux:~

## Changing dns ip:

Dns\_default\_ip 10.7.0.1

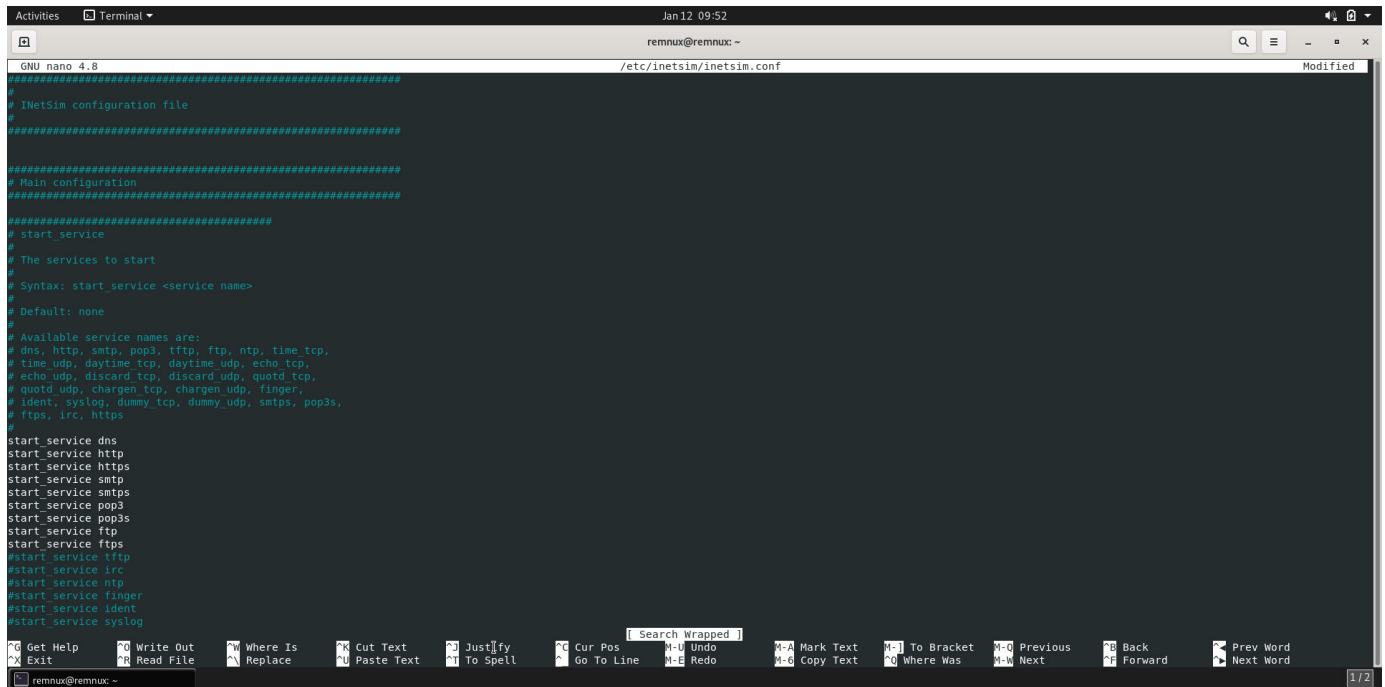


```
Activities Terminal Jan 12 09:52
remnux@remnux: ~
GNU nano 4.8 /etc/inetsim/inetsim.conf
#
#faketime_auto_increment      86400
#
#####
# Service DNS
#####
# dns_bind_port
#
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
#dns_bind_port      53
#
#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip      10.7.0.1
#
#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
#dns_default_hostname      somehost
#
I Wrote 1932 lines
Get Help Write Out Where Is Cut Text Justify Cur Pos M-U Undo M-A Mark Text M-I To Bracket M-O Previous M-B Back Prev Word
Exit Read File Replace Paste Text To Spell Go To Line M-E Redo M-C Copy Text M-W Where Was M-W Next M-F Forward Next Word
remnux@remnux: ~ 1/2
```



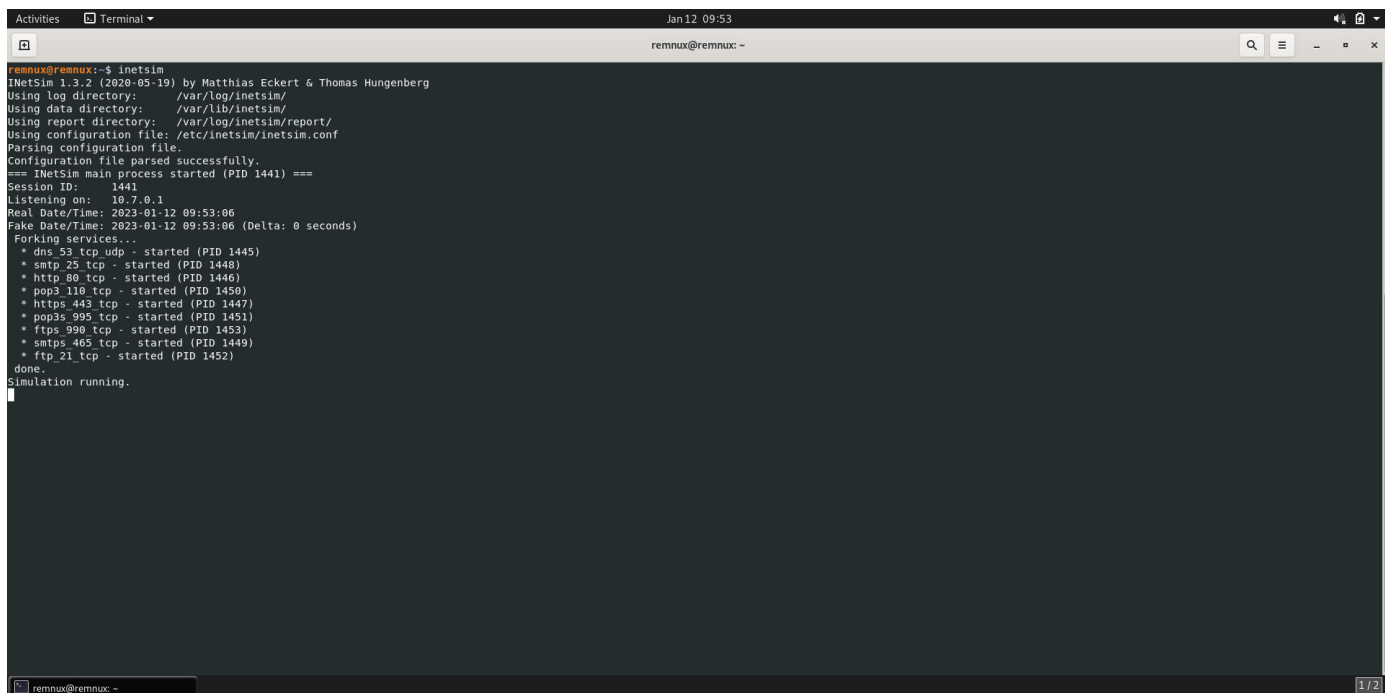
## Start the DNS service :

### Start\_service dns



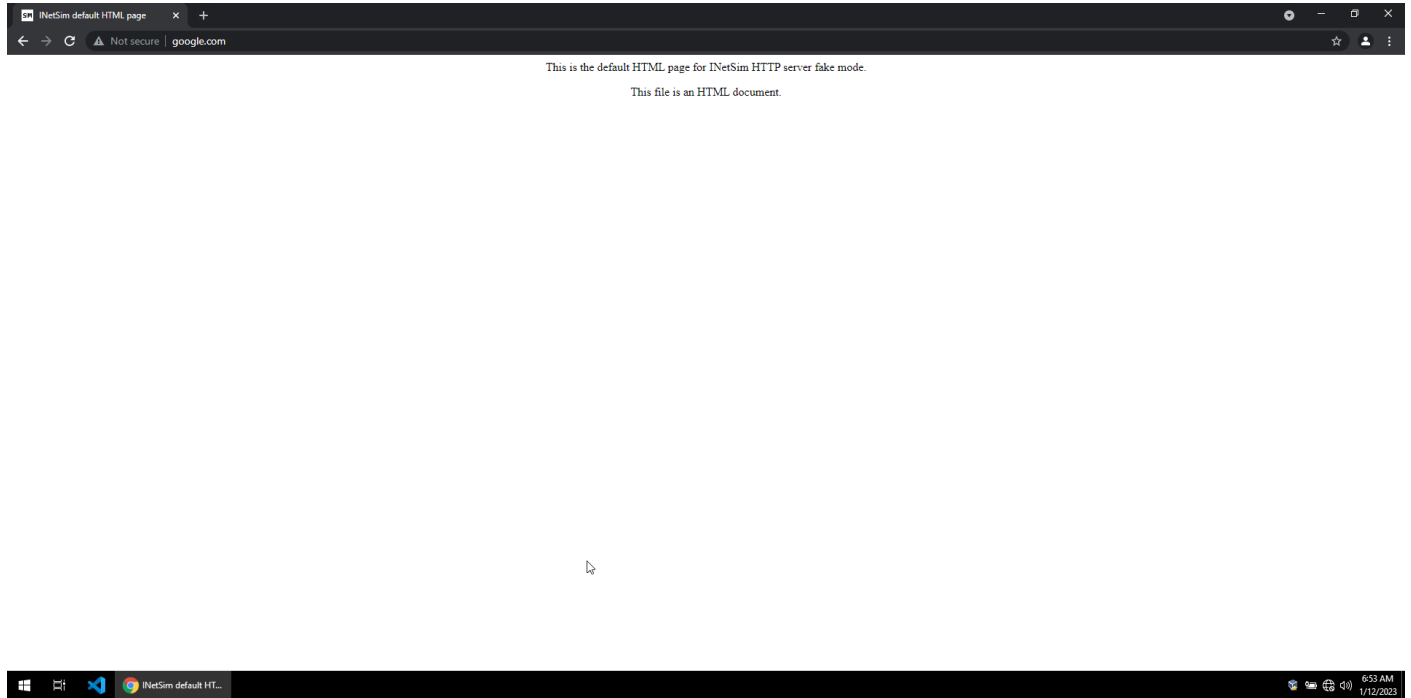
```
GNU nano 4.8 /etc/inetSim/inetSim.conf
#####
#
# InetSim configuration file
#
#####
# Main configuration
#####
#####
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time 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
```

## Start the FakeNet network simulation:



```
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.
```

On flareVM , accessing [www.google.com](http://www.google.com) , it is working :

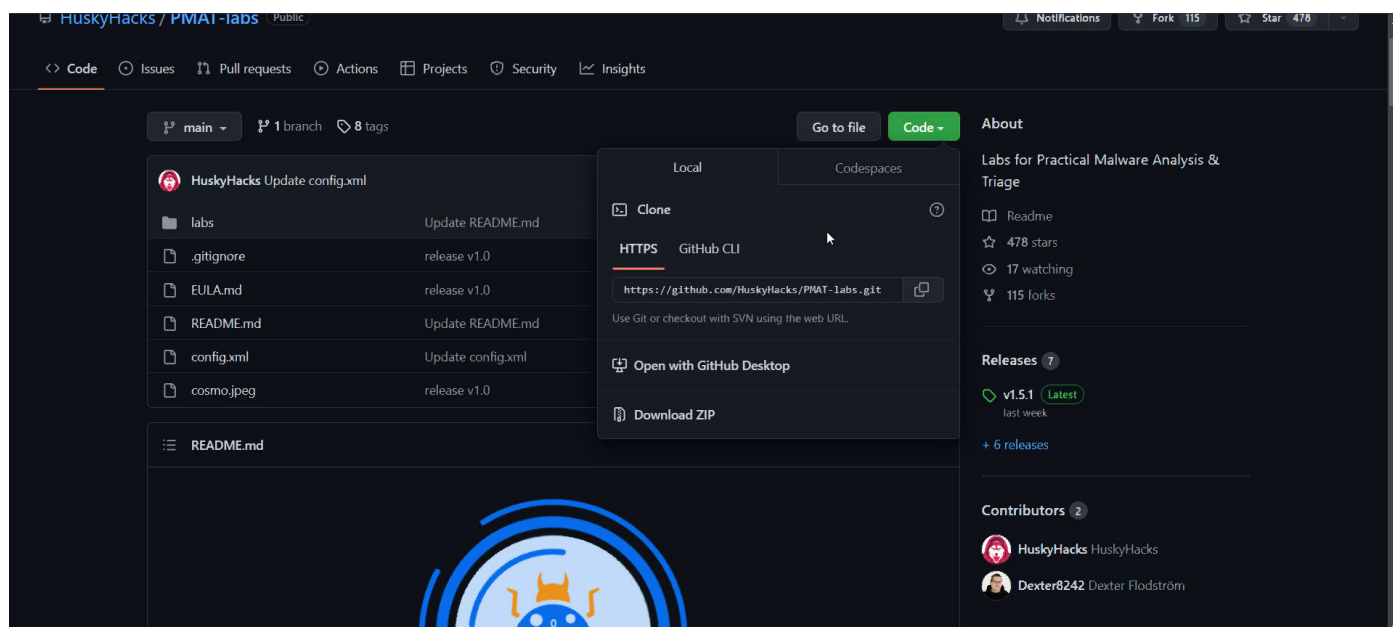


# Static Analysis

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:  
92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1  
FDA8A

## Prepare malware to be analyzed

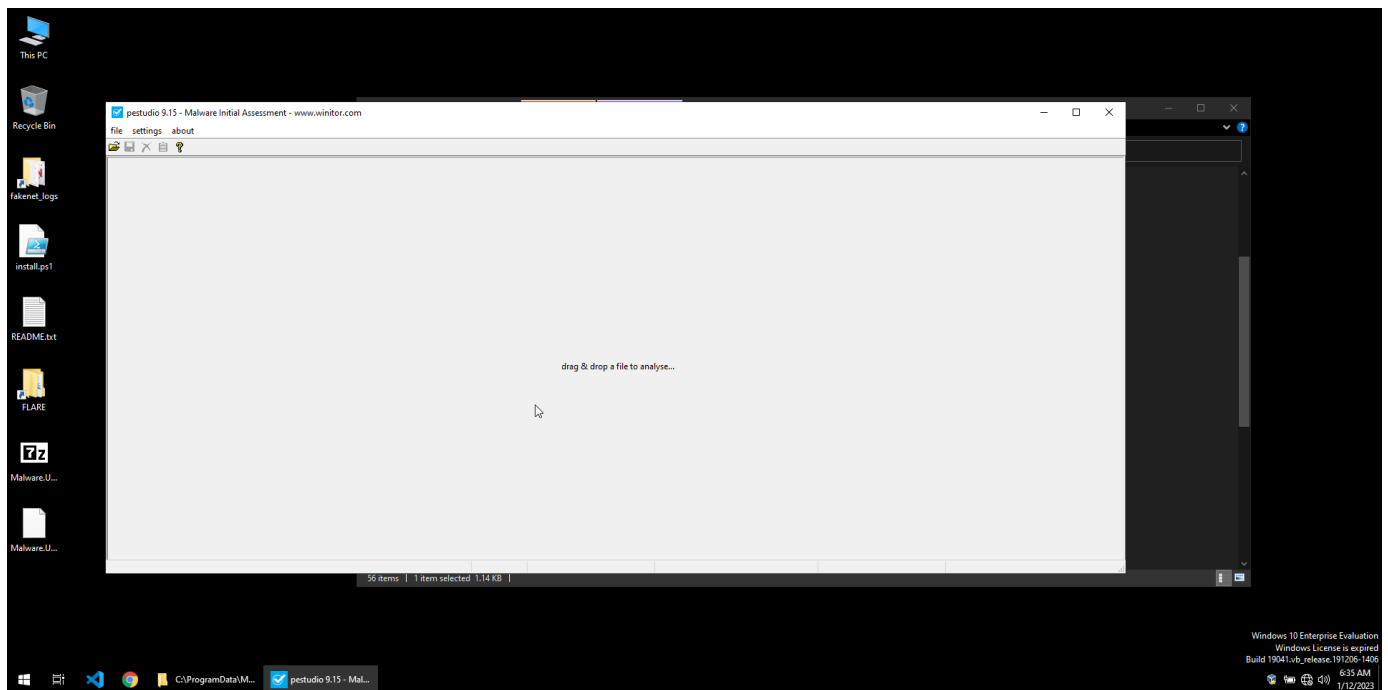


I dragged the malware , unarchive it and put it on desktop.

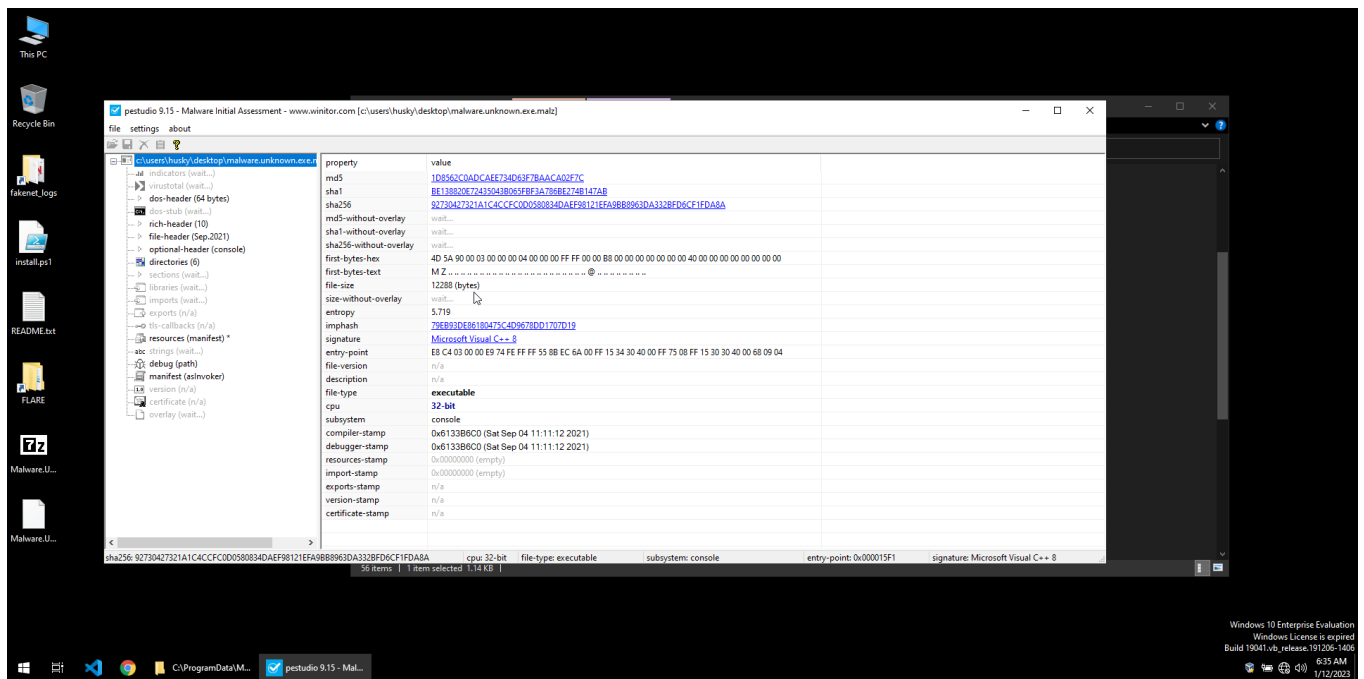


# Check with pestudio

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 .

92730427321a1c4ccfd050834dae98121efa9bb8963da332b6dcf1da8a

IntelDownload.exe

12.00 KB  
Size

2023-01-10 01:18:05 UTC  
2 days ago

49/76  
Community Score

49 security vendors and no sandboxes flagged this file as malicious

peexe runtime-modules debug-environment checks-network-adapters idr long-classes direct-cpu-disk-access checks-user-input spreader

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security vendors' analysis

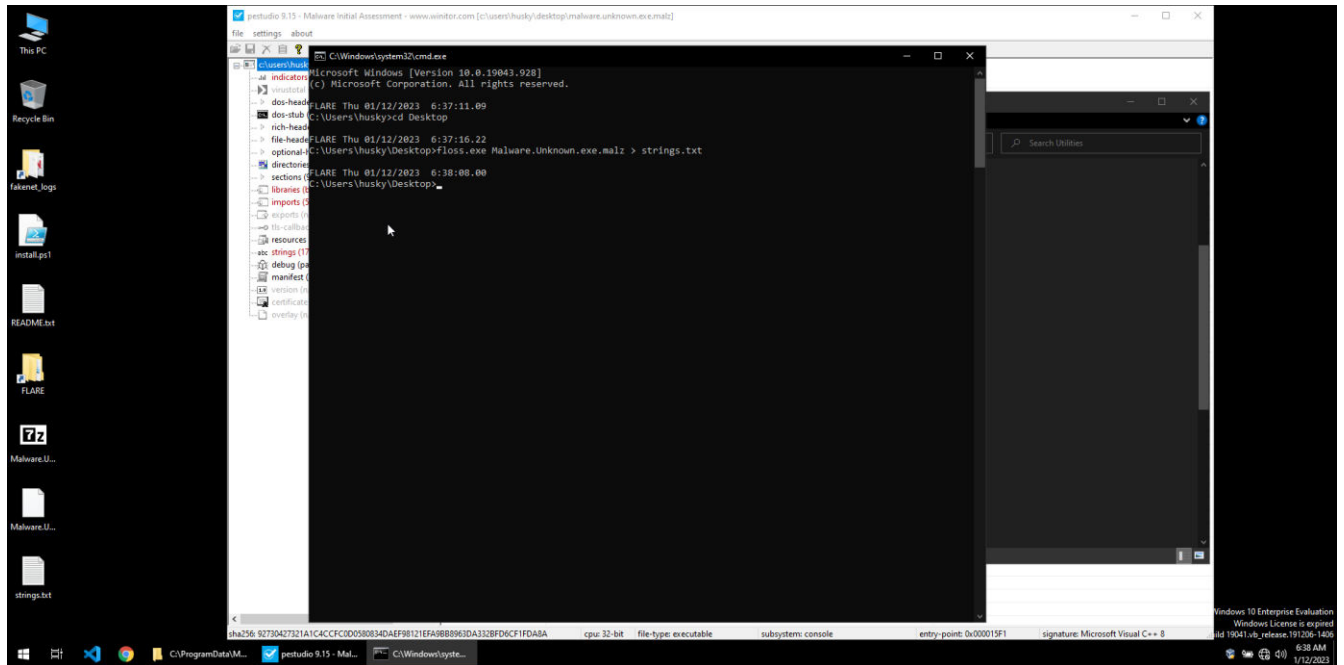
Ad-Aware	Gen Variant.Bulz.80.1065	Alibaba	Trojan.Win32.SelfDel.8551b3c
ALYac	Gen Variant.Bulz.80.1065	Anity-JVLT	Trojan.Win32.SelfDel
Avast	Trojan.Bulz.DC3929	Avast	Win32.Mahave-gen
AVG	Win32.Mahave-gen	Avira (no cloud)	TR.DelFiles.hdnja
BitDefender	Gen Variant.Bulz.80.1065	CrowdStrike Falcon	VirusShare_confidence_100% (vir)
Cybereason	Malicious.SelfDel	Cybereason	Unlabeled
Cynet	Malicious (score: 100)	Cyren	Win32.AdWare.VXPU.7917
Dr.Web	Trojan.MalDropt.15754	Elastic	Malicious (high confidence)
Emisoft	Gen Variant.Bulz.80.1065 (B)	eScan	Gen Variant.Bulz.80.1065
ESET-NOD32	Win32.TrojanDownloader.Small.BK04	F-Secure	Trojan.TR.DelFiles.vomps
Fortinet	Win32.FireEyeThreat	GDData	Gen Variant.Bulz.80.1065
Google	Detected	GridinSoft (no cloud)	Ransom.Win32.Sabalk.virus1
Ikarus	Trojan-Downloader.Win32.Small	Jiangmin	Trojan.Jinbuluo.1
Kaspersky	HEUR:Trojan.Win32.SelfDel.gen	Kingsoft	Win32.Trojan.Lindef (actual)
Lionic	Trojan.Win32.SelfDel.dlc	Malwarebytes	Trojan.SelfDelete
MAX	Malware (all Score=6)	MaxSecure	Trojan.Malware.300983.suigen
McAfee	RDH/Ransom	McAfee-GW-Edison	BehavesLike.Win32.Genetic.im

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

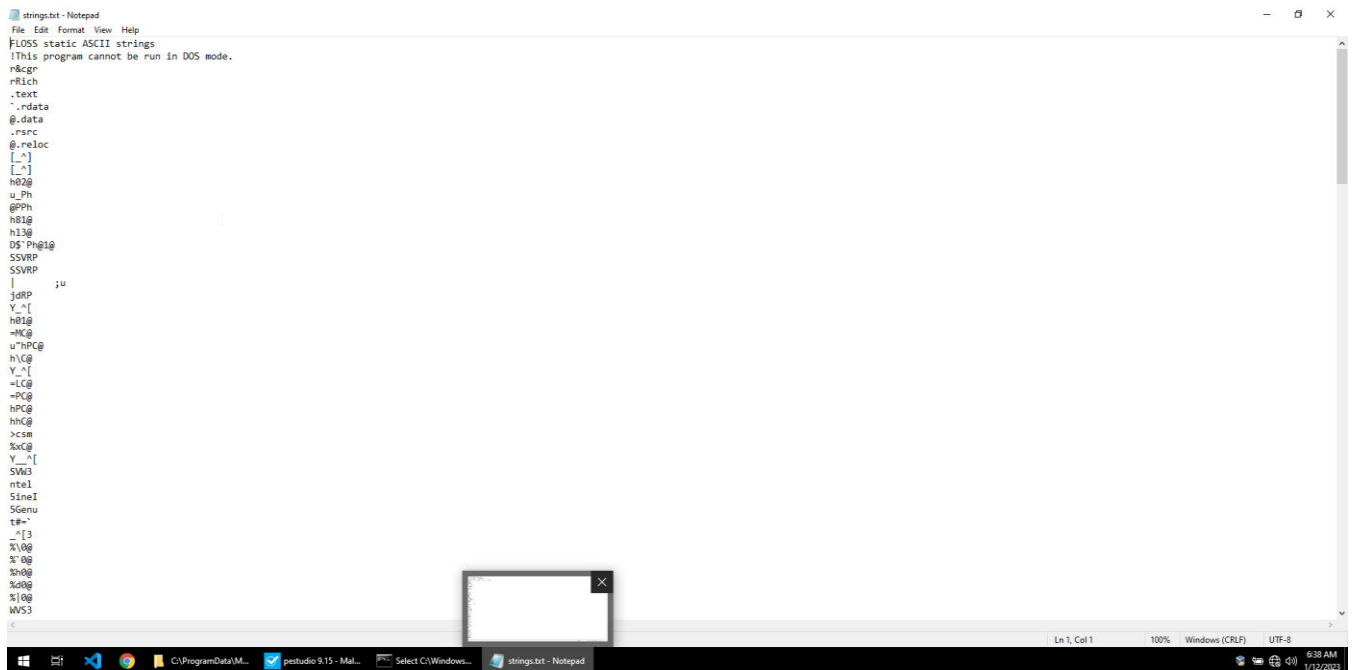
A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

## Extract Strings

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

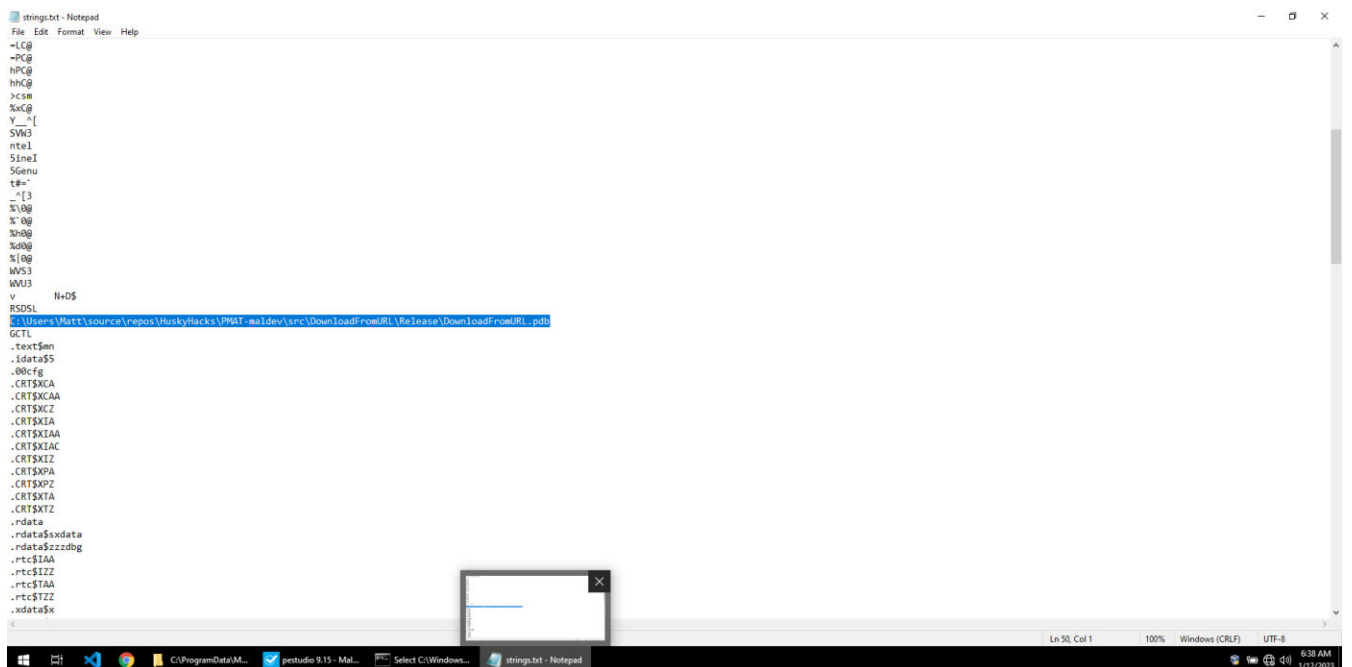


The text file owned after the command execution :



```
strings.txt - Notepad
File Edit Format View Help
FLOSS static ASCII strings
!This program cannot be run in DOS mode.
r&ngp
rRich
.text
.rdata
@.data
.rsrc
@.reloc
[.~]
h03@
u.Ph
@PPh
h81@
h13@
DS`Ph@1@
SSVRP
SSVRP
;u
jdrp
Y.^[
h81@
~M@
u`hPC@
h1C@
Y.^[
~LC@
~PC@
hPC@
h1C@
>csm
%xC@
Y.^[
SW3
nte1
Sine1
SGenu
t#="
_[3
%`0@
%`0@
%h0@
%h0@
%h0@
WS3
WS3
Ln 1, Col 1 100% Windows (CRLF) UTF-8 6:38 AM 1/12/2023
```

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



```
strings.txt - Notepad
File Edit Format View Help
~LC@
~PC@
hPC@
h1C@
>csm
%xC@
Y.^[
SW3
nte1
Sine1
SGenu
t#="
_[3
%`0@
%`0@
%h0@
%h0@
%h0@
WS3
WS3
v N+D$
RSDSL
C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFromURL.pdb
GCL
.text$en
.idata$5
00crg
.CRT$XCA
.CRT$XCAA
.CRT$XCZ
.CRT$XIA
.CRT$XIAA
.CRT$XIAC
.CRT$XIZ
.CRT$XPA
.CRT$XPZ
.CRT$XTA
.CRT$XTZ
.rdata
.rdata$xxdata
.rdata$zzzdbg
.rtc$IAA
.rtc$IZZ
.rtc$TAA
.rtc$TZZ
.xdata$X
Ln 50, Col 1 100% Windows (CRLF) UTF-8 6:38 AM 1/12/2023
```

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 .





# Imports used by the malware :

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\husky\desktop\malware.unknown.exe.malz]

file settings about

	name (52)	blacklist (8)	group (8)	ordinal (8)	library (11)
indicators (34)	IsInitialSetup	-	synchronization	-	kernel32.dll
↳ virustotal (offline)	IsProcessorFeaturePresent	-	reckoning	-	kernel32.dll
↳ dos-header (64 bytes)	IsDebuggerPresent	-	reckoning	-	kernel32.dll
↳ dos-stub (184 bytes)	QueryPerformanceCounter	-	reckoning	-	kernel32.dll
↳ rich-header (10)	URLDownloadToFileW	x	network	-	urlmon.dll
↳ file-header (Sep-2021)	InternetOpenW	x	network	-	wininet.dll
↳ optional-header (console)	InternetOpenUrlW	x	network	-	wininet.dll
↳ directories (8)	memmove	-	memory	-	vcruntime140.dll
↳ sections (91.67%)	GetSystemTimeAsFileTime	-	file	-	kernel32.dll
↳ libraries (blacklist) *	CreateProcessW	x	execution	-	kernel32.dll
↳ imports (52) *	GetCurrentProcessId	x	execution	-	kernel32.dll
↳ exports (n/a)	GetCurrentThreadId	x	execution	-	kernel32.dll
↳ io-callbacks (n/a)	TerminateProcess	x	execution	-	kernel32.dll
↳ resources (manifest) *	GetCurrentProcess	-	execution	-	kernel32.dll
↳ strings (170)	ShellExecuteW	x	execution	-	shell32.dll
↳ debug (path)	UnhandledExceptionFilter	-	exception	-	kernel32.dll
↳ manifest (asInvoker)	SetUnhandledExceptionFilter	-	exception	-	kernel32.dll
↳ certificate (n/a)	GetModuleFileNameW	-	dynamic-library	-	kernel32.dll
↳ overlay (n/a)	GetModuleHandleW	-	dynamic-library	-	kernel32.dll
	CloseHandle	-	-	-	kernel32.dll
	Query_perf_frequency	-	-	-	msvcp140.dll
	_Thrd_sleep	-	-	-	msvcp140.dll
	Query_perf_counter	-	-	-	msvcp140.dll
	_Xtreme_get_ticks	-	-	-	msvcp140.dll
	_current_exception	-	-	-	vcruntime140.dll
	_current_exception_context	-	-	-	vcruntime140.dll
	_except_handler4_common	-	-	-	vcruntime140.dll
	_p_commode	-	-	-	api-ms-win-cr...
	_stdio_common_vfprintf	-	-	-	api-ms-win-cr...
	_set_mode	-	-	-	api-ms-win-cr...
	_set_app_type	-	-	-	api-ms-win-cr...
	_set_app_type	-	-	-	api-ms-win-cr...
	_initialize_onexit_table	-	-	-	api-ms-win-cr...
	_register_onexit_function	-	-	-	api-ms-win-cr...
	_crt_atexit	-	-	-	api-ms-win-cr...
	_controlfp_s	-	-	-	api-ms-win-cr...
	_terminate	-	-	-	api-ms-win-cr...
	_set_app_type	-	-	-	api-ms-win-cr...
	_configure_narrow_argv	-	-	-	api-ms-win-cr...
	_register_thread_local_exe_at...	-	-	-	api-ms-win-cr...
	_cexit	-	-	-	api-ms-win-cr...
	_p_argv	-	-	-	api-ms-win-cr...

sha256: 92730427321A1C4CCFC0D058034DAEF8121FA8B88963DA332BFD6CF1FDABA cpu: 32-bit file-type: executable subsystem: console entry-point: 0x000015F1 signature: Microsoft Visual C++ 8

Windows taskbar: C:\ProgramData\... pestudio 9.15 - Mal... Select C:\Windows... strings.txt - Notepad

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

pestudio 9.15 - Malware Initial Assessment - www.winitor.com [c:\users\husky\desktop\malware.unknown.exe.malz]

file settings about

	encoding (2)	size (bytes)	file-offset	blacklist (8)	hint (50)	group (8)	value (170)
indicators (34)	unicode	76	0x0001CDD0	-	utility	-	ping 1.1.1.1 -n 1 -w 3000 > nul & C:\Users\Public\Documents\CB433101.dat.exe
↳ virustotal (offline)	unicode	4	0x0001D06C	-	utility	-	open
↳ dos-header (64 bytes)	unicode	11	0x0001C388	-	user-agent	-	Mozilla/5.0
↳ dos-stub (184 bytes)	unicode	57	0x0001D088	-	url-pattern	-	http://ad-5502admanager.helpdesklocal.favicon.ico
↳ rich-header (10)	unicode	21	0x0001CA40	-	url-pattern	-	http://huskybacks.de/
↳ file-header (Sep-2021)	ascii	19	0x000028FC	-	import	synchronization	IsInitialSetup
↳ optional-header (console)	ascii	25	0x00002880	-	import	reckoning	IsProcessorFeaturePresent
↳ directories (8)	ascii	23	0x0000289C	-	import	reckoning	QueryPerformanceCounter
↳ libraries (blacklist) *	ascii	17	0x00002912	-	import	reckoning	IsDebuggerPresent
↳ imports (52) *	ascii	23	0x000028E2	-	import	file	GetSystemTimeAsFileTime
↳ exports (n/a)	ascii	17	0x00002858	-	import	execution	GetCurrentProcess
↳ io-callbacks (n/a)	ascii	16	0x0000286C	x	import	execution	TerminateProcess
↳ resources (manifest) *	ascii	19	0x00002886	x	import	execution	GetCurrentProcessId
↳ strings (170)	ascii	18	0x000028CC	x	import	execution	GetCurrentThreadId
↳ debug (path)	ascii	24	0x0000281E	-	import	exception	UnhandledExceptionFilter
↳ manifest (asInvoker)	ascii	27	0x0000283A	-	import	exception	SetUnhandledExceptionFilter
↳ certificate (n/a)	ascii	11	0x00002438	-	import	exception	CloseHandle
↳ overlay (n/a)	ascii	21	0x00002482	-	import	-	Query_perf_frequency
	ascii	11	0x0000249A	-	import	-	_Thrd_sleep
	ascii	19	0x000024A8	-	import	-	Query_perf_counter
	ascii	16	0x0000248E	-	import	-	_Xtreme_get_ticks
	ascii	19	0x00002432	-	import	-	_current_exception
	ascii	27	0x00002448	-	import	-	_current_exception_context
	ascii	23	0x00002470	-	import	-	_except_handler4_common
	ascii	24	0x0000259C	-	import	-	_stdio_common_vfprintf
	ascii	15	0x0000258B	-	import	-	_set_mode
	ascii	13	0x000025CA	-	import	-	_set_app_type
	ascii	16	0x000025DA	-	import	-	_set_app_type
	ascii	22	0x000025EE	-	import	-	_initialize_onexit_table
	ascii	30	0x00002608	-	import	-	_register_onexit_function
	ascii	31	0x0000262A	-	import	-	_get_initial_narrow_environment
	ascii	9	0x0000264C	-	import	-	_initterm
	ascii	11	0x00002658	-	import	-	_initterm_s
	ascii	10	0x00002676	-	import	-	_set_mode
	ascii	10	0x00002684	-	import	-	_p_argv
	ascii	10	0x00002692	-	import	-	_p_argv
	ascii	42	0x00002684	-	import	-	_register_thread_local_exe_atexit_callback
	ascii	19	0x000026E2	-	import	-	_configthreadlocale
	ascii	13	0x000026F8	-	import	-	_set_new_mode
	ascii	12	0x00002708	-	import	-	_p_commode
	ascii	24	0x00002718	-	import	-	_initialize_onexit_table
	ascii	25	0x00002734	-	import	-	_register_onexit_function

sha256: 92730427321A1C4CCFC0D058034DAEF8121FA8B88963DA332BFD6CF1FDABA cpu: 32-bit file-type: executable subsystem: console entry-point: 0x000015F1 signature: Microsoft Visual C++ 8

Windows taskbar: C:\ProgramData\... pestudio 9.15 - Mal... Select C:\Windows... strings.txt - Notepad

# Details from virustotal :

Filetype : Win32 EXE

92730427321a1c4ccfc0d0580834dae98121efa9bb8963da332bf06cf1fda8a

Sign inSign up

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY16

Basic properties ⓘ

MD51d8562c0adcae734d63f7baaca027c

SHA-1be138820e72435043b065fb3a786be274b147ab

SHA-25692730427321a1c4ccfc0d0580834dae98121efa9bb8963da332bf06cf1fda8a

Vhash014056651d15555bzb7h11z13z23z45z

Authenthash5f18327b29c76da06f05240022cbde921e78fa2472b537d903008caeefb4365

Imphashf2d1b81b70ad3f2dccc6d462ae64dc4

Rich PE header hashfa59319837c5c2d12d4271dacda97ad2

SSDEEPT192 BR5KeZxKpjiHo3ugzjOkRKbyWkU7gwDR2FGV7E5pz67VSNi BjqVH8uejrbkhkP5FGV78N

TLSH11DF428D03F8D00FB1DF240579303796A5C0B6B2516EE197236BD214850E762E2F43316E

File typeWin32 EXE

MagicPE32 executable for MS Windows (console) Intel 80386 32-bit

TrIDWin32 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%)

DetectItEasyPE32Compiler: 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 size12.00 KB (12288 bytes)

History ⓘ

Creation Time2021-09-04 18:11:12 UTC

First Seen In The Wild2021-09-04 11:11:12 UTC

First Submission2021-10-08 06:53:51 UTC

Last Submission2023-01-03 06:46:00 UTC

Last Analysis2023-01-10 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 .

92730427321a1c4ccfc0d0580834dae98121efa9bb8963da332bf06cf1fda8a

Sign inSign up

InitialDownload.exe12.00 KBSize2023-01-10 01:18:08 UTC2 days agoEXE

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

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY16

Security vendors' analysis ⓘ

Ad-Aware ⓘ Gen.Variant.Bulz.801065Alibaba ⓘ Trojan.Win32/SelfDel.8551fe3c

ALYac ⓘ Gen.Variant.Bulz.801065Antiy-AVL ⓘ Trojan/Win32.SelfDel

Arcabit ⓘ Trojan.Bulz.DC3929Avast ⓘ Win32/Malware-gen

AVG ⓘ Win32/Malware-genAvira (no cloud) ⓘ TR/DelFiles.vdmja

BitDefender ⓘ Gen.Variant.Bulz.801065CrowdStrike Falcon ⓘ Win/malicious\_confidence\_100% (W)

Cybereason ⓘ Malicious.0e7243Cylance ⓘ Unsafe

Cynet ⓘ Malicious (score: 100)Cyren ⓘ W32/ABRisk.WXPJ-7017

DrWeb ⓘ Trojan.MulDrop19.15754Elastic ⓘ Malicious (high Confidence)

Emsisoft ⓘ Gen.Variant.Bulz.801065 (B)eScan ⓘ Gen.Variant.Bulz.801065

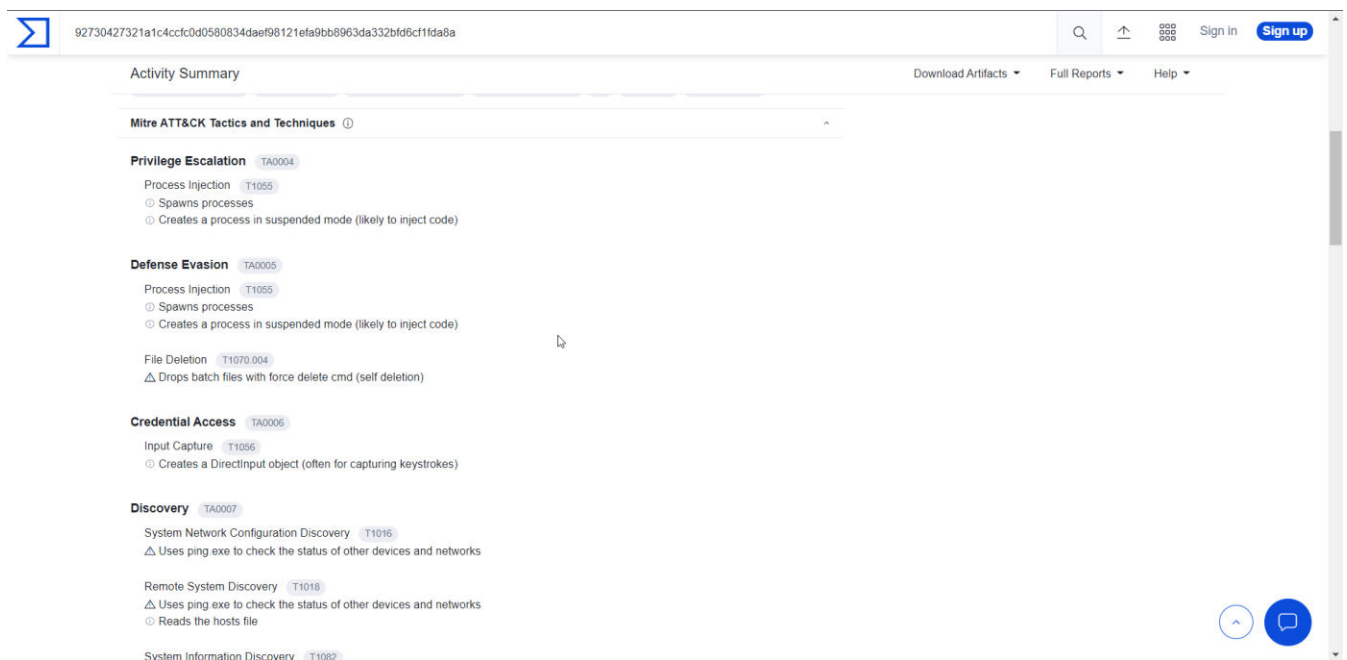
ESET-NOD32 ⓘ Win32/TrojanDownloader.Small.BKMFSecure ⓘ Trojan.TR/DelFiles.vdmja

Fortinet ⓘ W32/PossibleThreatGData ⓘ 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 through process injection that spawns processes , creates a process in suspended mode that is likely to inject code .
- Defense Evasion through 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

The screenshot shows a network analysis tool interface with a top navigation bar containing a search icon, an upload icon, a document icon, and links for 'Sign in' and 'Sign up'. The main content area is titled 'Activity Summary' and lists several categories of activity:

- Activity Summary**
  - Reads the hosts file
  - System Information Discovery (T1062)
    - Reads software policies
  - Security Software Discovery (T1518.001)
    - May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)
- Collection** (TA0009)
  - Input Capture (T1056)
    - Creates a DirectInput object (often for capturing keystrokes)
- Command and Control** (TA0011)
  - Application Layer Protocol (T1071)
    - Performs DNS lookups
  - Non-Application Layer Protocol (T1095)
    - Performs DNS lookups
- Crowdsourced IDS rules**
  - Matches rule **PROTOCOL-ICMP Unusual PING detected** from Snort registered user ruleset
    - successful-recon-limited
- Network Communication**
  - DNS Resolutions
    - + adl.windows.com

On the right side of the interface, there are icons for 'Download Artifacts', 'Full Reports', and 'Help'.

- Ssl-6582datamanager.helpdeskbro.local

And the IP Traffic :

- It pings 1.1.1.1
- And transfers data through 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

The screenshot shows the same network analysis tool interface, but with a different host selected: 'ssl-6582datamanager.helpdeskbro.local'. The 'Activity Summary' section is expanded, showing the following details:

- IP Traffic**
  - 1.1.1.1
  - 1.1.1.1 (ICMP)
  - 114.114.114.114:53 (UDP)
  - 13.107.39.203:80 (TCP)
  - 13.107.4.50:80 (TCP)
  - 192.168.0.1:137 (UDP)
  - 192.168.0.34:137 (UDP)
  - 20.80.129.13:443 (TCP)
  - 20.99.132.105:443 (TCP)
  - 20.99.133.109:443 (TCP)
- 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

The right side of the interface remains the same, with 'Download Artifacts', 'Full Reports', and 'Help' options.

## 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 .

## 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% "-210561499976291639597075320-1943561531490931517-10251767801338197986-1754718124
2724 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBC66683}
↳ 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% "-1128990772486315268-8266922651671789133160350191515669297411026976785-1514249974
↳ 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