ID: 491790
Sample Name: 78mne21kC0
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 22:40:19
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

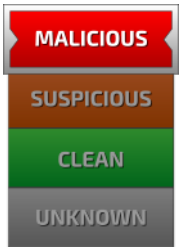
Linux Analysis Report 78mne21kC0

Overview

General Information

Sample Name:	78mne21kC0
Analysis ID:	491790
MD5:	12cf087e49d1f9a..
SHA1:	464abb479aa8d9..
SHA256:	9b4db7f46e24f6f…
Tags:	32 elf mirai motorola
Infos:	

Detection

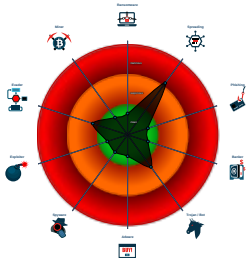


Score:	52
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Opens /proc/net/* files useful for find…
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample has stripped symbol table

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491790
Start date:	27.09.2021
Start time:	22:40:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	78mne21kC0
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal52.spre.lin@0/1@0/0

Process Tree

- **system is lnxubuntu20**
- 78mne21kC0 (PID: 5226, Parent: 5114, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/78mne21kC0
  - 78mne21kC0 New Fork (PID: 5228, Parent: 5226)
  - 78mne21kC0 New Fork (PID: 5230, Parent: 5226)
    - 78mne21kC0 New Fork (PID: 5232, Parent: 5230)
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

- AV Detection
- Spreading
- Networking
- System Summary
- Malware Analysis System Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Spreading:

Opens /proc/net/* files useful for finding connected devices and routers

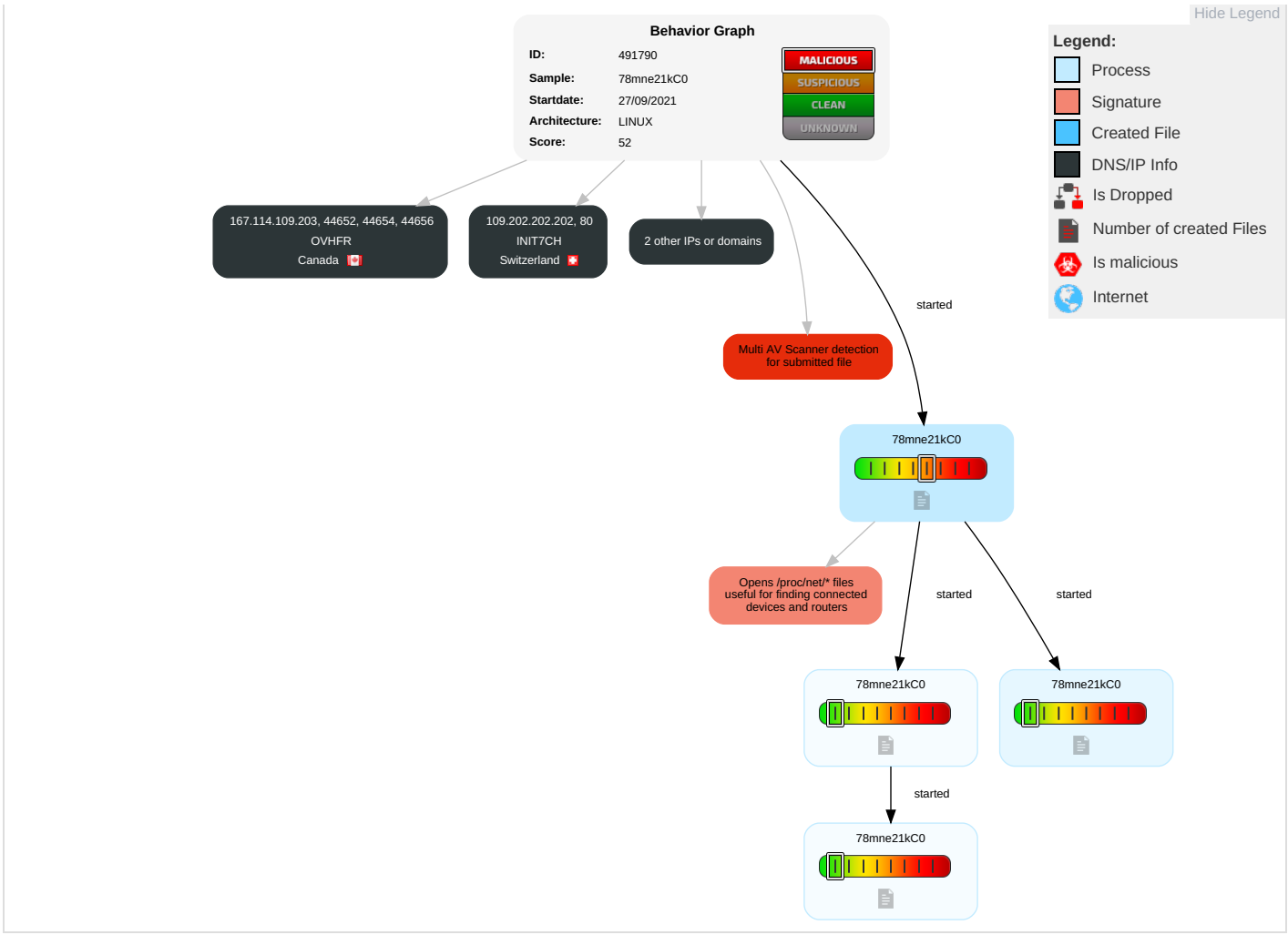
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Remote System Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
78mne21kC0	48%	Virustotal		Browse
78mne21kC0	47%	ReversingLabs	Linux.Backdoor.Bashlite	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.114.109.203	unknown	Canada		16276	OVHFR	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Runtime Messages

Command:	/tmp/78mne21kC0
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	gosh that chinese family at the other table sure ate alot
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
167.114.109.203	exIOc2VzNA	Get hash	malicious	Browse	
	QJWCkLL0hW	Get hash	malicious	Browse	
	sA7VIyESBy	Get hash	malicious	Browse	
	bmcmz7CH5k	Get hash	malicious	Browse	
	CTKpl4Eflw	Get hash	malicious	Browse	
	imqksAx51T	Get hash	malicious	Browse	
	8eyaMuD9DY	Get hash	malicious	Browse	
	tnMrX1z0d5	Get hash	malicious	Browse	
	X86_64	Get hash	malicious	Browse	
109.202.202.202	exIOc2VzNA	Get hash	malicious	Browse	
	QJWCkLL0hW	Get hash	malicious	Browse	
	sA7VIyESBy	Get hash	malicious	Browse	
	bmcmz7CH5k	Get hash	malicious	Browse	
	CTKpl4Eflw	Get hash	malicious	Browse	
	imqksAx51T	Get hash	malicious	Browse	
	8eyaMuD9DY	Get hash	malicious	Browse	
	tnMrX1z0d5	Get hash	malicious	Browse	
	H3NaLv48NK	Get hash	malicious	Browse	
	i07CkTx8C4	Get hash	malicious	Browse	
	p22l26A3Wu	Get hash	malicious	Browse	
	fVNp9NC9l9	Get hash	malicious	Browse	
	wlJuLkUpqE	Get hash	malicious	Browse	
	cAoLg1WlGi	Get hash	malicious	Browse	
	77sa4X7MY2	Get hash	malicious	Browse	
	X86_64	Get hash	malicious	Browse	
	rrVvnZMcFs	Get hash	malicious	Browse	
	pAu4km62R9	Get hash	malicious	Browse	
	kUFNxyzq7h	Get hash	malicious	Browse	
	QMVi2eFA3O	Get hash	malicious	Browse	
91.189.91.43	exIOc2VzNA	Get hash	malicious	Browse	
	QJWCkLL0hW	Get hash	malicious	Browse	
	sA7VIyESBy	Get hash	malicious	Browse	
	bmcmz7CH5k	Get hash	malicious	Browse	
	CTKpl4Eflw	Get hash	malicious	Browse	
	imqksAx51T	Get hash	malicious	Browse	
	8eyaMuD9DY	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tnMrX1z0d5	Get hash	malicious	Browse	
	H3NaLv48NK	Get hash	malicious	Browse	
	i07CkTx8C4	Get hash	malicious	Browse	
	p22l26A3Wu	Get hash	malicious	Browse	
	fVNp9NC9l9	Get hash	malicious	Browse	
	wlJuLkUpqE	Get hash	malicious	Browse	
	cAoLg1WlGi	Get hash	malicious	Browse	
	77sa4X7MY2	Get hash	malicious	Browse	
	X86_64	Get hash	malicious	Browse	
	rrVvnZMcFs	Get hash	malicious	Browse	
	pAu4km62R9	Get hash	malicious	Browse	
	kUFNxyzq7h	Get hash	malicious	Browse	
	QMVi2eFA3O	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CANONICAL-ASGB	exIOc2VzNA	Get hash	malicious	Browse	• 91.189.91.42
	QJWCkLL0hW	Get hash	malicious	Browse	• 91.189.91.42
	sA7VIyESBy	Get hash	malicious	Browse	• 91.189.91.42
	bmcmz7CH5k	Get hash	malicious	Browse	• 91.189.91.42
	CTKpl4Eflw	Get hash	malicious	Browse	• 91.189.91.42
	imqksAx51T	Get hash	malicious	Browse	• 91.189.91.42
	8eyaMuD9DY	Get hash	malicious	Browse	• 91.189.91.42
	tnMrX1z0d5	Get hash	malicious	Browse	• 91.189.91.42
	H3NaLv48NK	Get hash	malicious	Browse	• 91.189.91.42
	i07CkTx8C4	Get hash	malicious	Browse	• 91.189.91.42
	p22l26A3Wu	Get hash	malicious	Browse	• 91.189.91.42
	fVNp9NC9l9	Get hash	malicious	Browse	• 91.189.91.42
	wlJuLkUpqE	Get hash	malicious	Browse	• 91.189.91.42
	cAoLg1WlGi	Get hash	malicious	Browse	• 91.189.91.42
	77sa4X7MY2	Get hash	malicious	Browse	• 91.189.91.42
	X86_64	Get hash	malicious	Browse	• 91.189.91.42
	rrVvnZMcFs	Get hash	malicious	Browse	• 91.189.91.42
	pAu4km62R9	Get hash	malicious	Browse	• 91.189.91.42
	kUFNxyzq7h	Get hash	malicious	Browse	• 91.189.91.42
	QMVi2eFA3O	Get hash	malicious	Browse	• 91.189.91.42
OVHFR	exIOc2VzNA	Get hash	malicious	Browse	• 167.114.109.203
	QJWCkLL0hW	Get hash	malicious	Browse	• 167.114.109.203
	sA7VIyESBy	Get hash	malicious	Browse	• 167.114.109.203
	bmcmz7CH5k	Get hash	malicious	Browse	• 167.114.109.203
	CTKpl4Eflw	Get hash	malicious	Browse	• 167.114.109.203
	imqksAx51T	Get hash	malicious	Browse	• 167.114.109.203
	8eyaMuD9DY	Get hash	malicious	Browse	• 167.114.109.203
	tnMrX1z0d5	Get hash	malicious	Browse	• 167.114.109.203
	X86_64	Get hash	malicious	Browse	• 167.114.109.203
	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 51.255.34.79
	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe	Get hash	malicious	Browse	• 37.59.226.120
	ZFb3RmLJzo	Get hash	malicious	Browse	• 51.70.255.217
	Sht1aYGDIX	Get hash	malicious	Browse	• 51.178.244.189
	nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	Get hash	malicious	Browse	• 178.32.63.50

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	Get hash	malicious	Browse	• 178.32.63.50
	Lrs8NGx6VM.exe	Get hash	malicious	Browse	• 164.132.171.176
	Claim-838392655-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111
	2PzMc3x4WP.exe	Get hash	malicious	Browse	• 87.98.153.120
	e5jVcbuCo5.exe	Get hash	malicious	Browse	• 176.31.32.199
	i7qUJCnMz0.exe	Get hash	malicious	Browse	• 176.31.32.199
INIT7CH	exIOc2VzNA	Get hash	malicious	Browse	• 109.202.202.202
	QJWCkLL0hW	Get hash	malicious	Browse	• 109.202.202.202
	sA7VIyESBy	Get hash	malicious	Browse	• 109.202.202.202
	bmcmz7CH5k	Get hash	malicious	Browse	• 109.202.202.202
	CTKpl4Eflw	Get hash	malicious	Browse	• 109.202.202.202
	imqksAx51T	Get hash	malicious	Browse	• 109.202.202.202
	8eyaMuD9DY	Get hash	malicious	Browse	• 109.202.202.202
	tnMrX1z0d5	Get hash	malicious	Browse	• 109.202.202.202
	H3NaLv48NK	Get hash	malicious	Browse	• 109.202.202.202
	i07CkTx8C4	Get hash	malicious	Browse	• 109.202.202.202
	p22l26A3Wu	Get hash	malicious	Browse	• 109.202.202.202
	fVNp9NC9l9	Get hash	malicious	Browse	• 109.202.202.202
	wlJuLkUpqE	Get hash	malicious	Browse	• 109.202.202.202
	cAoLg1WlGi	Get hash	malicious	Browse	• 109.202.202.202
	77sa4X7MY2	Get hash	malicious	Browse	• 109.202.202.202
	X86_64	Get hash	malicious	Browse	• 109.202.202.202
	rrVvnZMcFs	Get hash	malicious	Browse	• 109.202.202.202
	pAu4km62R9	Get hash	malicious	Browse	• 109.202.202.202
	kUFNxyzq7h	Get hash	malicious	Browse	• 109.202.202.202
	QMVi2eFA3O	Get hash	malicious	Browse	• 109.202.202.202

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/tmp/qemu-open.cFPgFo (deleted)	
Process:	/tmp/78mne21kC0
File Type:	ASCII text
Category:	dropped
Size (bytes):	230
Entropy (8bit):	3.709552666863289
Encrypted:	false
SSDEEP:	6:iekrEcvwAsE5KlwSd4pzKaV6Lpms/a/1VCxGF:ur+m5MwSdIKaV6L1adVRF
MD5:	2E667F43AE18CD1FE3C108641708A82C

/tmp/qemu-open.cFPgFo (deleted)	
SHA1:	12B90DE2DA0FBCFE66F3D6130905E56C8D6A68D3
SHA-256:	6F721492E7A337C5B498A8F55F5EB7AC745AFF716D0B5B08EFF2C1B6B250F983
SHA-512:	D2A0EE2509154EC1098994F38BE172F98F4150399C534A04D5C675D7C05630802225019F19344CC9070C576BC465A4FEB382AC7712DE6BF25E9244B54A9DB830
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Iface.Destination.Gateway .Flags.RefCnt.Use.Metric.Mask..MTU.Window.IRTT .ens160.00000000.c0a80201.0003.0.0.0.000000 00.0.0.0.ens160.c0a80200.00000000.0001.0.0.0.ffffff00.0.0.0.

Static File Info

General

File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.069222226696124
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	78mne21kC0
File size:	89492
MD5:	12cf087e49d1f9abc65f3b9f6d62470c
SHA1:	464abb479aa8d908d534ba39691b427e21b65566
SHA256:	9b4db7f46e24f6f9748d2b82a2497fe237fce6b1f4922c6a4eaffd286a2d3466
SHA512:	156e7dcb2e6bf92cb46e7e1d0dffba83044a930a7a60edc0749675280 16a0a955ec70d5e016c33c6d72ff5b2d9ae38563fedfe42ed9db06d37d9cf2150ade3b2
SSDEEP:	1536:AcpLOlVa0aIh8FuX2W4Wsyf0/zH1B3fc+iDwy8RAlC:AcpyqaId+WFMXxiDwy8RAlC
File Content Preview:	.ELF.....D...4..[.....4. ...(.....K...K.....K...k...k.....g..... .dt.Q.....NV..a....da...".N^NuNV..J9..odf>"y..k. QJ.g.X.#...k.N."y..k. QJ.f.A.....J.g.Hy..K.N.X.....odN^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	88972
Section Header Size:	40
Number of Section Headers:	13
Header String Table Index:	12

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0x122b8	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x80012360	0x12360	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8001236e	0x1236e	0x283a	0x0	0x2	A	0	0	2
.eh_frame	PROGBITS	0x80014ba8	0x14ba8	0x4	0x0	0x2	A	0	0	4

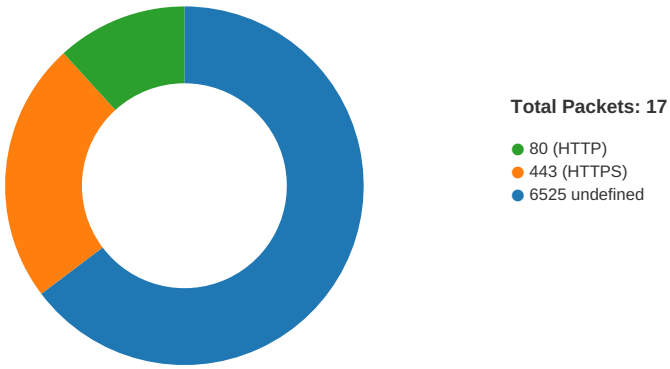
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.ctors	PROGBITS	0x80016bac	0x14bac	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80016bb4	0x14bb4	0x8	0x0	0x3	WA	0	0	4
.jcr	PROGBITS	0x80016bbc	0x14bbc	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80016bc0	0x14bc0	0x3a4	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80016f64	0x14f64	0x6420	0x0	0x3	WA	0	0	4
.comment	PROGBITS	0x0	0x14f64	0xbd0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x15b34	0x56	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x80000000	0x80000000	0x14bac	0x14bac	4.0365	0x5	R E	0x2000		.init .text .fini .rodata .eh_frame
LOAD	0x14bac	0x80016bac	0x80016bac	0x3b8	0x67d8	1.6693	0x6	RW	0x2000		.ctors .dtors .jcr .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: 78mne21kC0 PID: 5226 Parent PID: 5114

General

Start time:	22:41:00
Start date:	27/09/2021
Path:	/tmp/78mne21kC0
Arguments:	/tmp/78mne21kC0
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Deleted

File Read

File Written

Analysis Process: 78mne21kC0 PID: 5228 Parent PID: 5226

General

Start time:	22:41:00
Start date:	27/09/2021
Path:	/tmp/78mne21kC0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 78mne21kC0 PID: 5230 Parent PID: 5226

General

Start time:	22:41:00
Start date:	27/09/2021
Path:	/tmp/78mne21kC0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 78mne21kC0 PID: 5232 Parent PID: 5230

General

Start time:	22:41:00
Start date:	27/09/2021
Path:	/tmp/78mne21kC0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc