ID: 635398
Sample Name: HAEskA4vLV
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:03:12
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

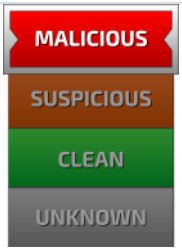
HAEskA4vLV

Overview

General Information

Sample Name:	HAEskA4vLV
Analysis ID:	635398
MD5:	445ea153f39e78..
SHA1:	1ab794165df55b..
SHA256:	3c9c1a3e7f02d9…
Tags:	32 elf mirai motorola
Infos:	

Detection



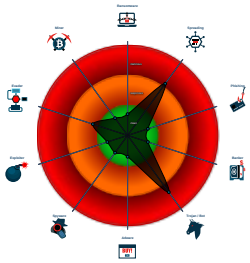
Mirai

Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample listens on a socket
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635398
Start date and time: 27/05/202221:03:12	2022-05-27 21:03:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HAEskA4vLV
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:	mal64.spre.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/HAEskA4vLV
PID:	6233
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- HAEskA4vLV (PID: 6233, Parent: 6135, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/HAEskA4vLV
  - HAEskA4vLV New Fork (PID: 6235, Parent: 6233)
  - HAEskA4vLV New Fork (PID: 6236, Parent: 6233)
    - HAEskA4vLV New Fork (PID: 6240, Parent: 6236)
    - HAEskA4vLV New Fork (PID: 6242, Parent: 6236)
      - HAEskA4vLV New Fork (PID: 6244, Parent: 6242)
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

System Summary

Sample tries to kill multiple processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

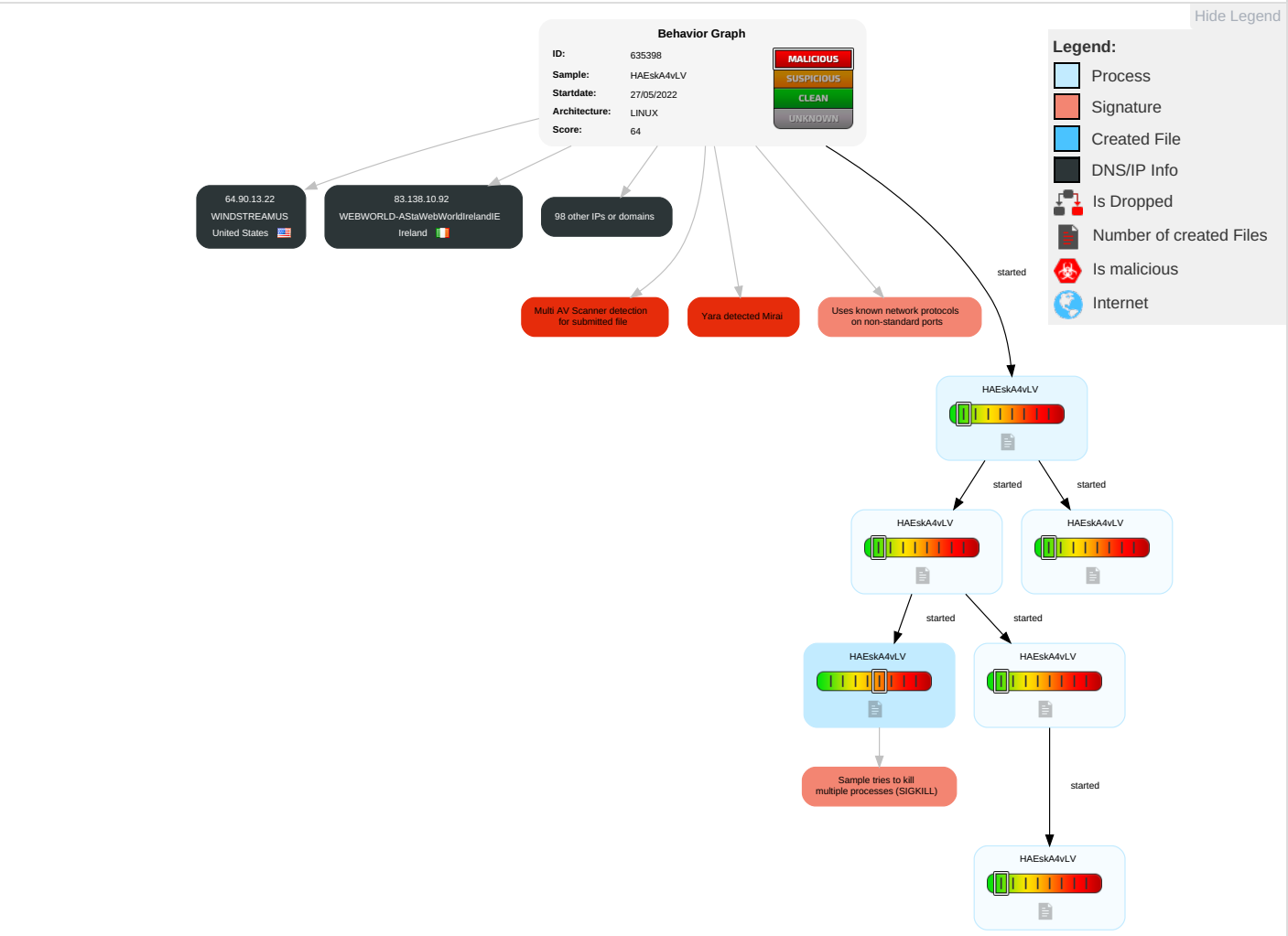
Mitre Att&ck Matrix

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	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Service Stop
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Non-Standard Port	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	1 Application Layer Protocol	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
HAEskA4vLV	37%	Virustotal		Browse
HAEskA4vLV	35%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

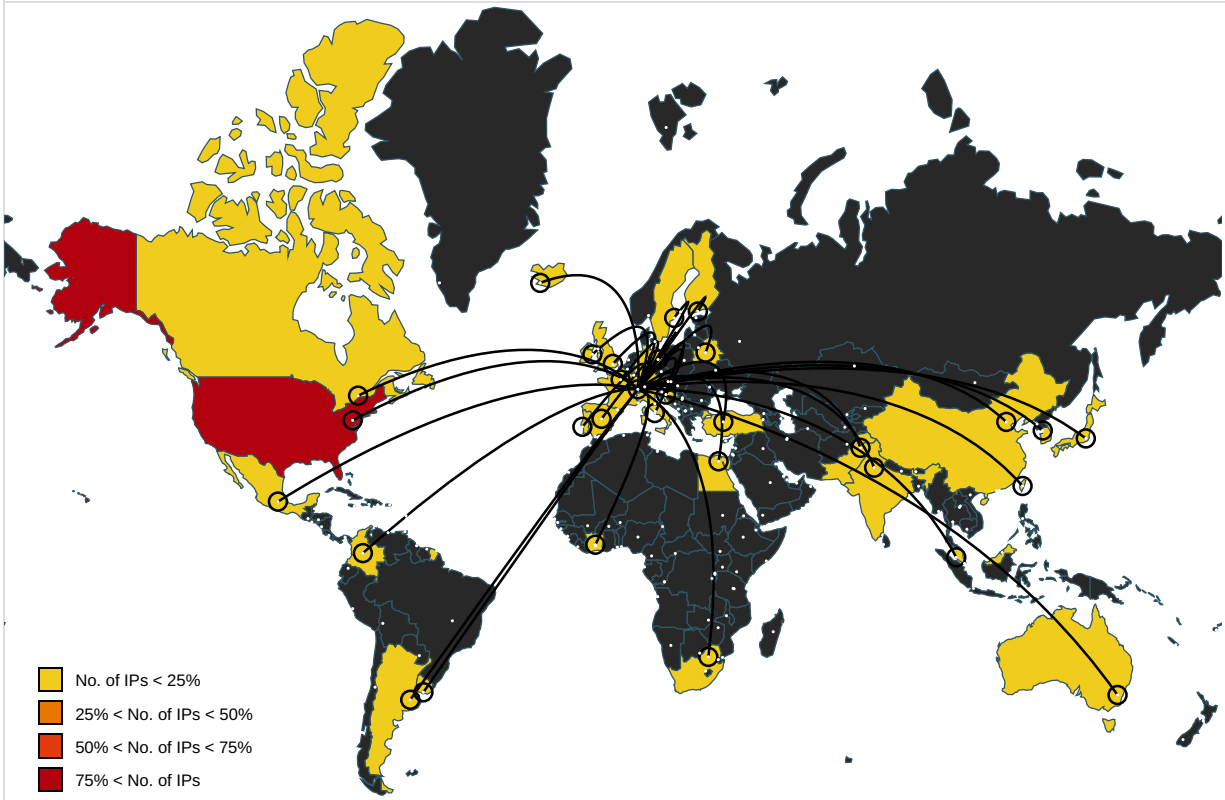
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
90.97.170.84	unknown	France		28708	ORANGEFR-PORTAL-ASDSImutualizedinternetaccessFR	false
169.5.24.89	unknown	United States		203	CENTURYLINK-LEGACY-LVLT-203US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.252.255.29	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
179.12.175.80	unknown	Colombia		27831	ColombiaMovilCO	false
31.107.23.184	unknown	United Kingdom		12576	EELtdGB	false
46.125.185.237	unknown	Austria		8412	TMARennweg97-99AT	false
30.35.136.86	unknown	United States		7922	COMCAST-7922US	false
217.179.192.222	unknown	United Kingdom		5503	RMIFLGB	false
94.122.216.129	unknown	Turkey		12978	DOGAN-ONLINETR	false
135.76.111.146	unknown	United States		18676	AVAYAUS	false
128.90.30.179	unknown	United States		22363	PHMGMT-AS1US	false
195.10.52.226	unknown	United Kingdom		1273	CWVodafoneGroupPLCEU	false
106.46.124.226	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
205.247.222.200	unknown	United States		3257	GTT-BACKBONEGTTDE	false
60.51.49.48	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
191.65.185.153	unknown	Colombia		26611	COMCELSACO	false
106.76.2.64	unknown	India		45271	ICLNET-AS-APIdeaCellularLimitedIN	false
246.57.16.74	unknown	Reserved		unknown	unknown	false
64.90.13.22	unknown	United States		7029	WINDSTREAMUS	false
223.68.161.195	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
93.84.101.62	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
67.127.118.193	unknown	United States		7018	ATT-INTERNET4US	false
255.162.56.216	unknown	Reserved		unknown	unknown	false
32.123.32.26	unknown	United States		7018	ATT-INTERNET4US	false
78.3.131.236	unknown	Croatia (LOCAL Name: Hrvatska)		5391	T-HTCroatianTelecomIncHR	false
80.137.246.164	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
201.252.24.249	unknown	Argentina		7303	TelecomArgentinaSAAR	false
98.98.237.205	unknown	United States		7018	ATT-INTERNET4US	false
67.48.33.85	unknown	United States		11427	TWC-11427-TEXASUS	false
198.191.91.196	unknown	United States		2152	CSUNET-NWUS	false
33.111.186.224	unknown	United States		2686	ATGS-MMD-ASUS	false
192.49.201.169	unknown	Finland		375	TIETOTIE-ASPOBox38FI-00441HelsinkiFinlandEU	false
144.152.175.199	unknown	United States		58541	CHINATELECOM-SHANDONG-QINGDAO-IDCQingdao266000CN	false
83.138.10.92	unknown	Ireland		30900	WEBWORLD-AStaWebWorldIrelandIE	false
126.26.13.195	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
34.7.3.33	unknown	United States		2686	ATGS-MMD-ASUS	false
181.48.255.124	unknown	Colombia		14080	TelmexColombiaSACO	false
73.215.212.83	unknown	United States		7922	COMCAST-7922US	false
106.72.235.235	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
164.151.240.108	unknown	South Africa		37130	SITA-ASZA	false
171.60.217.79	unknown	India		24560	AIRTELBROADBAND-AS-APBhartiAirtelLtdTelemediaServices	false
49.159.200.168	unknown	Taiwan; Republic of China (ROC)		24164	UBBNET-AS-TWUNIONBROADBANDNETWORKTW	false
217.198.143.142	unknown	Germany		34309	LINK11Link11GmbHDE	false
189.221.199.41	unknown	Mexico		28509	CablemasTelecomunicacionesSAdeCVMX	false
125.251.7.21	unknown	Korea Republic of		38394	GOESN-AS-KRGyeonggidoSeongnamOfficeofEducationKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
61.73.160.163	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
78.73.118.63	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
107.184.217.188	unknown	United States		20001	TWC-20001-PACWESTUS	false
202.139.135.57	unknown	Australia		7474	OPTUSCOM-AS01-AUSingTelOptusPtyLtdAU	false
219.86.3.214	unknown	Taiwan; Republic of China (ROC)		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	false
110.123.21.120	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
30.227.233.209	unknown	United States		7922	COMCAST-7922US	false
182.246.241.9	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
29.191.94.89	unknown	United States		7922	COMCAST-7922US	false
174.85.82.247	unknown	United States		20115	CHARTER-20115US	false
39.63.138.0	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
74.103.139.189	unknown	United States		701	UUNETUS	false
114.237.34.128	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
105.94.59.158	unknown	Egypt		36992	ETISALAT-MISREG	false
124.31.169.22	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
88.149.62.148	unknown	Iceland		12969	VODAFONE_ICELANDIS	false
12.198.36.119	unknown	United States		7018	ATT-INTERNET4US	false
142.116.146.84	unknown	Canada		577	BACOMCA	false
4.146.131.214	unknown	United States		3356	LEVEL3US	false
241.232.37.7	unknown	Reserved		unknown	unknown	false
64.156.138.117	unknown	United States		3356	LEVEL3US	false
114.53.79.211	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
154.234.45.165	unknown	Cote D'ivoire		36974	AFNET-ASCI	false
144.147.142.234	unknown	United States		1460	DNIC-ASBLK-01458-01460US	false
240.52.83.224	unknown	Reserved		unknown	unknown	false
156.70.138.52	unknown	United States		297	AS297US	false
147.254.126.164	unknown	United States		1213	HEANETIE	false
183.153.123.153	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
53.133.121.204	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
157.162.143.89	unknown	Germany		22192	SSHENETUS	false
192.77.104.107	unknown	United States		427	AFCONC-BLOCK1-ASUS	false
98.209.182.234	unknown	United States		7922	COMCAST-7922US	false
94.35.173.140	unknown	Italy		8612	TISCALI-IT	false
167.75.59.236	unknown	United States		3356	LEVEL3US	false
109.76.80.220	unknown	Ireland		15502	VODAFONE-IRELAND-ASNIE	false
19.183.164.159	unknown	United States		3	MIT-GATEWAYSUS	false
27.53.120.240	unknown	Taiwan; Republic of China (ROC)		9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
53.231.152.118	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
54.139.242.174	unknown	United States		14618	AMAZON-AESUS	false
202.39.229.207	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
18.141.1.158	unknown	United States		16509	AMAZON-02US	false
243.236.181.133	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.61.71.154	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
108.144.104.131	unknown	United States		16509	AMAZON-02US	false
100.83.140.204	unknown	Reserved		701	UUNETUS	false
245.118.65.228	unknown	Reserved		unknown	unknown	false
38.136.33.37	unknown	United States		174	COGENT-174US	false
81.76.63.240	unknown	United Kingdom		3269	ASN-IBSNAZIT	false
85.127.123.174	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
211.109.228.6	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
214.178.86.224	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
193.137.26.80	unknown	Portugal		1930	RCCNFundacaoparaaCienciaeaTecnologiaIPPT	false
15.172.248.37	unknown	United States		71	HP-INTERNET-ASUS	false
212.170.182.246	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
65.26.228.228	unknown	United States		10796	TWC-10796-MIDWESTUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.238586795542201
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	HAEskA4vLV

File size:	93480
MD5:	445ea153f39e7868760107609a343b28
SHA1:	1ab794165df55bdd9a4a6d1e7023b550fa29e277
SHA256:	3c9c1a3e7f02d9a27f946c3edc5c45554e8884262833b6c648a98880070ac017
SHA512:	2f52101989fc5e380669d1ed61d4deb71527b1d9c192994abcc0b0a0284a1463d8502459f7be5eacdac0bb162cd927b8002a1214595dc93e8504066a5ef5d059
SSDEEP:	1536:Mj+9mKLMisFvCuyMydl91jkjgAnsuouXqz88hZZro6SBvAhGDZ9agQk:fL4iaCfMydl91jCsupXqztZro6mN9hQk
TLSH:	CC933B97F800EDBEF809D7774453490AB230B7A04E921A727257396BEC7A1E4193BF46
File Content Preview:	.ELF.....D...4..k.....4. ...(.....g...g..... .....g.....f..... .dt.Q.....NV..a....da...J\N^NuNV..J9...Xf>"y.... QJ.g.X.#.....N."y.... QJ.f.A.....J.g.Hy..g.N.X.....XN^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:	93080
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

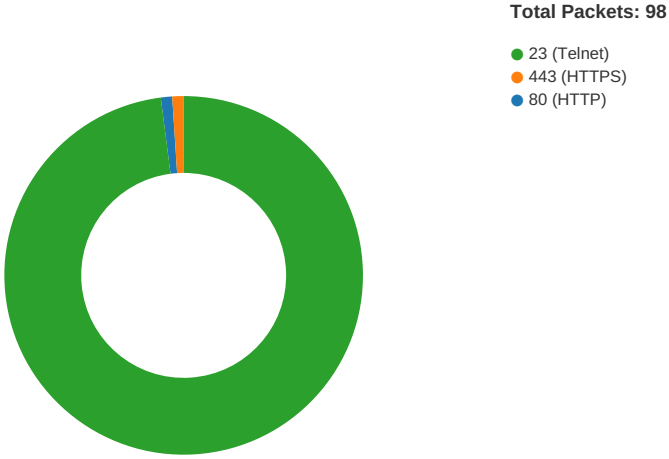
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0x14a86	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x80014b2e	0x14b2e	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x80014b3c	0x14b3c	0x1c5f	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x800187a0	0x167a0	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x800187a8	0x167a8	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x800187b4	0x167b4	0x3a4	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80018b58	0x16b58	0x62cc	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x16b58	0x3e	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	0x1679b	0x1679b	4.1174	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x167a0	0x800187a0	0x800187a0	0x3b8	0x6684	1.6081	0x6	RW	0x2000		.ctors .dtors .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: HAEskA4vLV PID: 6233, Parent PID: 6135

General

Start time:	21:04:03
Start date:	27/05/2022
Path:	/tmp/HAEskA4vLV
Arguments:	/tmp/HAEskA4vLV
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: HAEskA4vLV PID: 6235, Parent PID: 6233

General

Start time:	21:04:03
Start date:	27/05/2022
Path:	/tmp/HAEskA4vLV
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HAEskA4vLV PID: 6236, Parent PID: 6233

General

Start time:	21:04:03
Start date:	27/05/2022
Path:	/tmp/HAEskA4vLV
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HAEskA4vLV PID: 6240, Parent PID: 6236

General

Start time:	21:04:03
Start date:	27/05/2022

Path:	/tmp/HAEskA4vLV
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: HAEskA4vLV PID: **6242**, Parent PID: **6236**

General

Start time:	21:04:03
Start date:	27/05/2022
Path:	/tmp/HAEskA4vLV
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HAEskA4vLV PID: **6244**, Parent PID: **6242**

General

Start time:	21:04:03
Start date:	27/05/2022
Path:	/tmp/HAEskA4vLV
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc