ID: 1456793
Sample Name:
HTUyCRuDev.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 19:35:35
Date: 13/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

Linux Analysis Report

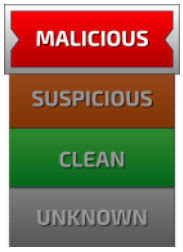
HTUyCRuDev.elf

Overview

General Information

Sample name:	HTUyCRuDev.elfrenamed because original name is a hash value
Original sample name:	cdfd23d13080c..
Analysis ID:	1456793
MD5:	cdfd23d13080c..
SHA1:	92244f7c8392a..
SHA256:	4dc3b6dc4cfda..
Tags:	32 elf mirai motorola
Infos:	

Detection

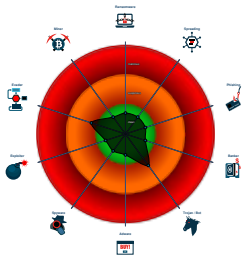


Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Detected TCP or UDP traffic on non…
- Sample has stripped symbol table
- Sample listens on a socket
- Tries to connect to HTTP servers, b…
- Uses the "uname" system call to qu…

Classification



General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1456793
Start date and time:	2024-06-13 19:35:35 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample name:	HTUyCRuDev.elfrenamed because original name is a hash value
Original Sample Name:	cdfd23d13080c787cf5784248d62133f.elf
Detection:	MAL
Classification:	mal56.linELF@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/HTUyCRuDev.elf
PID:	6210
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	JEW was here lol
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- HTUyCRuDev.elf (PID: 6210, Parent: 6122, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/HTUyCRuDev.elf
  - HTUyCRuDev.elf New Fork (PID: 6212, Parent: 6210)
  - HTUyCRuDev.elf New Fork (PID: 6213, Parent: 6210)
    - HTUyCRuDev.elf New Fork (PID: 6216, Parent: 6213)
    - HTUyCRuDev.elf New Fork (PID: 6217, Parent: 6213)
- **cleanup**

Yara Signatures

No yara matches

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

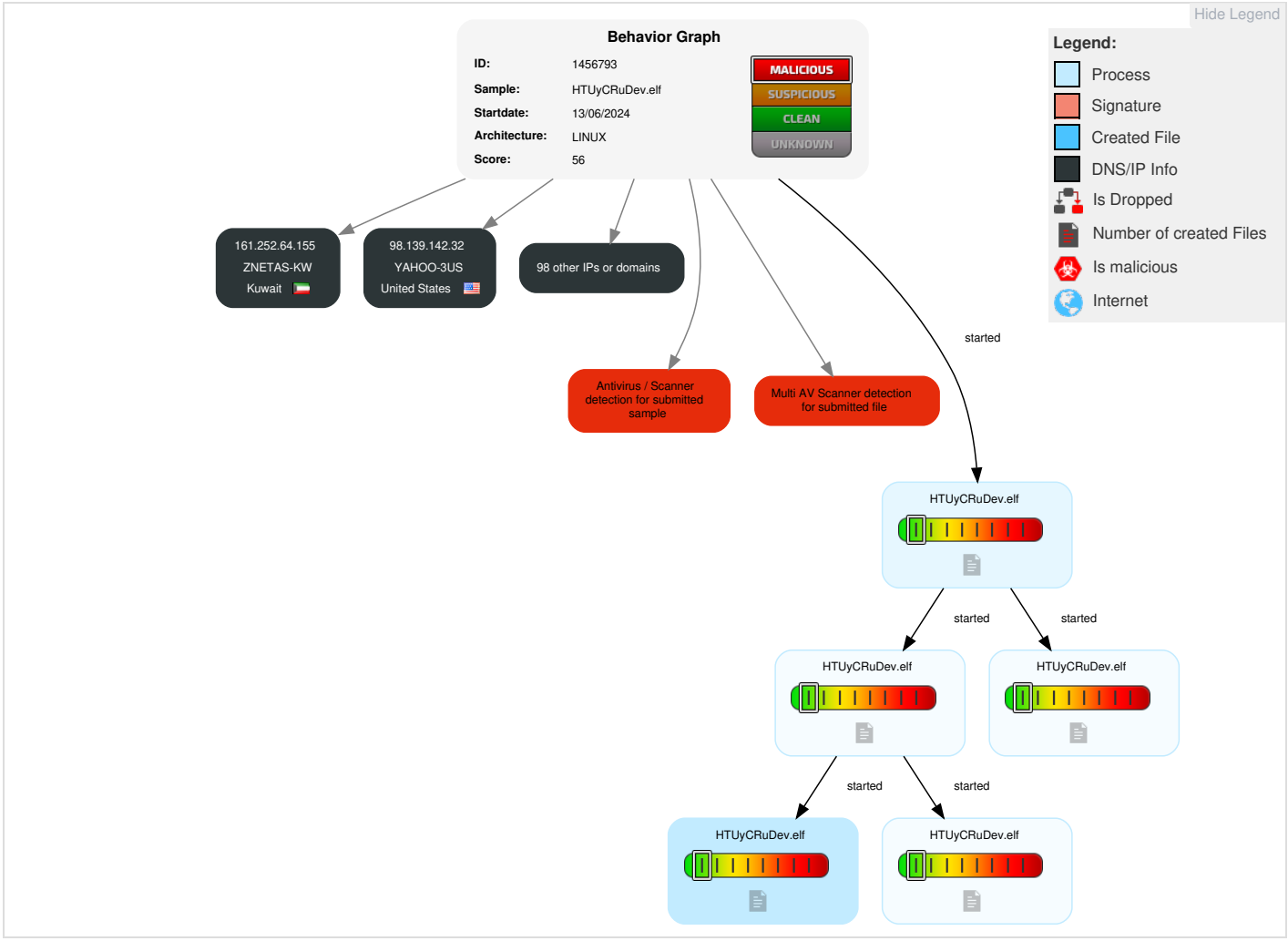
Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	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	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
HTUyCRuDev.elf	55%	ReversingLabs	Linux.Trojan.Mirai	
HTUyCRuDev.elf	100%	Avira	EXP/ELF.Mirai.Botnet.o	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

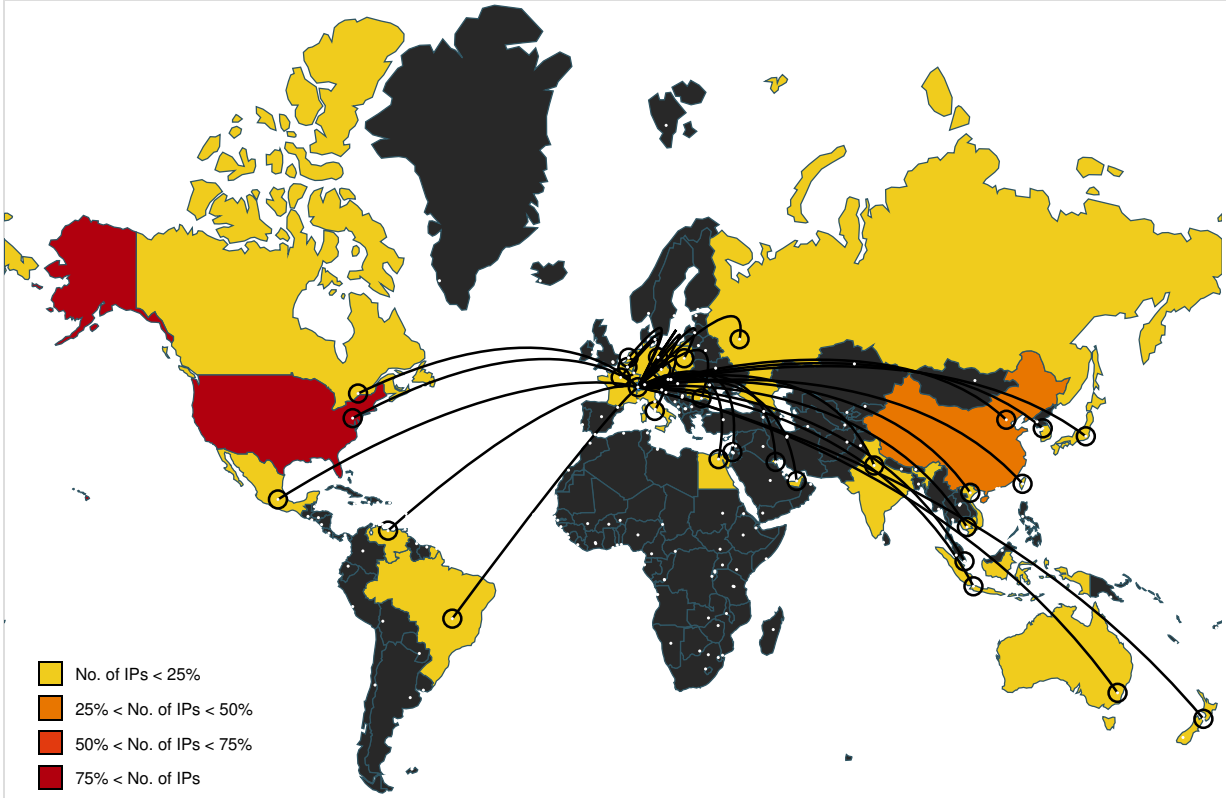
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
98.139.142.32	unknown	United States		26101	YAHOO-3US	false
116.175.62.41	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
211.214.93.246	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
58.40.193.242	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
111.80.81.134	unknown	Taiwan; Republic of China (ROC)		2510	INFOWEBFUJITSULIMITEDJP	false
65.66.253.140	unknown	United States		7018	ATT-INTERNET4US	false
139.191.120.134	unknown	European Union		2611	BELNETBE	false
155.229.97.21	unknown	United States		18566	MEGAPATH5-US	false
115.188.31.87	unknown	New Zealand		4771	SPARKNZSparkNewZealandTradingLtdNZ	false
63.75.247.60	unknown	United States		701	UUNETUS	false
114.73.115.157	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
184.216.100.5	unknown	United States		10507	SPCSUS	false
176.243.1.41	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
77.91.171.207	unknown	Palestinian Territory Occupied		12975	PALTEL-ASPALTELAutonomousSystemPS	false
97.118.60.43	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
173.229.136.204	unknown	United States		10405	UPRR-ASN-01US	false
117.114.195.159	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
155.90.12.142	unknown	United States		4010	DNIC-AS-04010US	false
93.231.244.24	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
121.44.191.221	unknown	Australia		4739	INTERNODE-ASInternodePtyLtdAU	false
47.111.235.129	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
53.25.129.93	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
186.164.26.182	unknown	Venezuela		21575	ENTELPERUSAPE	false
174.50.238.101	unknown	United States		7922	COMCAST-7922US	false
109.183.73.38	unknown	Czech Republic		12767	PRAGONET-ASCZ	false
12.174.10.254	unknown	United States		7018	ATT-INTERNET4US	false
175.131.187.169	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
112.220.121.6	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
182.23.97.162	unknown	Indonesia		4800	LINTASARTA-AS-APNetworkAccessProviderandInternetServic	false
4.31.146.161	unknown	United States		3356	LEVEL3US	false
114.52.161.116	unknown	Korea Republic of		18302	SKG_NW-AS-KRSKTelecomKR	false
109.32.62.199	unknown	Netherlands		15480	VFNL-ASVodafoneNLAutonomousSystemNL	false
49.57.109.29	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
12.77.153.113	unknown	United States		7018	ATT-INTERNET4US	false
138.203.175.153	unknown	Belgium		5488	BELGACOMBE	false
27.191.234.159	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
132.145.12.79	unknown	United States		31898	ORACLE-BMC-31898US	false
221.215.46.75	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
164.219.30.78	unknown	United States		5180	DNIC-ASBLK-05120-05376US	false
182.116.76.173	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
92.161.37.70	unknown	France		3215	FranceTelecom-OrangeFR	false
198.216.73.110	unknown	United States		3354	THENET-AS-3354US	false
184.145.64.108	unknown	Canada		577	BACOMCA	false
200.133.116.170	unknown	Brazil		1916	AssociacaoRedeNacionaldeEnsinoePesquisaBR	false
160.194.248.96	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
183.153.123.185	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
61.58.219.52	unknown	Taiwan; Republic of China (ROC)		9676	SAVECOM-TWSaveComInternationInc TW	false
93.7.2.230	unknown	France		15557	LDCOMNETFR	false
35.184.32.6	unknown	United States		15169	GOOGLEUS	false
113.171.247.190	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
170.11.192.63	unknown	United States		1621	ASN-SECURIANUS	false
190.205.79.171	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
104.169.169.5	unknown	United States		5650	FRONTIER-FRTRUS	false
206.155.113.41	unknown	United States		23280	OS33US	false
8.222.72.242	unknown	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
52.168.74.222	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
23.154.57.240	unknown	Reserved		26445	BNCUS	false
39.180.65.78	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
47.42.232.95	unknown	United States		20115	CHARTER-20115US	false
121.180.167.109	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
220.70.36.136	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
147.118.233.65	unknown	United States		10370	NORTHWEST-AIRLINESUS	false
36.37.168.145	unknown	Cambodia		38623	VIETTELCAMBODIA-AS-APISPIXPINCAMBODIAWITHTHEBESTVERV	false
98.10.209.90	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
126.68.137.13	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
76.207.131.216	unknown	United States		7018	ATT-INTERNET4US	false
12.88.113.233	unknown	United States		7018	ATT-INTERNET4US	false
161.252.64.155	unknown	Kuwait		42781	ZNETAS-KW	false
64.151.37.208	unknown	United States		18712	SUREWEST-KANSASUS	false
113.148.217.183	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
110.129.234.181	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
210.239.174.147	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
107.170.128.159	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
134.198.98.189	unknown	United States		36269	UOFSCRANTONUS	false
53.152.119.186	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
143.250.200.104	unknown	United States		27064	DNIC-ASBLK-27032-27159US	false
178.73.57.176	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
93.43.182.90	unknown	Italy		12874	FASTWEBIT	false
126.83.62.95	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
58.49.78.172	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
71.207.148.163	unknown	United States		7922	COMCAST-7922US	false
114.69.243.149	unknown	India		18002	WORLDPHONE-INASNumberforInterdomainRoutingIN	false
113.105.112.161	unknown	China		58466	CT-GUANGZHOU-IDCCHINANETGuangdongprovincenetworkCN	false
196.147.109.227	unknown	Egypt		36935	Vodafone-EG	false
189.227.237.82	unknown	Mexico		8151	UninetSAdeCVMX	false
100.158.41.172	unknown	United States		21928	T-MOBILE-AS21928US	false
169.151.182.215	unknown	United States		2386	INS-ASUS	false
134.31.121.145	unknown	Canada		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
92.255.42.53	unknown	Russian Federation		205282	RUSENRESRU	false
179.120.163.203	unknown	Brazil		26615	TIMSABR	false
137.175.34.2	unknown	United States		54600	PEGTECHINCUS	false
112.44.125.146	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
50.206.19.177	unknown	United States		7922	COMCAST-7922US	false
92.96.166.207	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
74.112.91.89	unknown	Canada		63350	FONCLOUDCA	false
37.251.157.124	unknown	Romania		34358	WEBCLASSITRO	false
39.29.180.17	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
19.57.4.154	unknown	United States		3	MIT-GATEWAYSUS	false
162.199.226.9	unknown	United States		7018	ATT-INTERNET4US	false
135.198.43.75	unknown	United States		8190	MDNXGB	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):	6.261140366553239
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	HTUyCRuDev.elf
File size:	61'432 bytes
MD5:	cdfd23d13080c787cf5784248d62133f
SHA1:	92244f7c8392ac821276be00de438806e9eba4c7
SHA256:	4dc3b6dc4cfda3cd8762083e96f394bae961573ffa269f961737a4ce6705c79f
SHA512:	b97efa9f5590bae9239f2e75ecf45980281d3e54ec40cf61965d38d664d6ddb0ac3892789bfa3780d00de7cc6e2553ef32403ad01ed06d3d93ac4e1f8a9dad46
SSDEEP:	768:neT+6JhUvtNaEVG1xPgj2x9+iGCvYN1ul8yXLyCIlqXxXv2XWFGN:nInQvtNFG1xIjeWvNUl8yXx2qBvyTN
TLSH:	21534E96B401AD3CFC5BE6BD40165A19FA313B3016A30F5B9BA7FC839C321A6DD16D41
File Content Preview:	.ELF.....D...4...h.....4. ...(..... .....(..... .dt.Q.....NV..a....da.....N^NuNV..J9...(f>"y.... QJ.g.X.#.....N."y.... QJ.f.A.....J.g.Hy....N.X.....(N^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

ELF header	
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:	61032
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

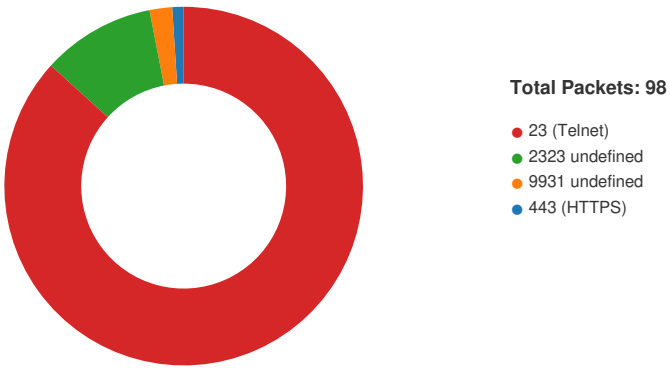
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0xdfd6	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000e07e	0xe07e	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000e08c	0xe08c	0xb6e	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x80010c00	0xec00	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80010c08	0xec08	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80010c14	0xec14	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80010e28	0xee28	0x2a8	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xee28	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	0xebfa	0xebfa	6.2931	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0xec00	0x80010c00	0x80010c00	0x228	0x4d0	3.0392	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: HTUyCRuDev.elf PID: **6210**, Parent PID: **6122**

General

Start time (UTC):	17:36:13
Start date (UTC):	13/06/2024
Path:	/tmp/HTUyCRuDev.elf
Arguments:	/tmp/HTUyCRuDev.elf
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: HTUyCRuDev.elf PID: **6212**, Parent PID: **6210**

General

Start time (UTC):	17:36:13
Start date (UTC):	13/06/2024
Path:	/tmp/HTUyCRuDev.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HTUyCRuDev.elf PID: **6213**, Parent PID: **6210**

General

Start time (UTC):	17:36:13
Start date (UTC):	13/06/2024
Path:	/tmp/HTUyCRuDev.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HTUyCRuDev.elf PID: **6216**, Parent PID: **6213**

General

Start time (UTC):	17:36:13
Start date (UTC):	13/06/2024
Path:	/tmp/HTUyCRuDev.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: HTUyCRuDev.elf PID: **6217**, Parent PID: **6213**

General

Start time (UTC):	17:36:13
Start date (UTC):	13/06/2024
Path:	/tmp/HTUyCRuDev.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc