ID: 553221
Sample Name: hWLlYv2MAX
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:57:49
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report hWLlYv2MAX 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
General Information 3
Process Tree 3
Yara Overview 4
PCAP (Network Traffic) 4
Jbx Signature Overview 4
AV Detection: 4
Networking: 4
Hooking and other Techniques for Hiding and Protection: 4
Stealing of Sensitive Information: 4
Remote Access Functionality: 4
Mitre Att&ck Matrix 4
Malware Configuration 5
Behavior Graph 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted IPs 6
Public 6
Runtime Messages 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
Static ELF Info 9
ELF header 9
Sections 9
Program Segments 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 10
System Behavior 10
Analysis Process: hWLlYv2MAX PID: 5210 Parent PID: 5109 10
General 10
File Activities 10
File Read 11
Analysis Process: hWLlYv2MAX PID: 5212 Parent PID: 5210 11
General 11
Analysis Process: hWLlYv2MAX PID: 5214 Parent PID: 5212 11
General 11
Analysis Process: hWLlYv2MAX PID: 5215 Parent PID: 5212 11
General 11
Analysis Process: hWLlYv2MAX PID: 5218 Parent PID: 5212 11
General 11
File Activities 11
File Read 11
Directory Enumerated 11
Analysis Process: dash PID: 5260 Parent PID: 4331 12
General 12
Analysis Process: rm PID: 5260 Parent PID: 4331 12
General 12
File Activities 12
File Deleted 12
File Read 12

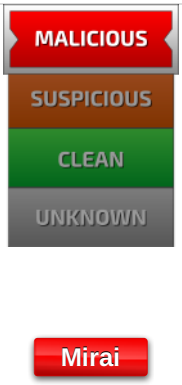
Linux Analysis Report hWLlYv2MAX

Overview

General Information

Sample Name:	hWLlYv2MAX
Analysis ID:	553221
MD5:	dbbc5166ca6759..
SHA1:	26f84c2f48d9bd5..
SHA256:	086d4bcb764c12..
Tags:	32 elf mirai motorola
Infos:	

Detection

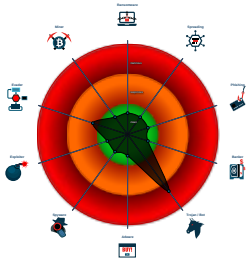


Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample has stripped symbol table
- Uses the "uname" system call to qu...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...
- Executes the "rm" command used to...
- Sample listens on a socket
- Sample contains strings indicative o...

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:	34.0.0 Boulder Opal
Analysis ID:	553221
Start date:	14.01.2022
Start time:	13:57:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	hWLlYv2MAX
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:	mal68.troj.lin@0/0@0/0
Warnings:	Show All

Process Tree

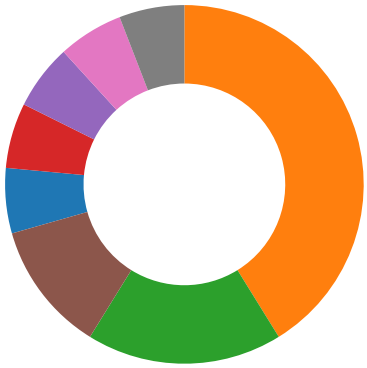
- **system is lnxubuntu20**
- hWLlYv2MAX (PID: 5210, Parent: 5109, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/hWLlYv2MAX
  - hWLlYv2MAX New Fork (PID: 5212, Parent: 5210)
    - hWLlYv2MAX New Fork (PID: 5214, Parent: 5212)
    - hWLlYv2MAX New Fork (PID: 5215, Parent: 5212)
    - hWLlYv2MAX New Fork (PID: 5218, Parent: 5212)
- dash New Fork (PID: 5260, Parent: 4331)
- rm (PID: 5260, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.c898EgJy36 /tmp/tmp.k9ZN1wUC0G /tmp/tmp.JL9rmsZ4ya
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

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

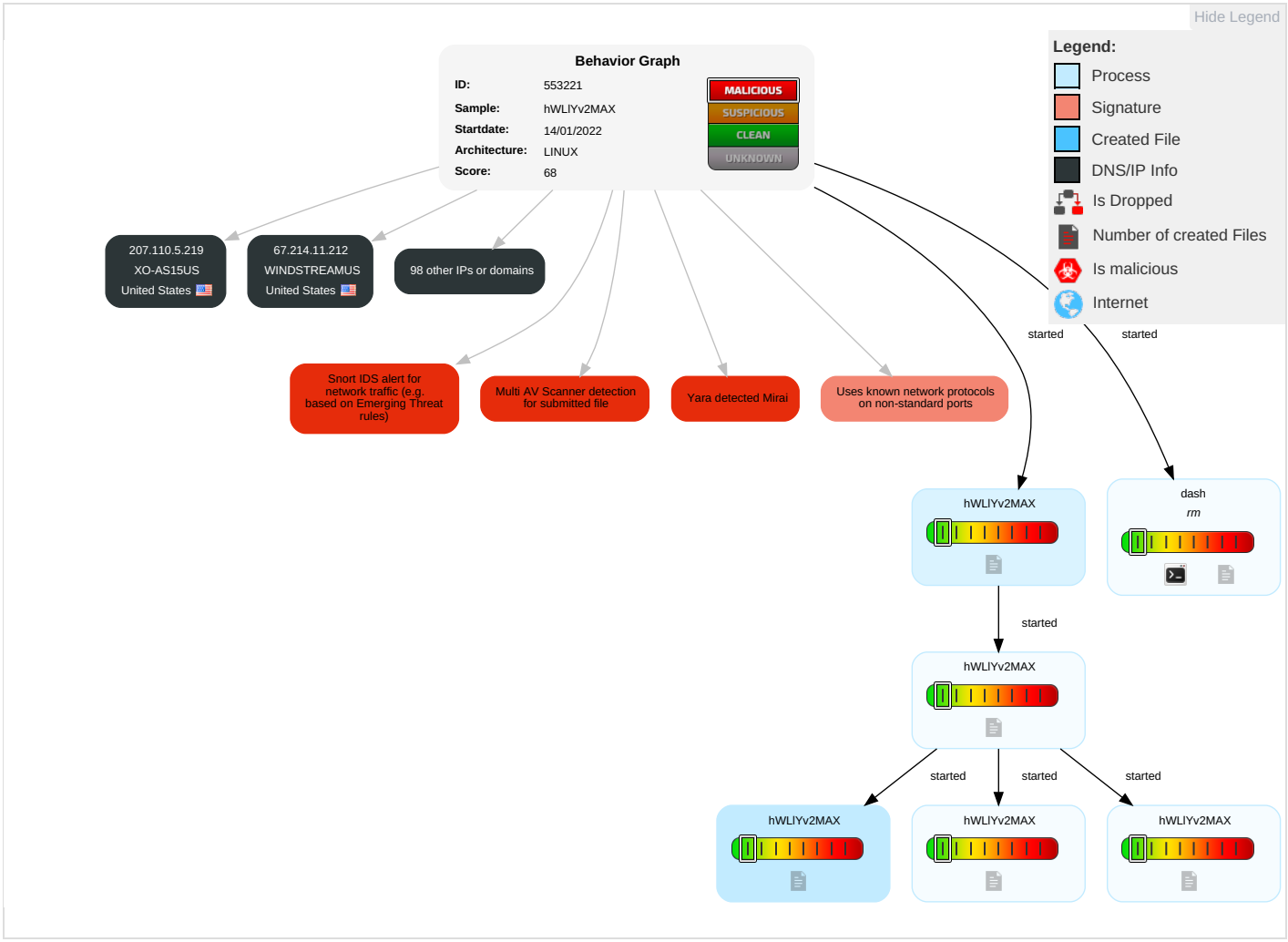
Mitre Att&ck Matrix

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	File Deletion 1	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	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 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
hWLIYv2MAX	34%	Metadefender		Browse
hWLIYv2MAX	58%	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

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.187.134.146	unknown	United States		701	UUNETUS	false
188.40.114.118	unknown	Germany		24940	HETZNER-ASDE	false
182.86.109.112	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
189.6.48.51	unknown	Brazil		28573	CLAROSABR	false
177.45.178.7	unknown	Brazil		19182	TELEFONICABRASILSABR	false
70.204.156.162	unknown	United States		22394	CELLCOUS	false
83.206.110.213	unknown	France		3215	FranceTelecom-OrangeFR	false
31.253.231.57	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
140.244.7.222	unknown	United States		22488	CENGAGE-NYALBUS	false
223.252.212.230	unknown	China		45062	NETEASE-ASGuangzhouNetEaseComputerSystemCoLtdCN	false
134.233.55.95	unknown	United States		531	DNIC-AS-00531US	false
175.19.79.139	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
52.186.170.176	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
9.220.201.31	unknown	United States		3356	LEVEL3US	false
125.10.124.39	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
154.42.81.61	unknown	United States		174	COGENT-174US	false
223.199.86.53	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
170.221.237.217	unknown	United States		8103	STATE-OF-FLAUS	false
110.161.133.195	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
8.244.110.122	unknown	United States		3356	LEVEL3US	false
47.223.219.114	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
204.73.77.29	unknown	United States		5006	VOYANTUS	false
159.89.53.206	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
88.85.139.111	unknown	Finland		34263	MPYNET-ASMikonkatu16FI	false
87.24.144.210	unknown	Italy		3269	ASN-IBSNAZIT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.229.163.128	unknown	United States		7922	COMCAST-7922US	false
36.97.39.151	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
194.3.186.160	unknown	France		3215	FranceTelecom-OrangeFR	false
177.62.126.184	unknown	Brazil		26599	TELEFONICABRASILSABR	false
4.77.193.188	unknown	United States		3356	LEVEL3US	false
69.17.129.80	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
131.106.230.187	unknown	United States		6079	RCN-ASUS	false
58.76.145.3	unknown	Korea Republic of		23584	HYROADPUSAN-AS-KRPUSANCABLETVSYSTEMCOLTDKR	false
114.99.149.239	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
209.61.254.234	unknown	United States		14361	HOPONE-GLOBALUS	false
73.58.216.132	unknown	United States		7922	COMCAST-7922US	false
178.164.247.26	unknown	Hungary		20845	DIGICABLEHU	false
58.208.204.132	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
101.145.47.129	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
115.244.44.118	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
142.228.94.116	unknown	Canada		13576	SDNW-13576US	false
76.124.251.209	unknown	United States		7922	COMCAST-7922US	false
69.111.100.174	unknown	United States		7018	ATT-INTERNET4US	false
12.186.214.9	unknown	United States		7018	ATT-INTERNET4US	false
44.57.111.197	unknown	United States		7377	UCSDUS	false
64.75.129.18	unknown	United States		3776	ALOHANETUS	false
138.52.21.209	unknown	United States		2611	BELNETBE	false
86.209.52.138	unknown	France		3215	FranceTelecom-OrangeFR	false
77.227.142.204	unknown	Spain		12430	VODAFONE_ESES	false
219.106.230.114	unknown	Japan		9600	SONYTELECOMSo-netCorporationJP	false
99.55.160.71	unknown	United States		7018	ATT-INTERNET4US	false
208.141.122.166	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
83.69.89.6	unknown	Russian Federation		20485	TRANSTELECOMMoscowRussiaRU	false
110.246.240.102	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
71.16.36.162	unknown	United States		7029	WINDSTREAMUS	false
139.69.76.112	unknown	United States		3549	LVLT-3549US	false
155.111.136.85	unknown	United States		61153	PROCTERGAMBLENCSCDE	false
116.40.101.187	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
72.74.241.129	unknown	United States		701	UUNETUS	false
192.70.163.14	unknown	United States		19102	PCI-TWUS	false
175.182.19.68	unknown	Taiwan; Republic of China (ROC)		4780	SEEDNETDigitalUnitedIncTW	false
81.120.198.52	unknown	Italy		20959	TELECOM-ITALIA-DATA-COMIT	false
110.35.194.98	unknown	Korea Republic of		10175	HCNKUMHO-AS-KRKumhoCableKR	false
156.129.36.244	unknown	United States		29975	VODACOM-ZA	false
49.172.195.42	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
67.214.11.212	unknown	United States		7029	WINDSTREAMUS	false
174.166.95.198	unknown	United States		7922	COMCAST-7922US	false
187.24.104.209	unknown	Brazil		22085	ClaroSABR	false
156.18.88.93	unknown	France		1945	FR-LYRESLyonRechercheetEnseignementSuperieurLyRESE	false
207.110.5.219	unknown	United States		2828	XO-AS15US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
171.145.133.68	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
193.213.89.118	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
111.86.101.187	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
137.130.207.26	unknown	United States		668	DNIC-AS-00668US	false
120.148.134.107	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
199.210.134.183	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
152.116.213.254	unknown	United States		2018	TENET-1ZA	false
57.132.226.212	unknown	Belgium		2686	ATGS-MMD-ASUS	false
200.252.173.152	unknown	Brazil		4230	CLAROSABR	false
77.94.72.218	unknown	Italy		3302	AS-IRIDEOS-IN-NETAPPIT	false
69.2.210.81	unknown	United States		13649	ASN-VINSUS	false
165.151.151.130	unknown	United States		4193	WA-STATE-GOVUS	false
13.178.149.44	unknown	United States		7018	ATT-INTERNET4US	false
66.169.57.64	unknown	United States		20115	CHARTER-20115US	false
190.25.231.76	unknown	Colombia		19429	ETB-ColombiaCO	false
185.41.197.136	unknown	Russian Federation		62293	URALCHEM-ASRU	false
101.118.159.71	unknown	Australia		133612	VODAFONE-AS-APVodafoneAustraliaPtyLtdAU	false
196.28.205.125	unknown	South Africa		10474	OPTINETZA	false
179.131.171.229	unknown	Brazil		26599	TELEFONICABRASILSABR	false
52.78.77.106	unknown	United States		16509	AMAZON-02US	false
124.101.251.71	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
17.234.172.134	unknown	United States		714	APPLE-ENGINEERINGUS	false
192.64.216.108	unknown	United States		21719	CHLUS	false
102.141.251.90	unknown	South Africa		327962	PacketSkyZA	false
171.69.168.90	unknown	United States		109	CISCOSYSTEMSUS	false
72.112.23.193	unknown	United States		22394	CELLCOUS	false
151.23.37.146	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
181.159.27.113	unknown	Colombia		26611	COMCELSACO	false
175.10.90.22	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
102.197.90.230	unknown	unknown		36926	CKL1-ASNKE	false

Runtime Messages

Command:	/tmp/hWLlYv2MAX
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Yakuza Botnet
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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):	6.323596942049037
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	hWLlYv2MAX
File size:	63168
MD5:	dbbc5166ca67592d716184c23f486c00
SHA1:	26f84c2f48d9bd5b81e38320adfa97c01086f9a3
SHA256:	086d4bcb764c124e4201e24a6ccb387fd8888bd080a5f7278acbd4ddf94ca5a6
SHA512:	273d1aacfb118de6d1aebd1bb95c0f33638b8df6bc4cc6c06b60a9004d3ff3f393ae2590f7b4f0c22b491ea6e2dc7a509badf89a8600bec9efd0c5b8e81aaf41
SSDEEP:	768:2Peril+KxTYbr7JMvr75ghiDWLQLuj/SEcVW9+KY7GQAWD884VTJg:2PopuFgIWQSLSK9+K4G/g8fm
File Content Preview:	.ELF.....D...4...0.....4. ...(.....6...6..... .....<...<...<.....' ..... .dt.Q.....NV..a....da.....N^NuNV..J9....f>"y...T QJ.g.X.#....TN."y...T QJ.f.A....J.g.Hy...8N.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
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:	62768
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

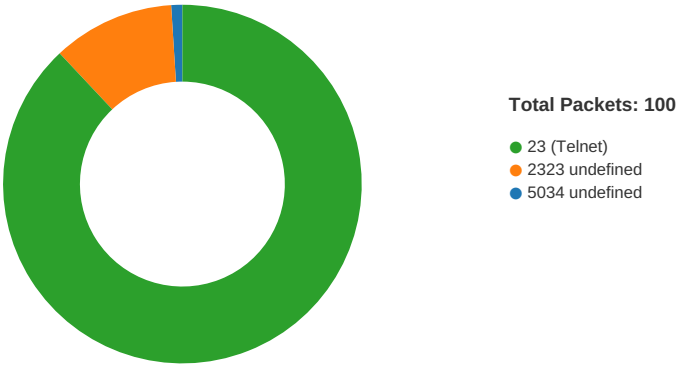
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0xe522	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000e5ca	0xe5ca	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000e5d8	0xe5d8	0xb5e	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x8001113c	0xf13c	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80011144	0xf144	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80011150	0xf150	0x3a0	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x800114f0	0xf4f0	0x236c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf4f0	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	0xf136	0xf136	4.1805	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0xf13c	0x8001113c	0x8001113c	0x3b4	0x2720	1.6888	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: hWLlYv2MAX PID: 5210 Parent PID: 5109

General

Start time:	13:58:31
Start date:	14/01/2022
Path:	/tmp/hWLlYv2MAX
Arguments:	/tmp/hWLlYv2MAX
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: hWLIYv2MAX PID: 5212 Parent PID: 5210

General

Start time:	13:58:31
Start date:	14/01/2022
Path:	/tmp/hWLIYv2MAX
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: hWLIYv2MAX PID: 5214 Parent PID: 5212

General

Start time:	13:58:31
Start date:	14/01/2022
Path:	/tmp/hWLIYv2MAX
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: hWLIYv2MAX PID: 5215 Parent PID: 5212

General

Start time:	13:58:31
Start date:	14/01/2022
Path:	/tmp/hWLIYv2MAX
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: hWLIYv2MAX PID: 5218 Parent PID: 5212

General

Start time:	13:58:31
Start date:	14/01/2022
Path:	/tmp/hWLIYv2MAX
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: dash PID: 5260 Parent PID: 4331

General

Start time:	13:59:55
Start date:	14/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5260 Parent PID: 4331

General

Start time:	13:59:55
Start date:	14/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.c898EgJy36 /tmp/tmp.k9ZN1wUC0G /tmp/tmp.JL9rmsZ4ya
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read