ID: 553490
Sample Name: 8p2APHSDxx
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 01:27:48
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report 8p2APHSDxx 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
System Summary: 4
Data Obfuscation: 4
Hooking and other Techniques for Hiding and Protection: 4
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 5
Malware Configuration 5
Behavior Graph 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
URLs from Memory and Binaries 6
Contacted IPs 7
Public 7
Runtime Messages 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 10
General 10
Static ELF Info 10
ELF header 10
Program Segments 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 11
System Behavior 11
Analysis Process: 8p2APHSDxx PID: 5219 Parent PID: 5120 11
General 11
File Activities 11
File Read 11
Analysis Process: 8p2APHSDxx PID: 5221 Parent PID: 5219 11
General 11
File Activities 11
File Read 11
Directory Enumerated 11
Analysis Process: 8p2APHSDxx PID: 5222 Parent PID: 5219 12
General 12
Analysis Process: 8p2APHSDxx PID: 5223 Parent PID: 5219 12
General 12
Analysis Process: 8p2APHSDxx PID: 5227 Parent PID: 5223 12
General 12
File Activities 12
File Read 12
Directory Enumerated 12
Analysis Process: 8p2APHSDxx PID: 5325 Parent PID: 5227 12
General 12
Analysis Process: 8p2APHSDxx PID: 5327 Parent PID: 5227 12
General 12
Analysis Process: 8p2APHSDxx PID: 5229 Parent PID: 5223 13
General 13
Analysis Process: 8p2APHSDxx PID: 5231 Parent PID: 5223 13
General 13

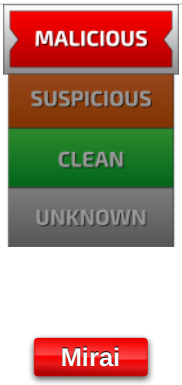
Linux Analysis Report 8p2APHSDxx

Overview

General Information

Sample Name:	8p2APHSDxx
Analysis ID:	553490
MD5:	adcb553ec94702..
SHA1:	b7c64b1604b684..
SHA256:	6631ba2378a01a..
Tags:	32 elf mips mirai
Infos:	

Detection

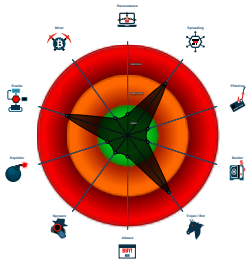


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample is packed with UPX
- Uses known network protocols on no...
- Sample tries to kill multiple processe...
- Sample contains only a LOAD segm...
- 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

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

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:	553490
Start date:	15.01.2022
Start time:	01:27:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8p2APHSDxx
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:	mal76.spre.troj.evad.lin@0/0@0/0
Warnings:	Show All

Process Tree

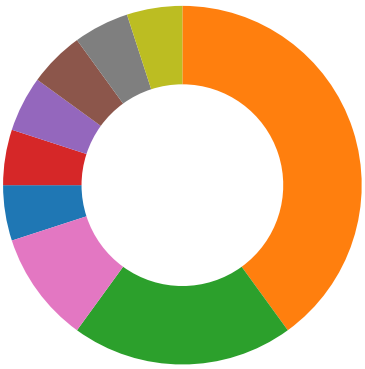
- **system is lnxubuntu20**
- 8p2APHSDxx (PID: 5219, Parent: 5120, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/8p2APHSDxx
  - 8p2APHSDxx New Fork (PID: 5221, Parent: 5219)
  - 8p2APHSDxx New Fork (PID: 5222, Parent: 5219)
  - 8p2APHSDxx New Fork (PID: 5223, Parent: 5219)
    - 8p2APHSDxx New Fork (PID: 5227, Parent: 5223)
      - 8p2APHSDxx New Fork (PID: 5325, Parent: 5227)
      - 8p2APHSDxx New Fork (PID: 5327, Parent: 5227)
    - 8p2APHSDxx New Fork (PID: 5229, Parent: 5223)
    - 8p2APHSDxx New Fork (PID: 5231, Parent: 5223)
- **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

System Summary:

Sample tries to kill multiple processes (SIGKILL)

Data Obfuscation:

Sample is packed with UPX

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

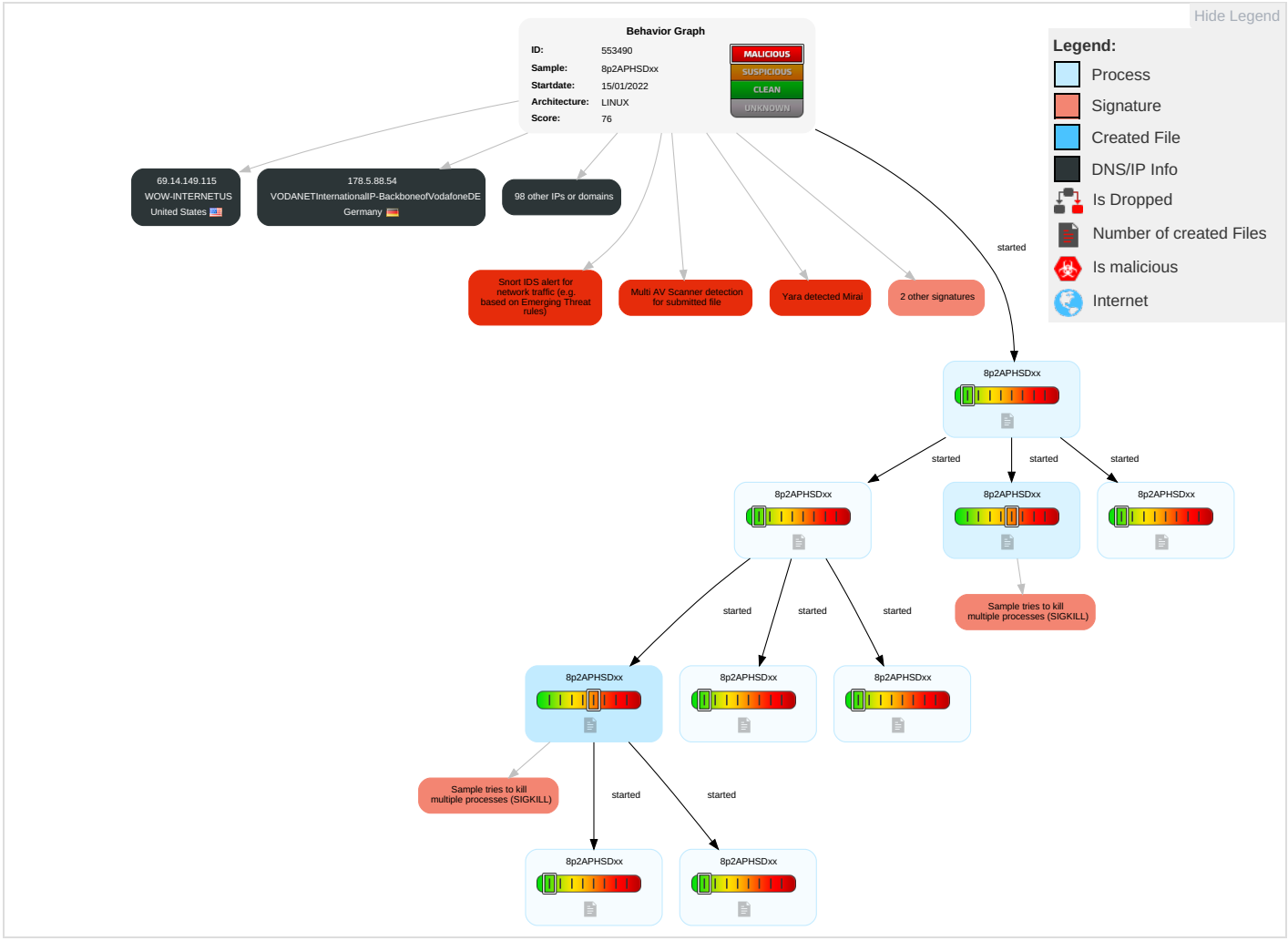
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated Files or Information 1	OS Credential Dumping 1	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	Mod Syst Parti
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	Devi Lock
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	Dele Devi Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
8p2APHSDxx	26%	Virustotal		Browse
8p2APHSDxx	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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.240.10.100	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
211.23.120.136	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
178.198.88.188	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
37.252.74.80	unknown	Armenia		44395	ORG-UL31-RIPEAM	false
217.220.244.241	unknown	Italy		8968	BT-ITALIAIT	false
212.143.94.167	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
82.47.250.59	unknown	United Kingdom		5089	NTLGB	false
31.219.188.58	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
249.63.217.224	unknown	Reserved		unknown	unknown	false
181.222.227.132	unknown	Brazil		28573	CLAROSABR	false
70.141.98.97	unknown	United States		7018	ATT-INTERNET4US	false
220.56.37.166	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
83.120.11.184	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
84.76.228.163	unknown	Spain		12479	UNI2-ASES	false
113.3.233.8	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
70.108.52.36	unknown	United States		701	UUNETUS	false
211.192.59.240	unknown	Korea Republic of		10056	HDMF-ASHyundaiMarinFireInsuranceKR	false
163.132.253.75	unknown	Japan		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
177.237.65.14	unknown	Mexico		28512	CablemasTelecomunicacionesSAdeCVMX	false
62.107.7.104	unknown	Denmark		197288	STOFANETDK	false
148.223.139.78	unknown	Mexico		8151	UninetSAdeCVMX	false
141.179.119.106	unknown	Saudi Arabia		197921	HBTFJO	false
201.159.85.21	unknown	Brazil		61764	RioGrandeTecnologiaeComunicMultimidiaLtdaBR	false
176.165.90.113	unknown	France		5410	BOUYGTEL-ISPFR	false
91.40.119.89	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
53.107.17.53	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
125.202.66.136	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
141.21.2.208	unknown	Germany		205046	FZI-AS-1DE	false
43.110.126.181	unknown	Japan		4249	LILLY-ASUS	false
84.252.55.41	unknown	Bulgaria		202043	BIA-BG	false
141.174.45.213	unknown	United States		29601	UPM-KYMMENE-ASKuusankoskiFinlandFI	false
154.79.94.130	unknown	Kenya		36926	CKL1-ASNKE	false
90.102.156.246	unknown	France		3215	FranceTelecom-OrangeFR	false
73.161.10.124	unknown	United States		7922	COMCAST-7922US	false
47.208.204.100	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
80.81.167.38	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
104.247.124.210	unknown	Reserved		63052	AS-CBBCCA	false
60.117.131.60	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
200.163.89.110	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
135.222.21.228	unknown	United States		10455	LUCENT-CIOUS	false
82.219.83.106	unknown	United Kingdom		30740	EXA-NETWORKSExaNetworksLimitedGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.111.187.52	unknown	Philippines		9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	false
161.135.98.184	unknown	United States		7726	FITC-ASUS	false
63.234.234.118	unknown	United States		12068	RC-ASNUS	false
92.204.156.190	unknown	Germany		398108	GO-DADDY-COM-LLCUS	false
74.240.110.136	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
76.253.229.96	unknown	United States		25993	AS-25993US	false
202.22.122.95	unknown	Japan		24183	DTS-ISP-CORE1-APDTSLTDNZ	false
1.255.125.250	unknown	Korea Republic of		9770	SPEEDONSTV-AS-KRLGHelloVisionCorpKR	false
173.33.198.208	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
89.146.240.36	unknown	Germany		8495	INTERNET_AGFrankfurt-Munich-Stuttgart-Amsterdam-LondonDE	false
37.234.77.118	unknown	Hungary		8448	PGSM-HUTorokbalintHungaryHU	false
69.14.149.115	unknown	United States		12083	WOW-INTERNETUS	false
113.10.164.169	unknown	Hong Kong		17444	NWT-AS-APASnumberforNewWorldTelephoneLtdHK	false
209.220.117.178	unknown	United States		701	UUNETUS	false
182.115.198.175	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
93.171.122.42	unknown	Czech Republic		42772	A1-BY-ASBY	false
2.67.68.255	unknown	Sweden		44034	HI3GSE	false
178.5.88.54	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
179.218.233.71	unknown	Brazil		28573	CLAROSABR	false
254.102.133.230	unknown	Reserved		unknown	unknown	false
85.246.144.11	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
161.104.78.249	unknown	France		7582	UMAC-AS-APUniversityofMacauMO	false
195.239.166.37	unknown	Russian Federation		3216	SOVAM-ASRU	false
150.23.109.183	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
189.22.73.157	unknown	Brazil		4230	CLAROSABR	false
152.201.10.86	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
43.2.122.58	unknown	Japan		4249	LILLY-ASUS	false
108.232.93.2	unknown	United States		7018	ATT-INTERNET4US	false
206.123.203.244	unknown	United States		398163	FIBERWESTUS	false
31.7.153.206	unknown	Italy		49360	POSIVITO-ASIT	false
177.254.188.54	unknown	Colombia		27831	ColombiaMovilCO	false
41.186.146.32	unknown	Rwanda		36890	MTNRW-ASNRW	false
171.57.213.144	unknown	India		9874	STARHUB-MOBILEStarHubLtdSG	false
16.175.78.233	unknown	United States		unknown	unknown	false
190.5.112.131	unknown	Honduras		27696	ColumbusNetworksdeHondurasSdeRLHN	false
217.193.146.101	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
93.129.239.86	unknown	Germany		6805	TDDE-ASN1DE	false
176.196.224.100	unknown	Russian Federation		39927	ELIGHT-ASRU	false
85.45.213.112	unknown	Italy		3269	ASN-IBSNAZIT	false
175.236.53.194	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
122.202.99.11	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	false
67.146.27.203	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
101.211.73.136	unknown	India		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
117.91.17.152	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
1.209.161.81	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
8.102.25.77	unknown	United States		3356	LEVEL3US	false
220.108.43.145	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
59.79.11.124	unknown	China		24364	CNGI-SH-IX-AS-APCERNET2IXatShanghaiJiaotongUniversity	false
14.239.224.160	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
250.255.172.193	unknown	Reserved		unknown	unknown	false
180.139.77.69	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
73.215.161.119	unknown	United States		7922	COMCAST-7922US	false
165.77.133.148	unknown	United States		4725	ODNSoftBankMobileCorpJP	false
130.0.91.47	unknown	Germany		61097	CLOUDSOFTCATGB	false
207.173.38.45	unknown	United States		7385	ALLSTREAMUS	false
83.141.103.223	unknown	Ireland		25441	IBIS-ASImagineGroupLtdIE	false
2.215.62.55	unknown	Germany		6805	TDDE-ASN1DE	false
93.130.166.68	unknown	Germany		6805	TDDE-ASN1DE	false
71.66.146.46	unknown	United States		10796	TWC-10796-MIDWESTUS	false

Runtime Messages

Command:	/tmp/8p2APHSDxx
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
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 LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.881439929683926
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	8p2APHSDxx
File size:	27260
MD5:	adcb553ec947029a484f9f4995ffbe0a
SHA1:	b7c64b1604b6847888619ae3b2af85faa9ffa741
SHA256:	6631ba2378a01aade3a4f46cae3b80a33bbf06bae53412e27c72d23f1fcc9397
SHA512:	70a49668a43a4fd03b6729c01766ce36b01e6ae2c5ce971844658497a339f767a6c400ca57398ba41363f44317ab96c90c8bede5a6752ea696c6870ab41b8a0f
SSDEEP:	384:dVH6HCf/Xf+tnc+GwfwMaMKjZD7anhIOtmXXMjrg26ichWMIBDcyqLh0RWGVCz0s:dt6gvMWB4eOwXQ/6iJ3BoJLhUWL
File Content Preview:	.ELF.....V..4.....4. ...(.....Ui..Ui.....p...p.E.p.E.....f.&nUPX!d.....T.....?.E.h;....#.....b.L#>c7}.'N.5.K..N..c.Q.4.6....t.....~3...Y|T\.....;.a7...xZ.\.\....R.....

Static ELF Info

ELF header

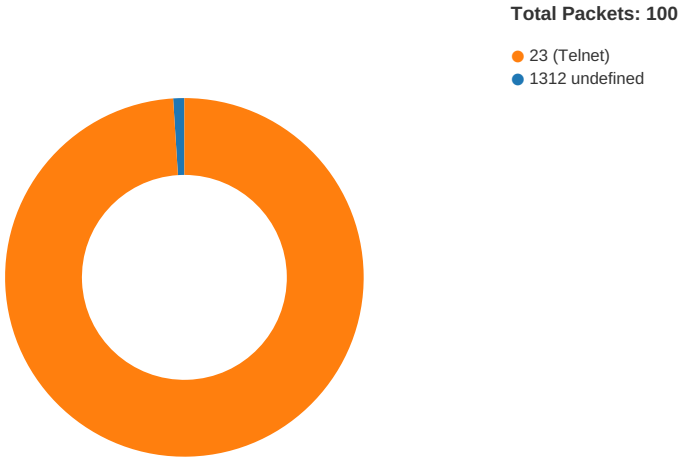
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x105618
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x6955	0x6955	4.1767	0x5	R E	0x10000		
LOAD	0x1870	0x451870	0x451870	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: 8p2APHSDxx PID: 5219 Parent PID: 5120

General

Start time:	01:28:30
Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	/tmp/8p2APHSDxx
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: 8p2APHSDxx PID: 5221 Parent PID: 5219

General

Start time:	01:28:30
Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: 8p2APHSDxx PID: 5222 Parent PID: 5219

General

Start time:	01:28:30
Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 8p2APHSDxx PID: 5223 Parent PID: 5219

General

Start time:	01:28:30
Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 8p2APHSDxx PID: 5227 Parent PID: 5223

General

Start time:	01:28:30
Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: 8p2APHSDxx PID: 5325 Parent PID: 5227

General

Start time:	01:31:36
Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 8p2APHSDxx PID: 5327 Parent PID: 5227

General

Start time:	01:31:36

Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 8p2APHSDxx PID: 5229 Parent PID: 5223

General

Start time:	01:28:30
Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 8p2APHSDxx PID: 5231 Parent PID: 5223

General

Start time:	01:28:30
Start date:	15/01/2022
Path:	/tmp/8p2APHSDxx
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9