ID: 507421
Sample Name: Rpl2Twyrts
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 08:36:22
Date: 22/10/2021
Version: 33.0.0 White Diamond

Table of Contents

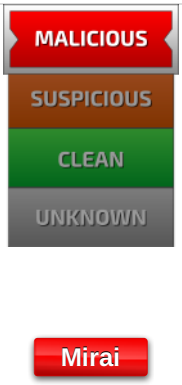
Linux Analysis Report Rpl2Twyrts

Overview

General Information

Sample Name:	Rpl2Twyrts
Analysis ID:	507421
MD5:	4635e3761f10a21.
SHA1:	a33d4b91fc25603.
SHA256:	91ccea41a26fce7..
Tags:	32 elf mips mirai
Infos:	

Detection

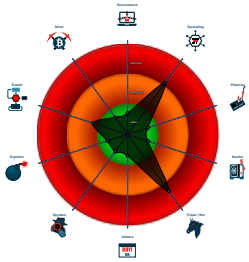


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample tries to kill many processes...
- 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 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:	33.0.0 White Diamond
Analysis ID:	507421
Start date:	22.10.2021
Start time:	08:36:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Rpl2Twyrts
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:	mal72.spre.troj.lin@0/2@0/0
Warnings:	Show All

Process Tree

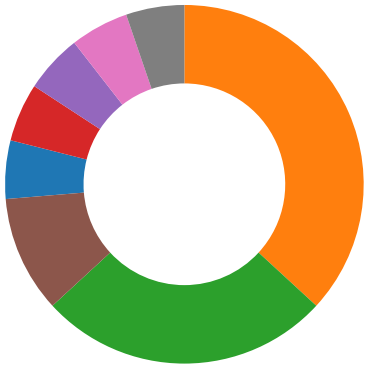
- **system is lnxubuntu20**
- Rpl2Twyrts (PID: 5246, Parent: 5121, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/Rpl2Twyrts
  - Rpl2Twyrts New Fork (PID: 5248, Parent: 5246)
  - Rpl2Twyrts New Fork (PID: 5249, Parent: 5246)
  - Rpl2Twyrts New Fork (PID: 5252, Parent: 5246)
    - Rpl2Twyrts New Fork (PID: 5254, Parent: 5252)
    - Rpl2Twyrts New Fork (PID: 5255, Parent: 5252)
    - Rpl2Twyrts New Fork (PID: 5257, Parent: 5252)
- systemd New Fork (PID: 5287, Parent: 1)
- sshd (PID: 5287, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5290, Parent: 1)
- sshd (PID: 5290, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

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 many 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

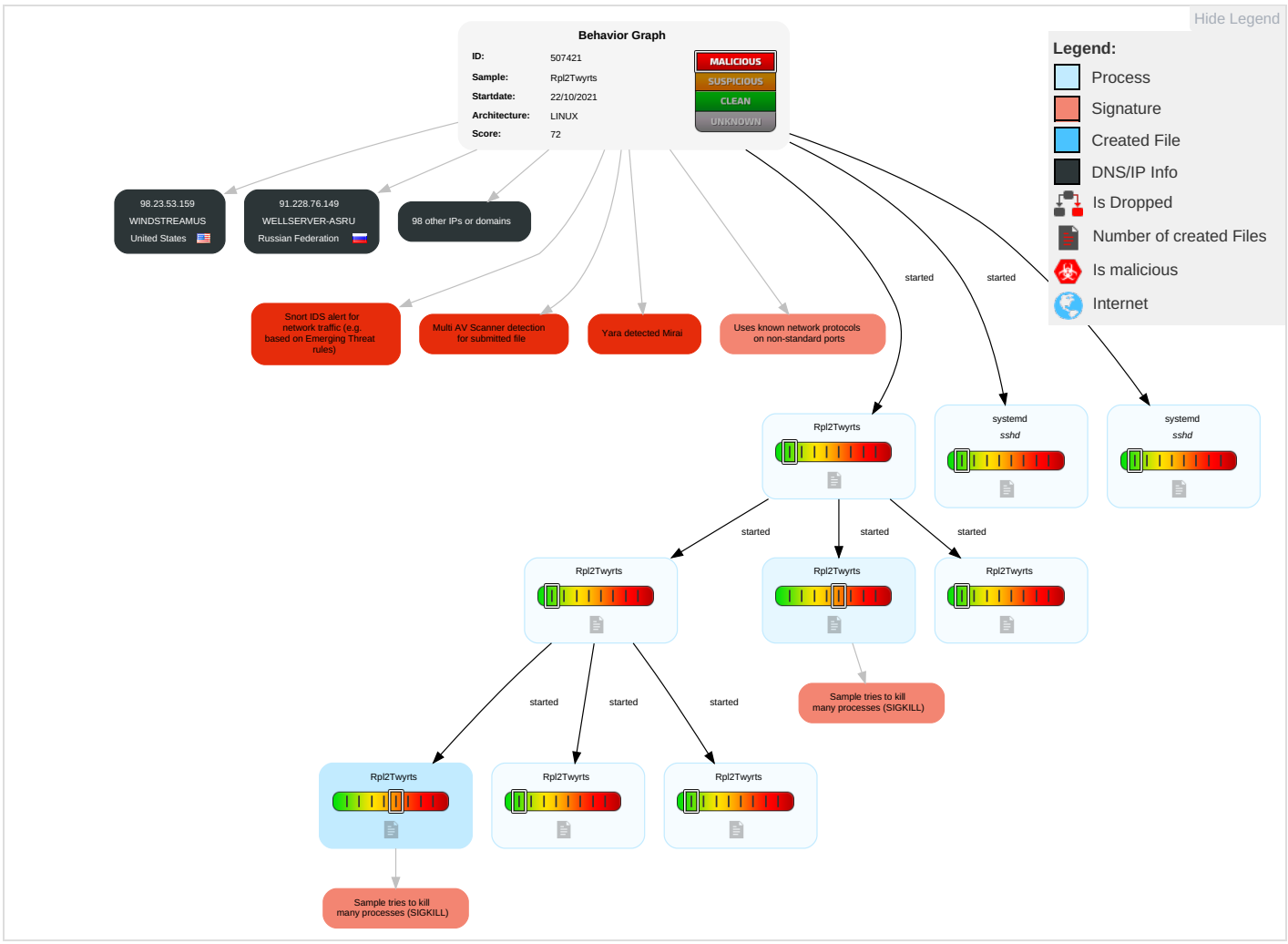
Mitre Att&ck Matrix

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	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	Modify System Partitio
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 Lockou
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
Rpl2Twyrts	50%	Virustotal		Browse
Rpl2Twyrts	53%	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
39.203.104.226	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
190.89.152.5	unknown	unknown		270374	KINGTELECOMUNICACOESBR	false
160.248.184.59	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
86.237.87.136	unknown	France		3215	FranceTelecom-OrangeFR	false
159.178.169.160	unknown	United States		6356	NERDCNETUS	false
198.117.113.163	unknown	United States		297	AS297US	false
170.131.168.48	unknown	United States		13954	STAPLESUS	false
77.152.117.114	unknown	France		15557	LDCOMNETFR	false
187.196.136.136	unknown	Mexico		8151	UninetSAdeCVMX	false
183.206.48.83	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
155.93.197.94	unknown	South Africa		37680	COOL-IDEASZA	false
118.155.201.133	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
65.37.101.238	unknown	United States		5650	FRONTIER-FRTRUS	false
42.21.33.100	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
45.226.163.131	unknown	Brazil		267045	EASYCONNECTTECNOLOGIAJACILTDABR	false
153.233.14.113	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
98.23.53.159	unknown	United States		7029	WINDSTREAMUS	false
64.253.255.224	unknown	United States		20428	GLOWPOINT-ASUS	false
160.199.79.178	unknown	Japan		7679	QTNETQTnetIncJP	false
93.249.80.159	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
74.217.215.131	unknown	United States		12182	INTERNAP-2BLKUS	false
88.74.255.198	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
58.21.123.207	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
70.63.62.155	unknown	United States		10796	TWC-10796-MIDWESTUS	false
200.138.172.31	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
161.249.2.143	unknown	United States		396269	BPL-ASNUS	false
158.34.189.234	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
84.38.119.247	unknown	Austria		43939	INTERNETIA_ETTH2-ASNoc-BialystokPL	false
8.156.46.207	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
211.11.169.244	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
12.121.131.53	unknown	United States		7018	ATT-INTERNET4US	false
179.73.32.17	unknown	Brazil		26615	TIMSABR	false
75.203.112.61	unknown	United States		22394	CELLCOUS	false
82.174.187.190	unknown	Netherlands		13127	VERSATELASfortheTrans-EuropeanTele2IPTransportbackbo	false
186.57.123.203	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
115.136.104.95	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
110.144.98.170	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
105.118.219.175	unknown	Nigeria		36873	VNL1-ASNG	false
19.180.211.252	unknown	United States		3	MIT-GATEWAYSUS	false
100.15.26.7	unknown	United States		701	UUNETUS	false
158.47.217.111	unknown	Italy		12551	AS-ENEL-IT	false
251.36.138.169	unknown	Reserved		unknown	unknown	false
84.50.15.196	unknown	Estonia		3249	ESTPAKEE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
251.246.87.35	unknown	Reserved		unknown	unknown	false
80.194.99.5	unknown	United Kingdom		5089	NTLGB	false
162.195.248.48	unknown	United States		7018	ATT-INTERNET4US	false
190.40.159.241	unknown	Peru		6147	TelefonicadelPeruSAAPE	false
31.18.171.187	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
87.204.237.150	unknown	Poland		12741	AS-NETIAWarszawa02-822PL	false
27.12.141.82	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
58.250.84.179	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
149.212.83.51	unknown	Denmark		8386	KOCNETTR	false
37.52.64.35	unknown	Ukraine		6849	UKRTELNETUA	false
191.96.28.113	unknown	Chile		61317	ASDETUKhttpwwwheficedcomGB	false
104.186.4.233	unknown	United States		7018	ATT-INTERNET4US	false
124.181.3.104	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
242.153.131.112	unknown	Reserved		unknown	unknown	false
198.101.133.16	unknown	United States		19994	RACKSPACEUS	false
125.113.41.119	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
112.99.82.219	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
103.146.47.155	unknown	unknown		139848	SHIPL-AS-APSAFEGUARDHOMEIMPROVEMENTSPTYLTDAU	false
182.26.120.99	unknown	Indonesia		4795	INDOSATM2-IDINDOSATM2ASNID	false
120.21.19.134	unknown	Australia		133612	VODAFONE-AS-APVodafoneAustraliaPtyLtdAU	false
90.78.51.144	unknown	France		3215	FranceTelecom-OrangeFR	false
108.22.114.219	unknown	United States		701	UUNETUS	false
42.222.34.226	unknown	China		4249	LILLY-ASUS	false
19.146.221.131	unknown	United States		3	MIT-GATEWAYSUS	false
170.244.191.219	unknown	Argentina		265630	COMISSODANTEANIBALAR	false
187.111.50.119	unknown	Brazil		262711	TURBOMAXTELECOMUNICACOESLTDABR	false
70.196.121.123	unknown	United States		6167	CELLCO-PARTUS	false
247.151.111.14	unknown	Reserved		unknown	unknown	false
37.11.20.196	unknown	Spain		12479	UNI2-ASES	false
209.146.99.63	unknown	United States		395753	KKRUS	false
87.48.91.173	unknown	Denmark		3292	TDCTDCASDK	false
91.228.76.149	unknown	Russian Federation		56864	WELLSERVER-ASRU	false
146.93.13.52	unknown	United States		18709	BOTWUS	false
71.219.170.252	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
23.235.61.72	unknown	United States		64252	ATSIUS	false
141.216.159.236	unknown	United States		394769	UMF-7-ASUS	false
111.146.116.201	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
192.232.122.104	unknown	United States		5647	ASN-KODAKUS	false
95.36.120.123	unknown	Netherlands		15670	BBNED-AS1NL	false
103.187.81.173	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
97.223.137.109	unknown	United States		6167	CELLCO-PARTUS	false
133.167.242.237	unknown	Japan		9371	SAKURA-CSAKURAInternetIncJP	false
95.183.142.160	unknown	Turkey		8517	ULAKNETTR	false
159.28.99.182	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
241.198.25.193	unknown	Reserved		unknown	unknown	false
251.102.148.138	unknown	Reserved		unknown	unknown	false
83.106.59.198	unknown	United Kingdom		2529	DEMON-INTERNETNowmaintainedbyCableWirelessWorldwide	false
138.244.67.215	unknown	Germany		12816	MWN-ASDE	false
43.88.162.92	unknown	Japan		4249	LILLY-ASUS	false
162.30.154.204	unknown	United States		46483	RGHSUS	false
90.95.34.132	unknown	France		8953	ASN-ORANGE-ROMANIARO	false
82.47.8.178	unknown	United Kingdom		5089	NTLGB	false
43.99.42.139	unknown	Japan		4249	LILLY-ASUS	false
180.87.26.156	unknown	India		6453	AS6453US	false
115.163.218.70	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
244.243.93.7	unknown	Reserved		unknown	unknown	false
19.30.92.146	unknown	United States		3	MIT-GATEWAYSUS	false

Runtime Messages

Command:	/tmp/Rpl2Twyrts
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
70.63.62.155	raCyB7pYpd	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	zYMp3detVO	Get hash	malicious	Browse	• 182.10.78.173
	ggtS1fKIqX	Get hash	malicious	Browse	• 39.208.68.184
	oH6qNmnFRP	Get hash	malicious	Browse	• 182.8.245.170
	b3astmode.arm7	Get hash	malicious	Browse	• 39.205.24.41
	PFD33mzc5l	Get hash	malicious	Browse	• 39.210.152.58
	hNsTaM2BAu	Get hash	malicious	Browse	• 39.211.166.212
	x86	Get hash	malicious	Browse	• 39.210.152.36
	8jfOcvTqQA	Get hash	malicious	Browse	• 182.9.38.56
	jQCJldg3pv	Get hash	malicious	Browse	• 39.198.157.101
	jMJ8Uz4Mhk	Get hash	malicious	Browse	• 39.216.238.64
	ATc5uxXITp	Get hash	malicious	Browse	• 39.239.5.147
	IN7REq0Jv5	Get hash	malicious	Browse	• 182.3.113.176
	pandora.x86	Get hash	malicious	Browse	• 39.221.131.173
	pandora.arm	Get hash	malicious	Browse	• 182.2.171.171
	KEgx4lC3Ni	Get hash	malicious	Browse	• 39.221.113.150
	Qfx7rFWkI5	Get hash	malicious	Browse	• 39.232.121.185
	OcO4KUSfwn	Get hash	malicious	Browse	• 39.195.240.250

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DGTm0edlSX	Get hash	malicious	Browse	• 39.237.138.116
	1WL2kQmrNk	Get hash	malicious	Browse	• 182.12.155.124
	1Mwzgsrx9C	Get hash	malicious	Browse	• 114.126.201.55

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5290/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	-1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Ckvn:Cm
MD5:	3FD0BF07C83F464293873F94C4FEBF64
SHA1:	A10B2D66A4BA43FC3B81098BD761343051789CC0
SHA-256:	CD46DE89F7C34FEBE64A548F2A948CC6B9E8AF9724A496B28331DBE09769F79E
SHA-512:	A5E78FBF75B7232D1F0F65FA9D791953E29152D2C7C520CCCC1536337216754CB9C6C8BB6B66C6BE14B81C1CF33126E94EE015BC721EB77C0F5A120E2AF99DA
Malicious:	false
Reputation:	low
Preview:	5290.

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.425468889262933
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Rpl2Twyrts
File size:	71764
MD5:	4635e3761f10a21d01fec0df9fa36e2f

General

SHA1:	a33d4b91fc25603b0ed98b17381f6a6e017f6c32
SHA256:	91ccea41a26fce7feab89f9b17c889b9f7c37f29b5b5a9390a7d3f2990f43cfa
SHA512:	96722d00ad0e84259b5a93ee5a1226af820855fe20889a2782b5fad7dae45555def4877628f610e8ab375ea9581ac7d84b1cb37de7d25808063ee131f05ab0a5
SSDEEP:	768:YU6bhcgHSIJWB+cHlfD2wLX3YEwja6PN1oAg5oRKxeU3hVpxedxAxePx28szI2Zx:YU6bh1HkV2wEVjZPzgj1GCK2dFsTcJ
File Content Preview:	.ELF.....`.@.4...L.....4. ...(.....@...@.....E...E.....Q.td.....<...'!.....'.....<...'!... .....9'.. .....<...'!.....9

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:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	71244
Section Header Size:	40
Number of Section Headers:	13
Header String Table Index:	12

Sections

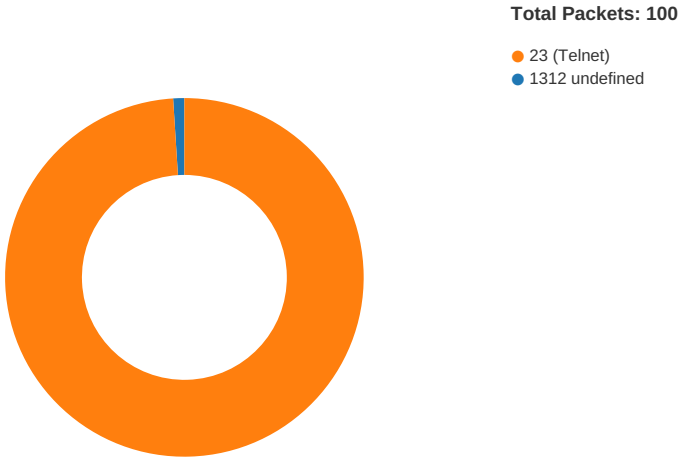
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x10710	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x410830	0x10830	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x410890	0x10890	0x660	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x451000	0x11000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x451008	0x11008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x451020	0x11020	0x190	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4511b0	0x111b0	0x444	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x4515f4	0x115f4	0x24	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x451620	0x115f4	0x2a0	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x72c	0x115f4	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x115f4	0x57	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	0x400000	0x400000	0x10ef0	0x10ef0	3.3609	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x11000	0x451000	0x451000	0x5f4	0x8c0	1.7941	0x6	RW	0x10000		.ctors .dtors .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: Rpl2Twyrts PID: 5246 Parent PID: 5121

General

Start time:	08:37:07
Start date:	22/10/2021
Path:	/tmp/Rpl2Twyrts
Arguments:	/tmp/Rpl2Twyrts
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: Rpl2Twyrts PID: 5248 Parent PID: 5246

General

Start time:	08:37:07
Start date:	22/10/2021
Path:	/tmp/Rpl2Twyrts
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: Rpl2Twyrts PID: 5249 Parent PID: 5246

General

Start time:	08:37:07
Start date:	22/10/2021
Path:	/tmp/Rpl2Twyrts
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: Rpl2Twyrts PID: 5252 Parent PID: 5246

General

Start time:	08:37:07
Start date:	22/10/2021
Path:	/tmp/Rpl2Twyrts
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: Rpl2Twyrts PID: 5254 Parent PID: 5252

General

Start time:	08:37:08
Start date:	22/10/2021
Path:	/tmp/Rpl2Twyrts
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: Rpl2Twyrts PID: 5255 Parent PID: 5252

General

Start time:	08:37:08
Start date:	22/10/2021
Path:	/tmp/Rpl2Twyrts
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: Rpl2Twyrts PID: 5257 Parent PID: 5252

General

Start time:	08:37:08

Start date:	22/10/2021
Path:	/tmp/Rpl2Twyrts
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: systemd PID: 5287 Parent PID: 1

General

Start time:	08:37:21
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5287 Parent PID: 1

General

Start time:	08:37:21
Start date:	22/10/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5290 Parent PID: 1

General

Start time:	08:37:21
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5290 Parent PID: 1

General

Start time:	08:37:21
Start date:	22/10/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated