ID: 1564805
Sample Name: sora.sh4.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 19:57:10
Date: 28/11/2024
Version: 41.0.0 Charoite

Table of Contents

Linux Analysis Report

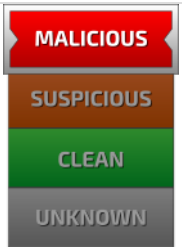
sora.sh4.elf

Overview

General Information

Sample name:	sora.sh4.elf
Analysis ID:	1564805
MD5:	ddd7c47a4422…
SHA1:	4a4d85fe96503..
SHA256:	591d03ac5bad…
Tags:	elf Mirai user-abuse_ch
Infos:	

Detection



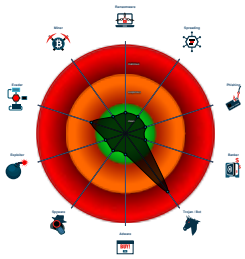
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Yara detected Mirai
- Detected TCP or UDP traffic on non…
- Enumerates processes within the "p…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Yara signature match

Classification



General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1564805
Start date and time:	2024-11-28 19:57:10 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 24s
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:	sora.sh4.elf
Detection:	MAL
Classification:	mal80.troj.linELF@0/0@2/0

Warnings

Runtime Messages

Command:	/tmp/sora.sh4.elf
PID:	5534
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**

- sora.sh4.elf (PID: 5534, Parent: 5452, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/sora.sh4.elf
  - sora.sh4.elf New Fork (PID: 5537, Parent: 5534)
  - sora.sh4.elf New Fork (PID: 5539, Parent: 5534)
  - sora.sh4.elf New Fork (PID: 5540, Parent: 5534)
    - sora.sh4.elf New Fork (PID: 5543, Parent: 5540)
    - sora.sh4.elf New Fork (PID: 5544, Parent: 5540)
    - sora.sh4.elf New Fork (PID: 5546, Parent: 5540)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	http://osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	http://https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
sora.sh4.elf	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
sora.sh4.elf	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
sora.sh4.elf	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0xe4e4:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A

Memory Dumps

Source	Rule	Description	Author	Strings
5539.1.00007f952c37f000.00007f952c38f000.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
5539.1.00007f952c37f000.00007f952c38f000.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5539.1.00007f952c37f000.00007f952c38f000.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0xe4e4:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
5534.1.00007f952c37f000.00007f952c38f000.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
5534.1.00007f952c37f000.00007f952c38f000.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	

Click to see the 5 entries

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

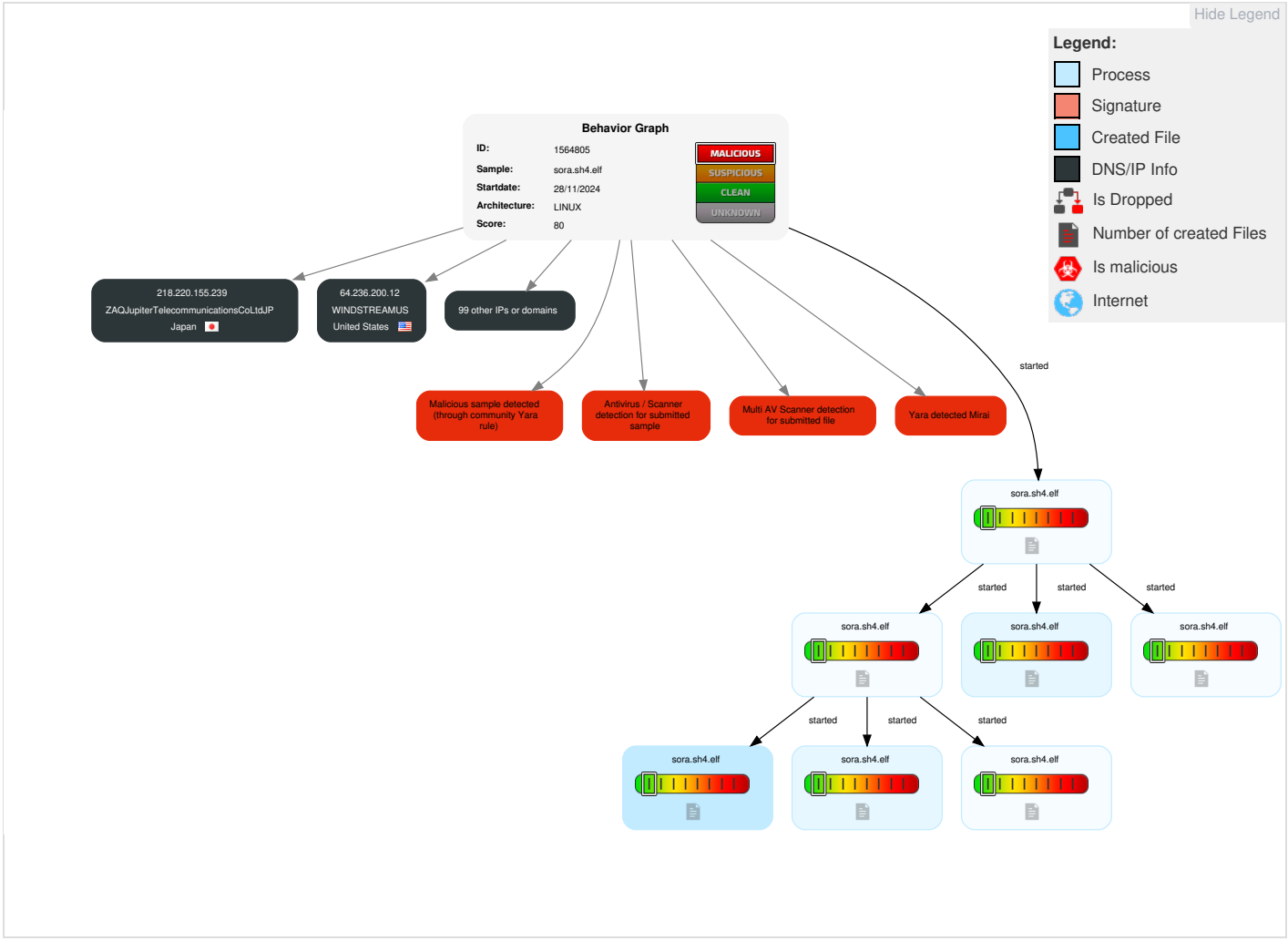
Mitre Att&ck Matrix

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	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 Non-Standard Port	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-Application Layer Protocol	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
sora.sh4.elf	71%	ReversingLabs	Linux.Trojan.Mirai	
sora.sh4.elf	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

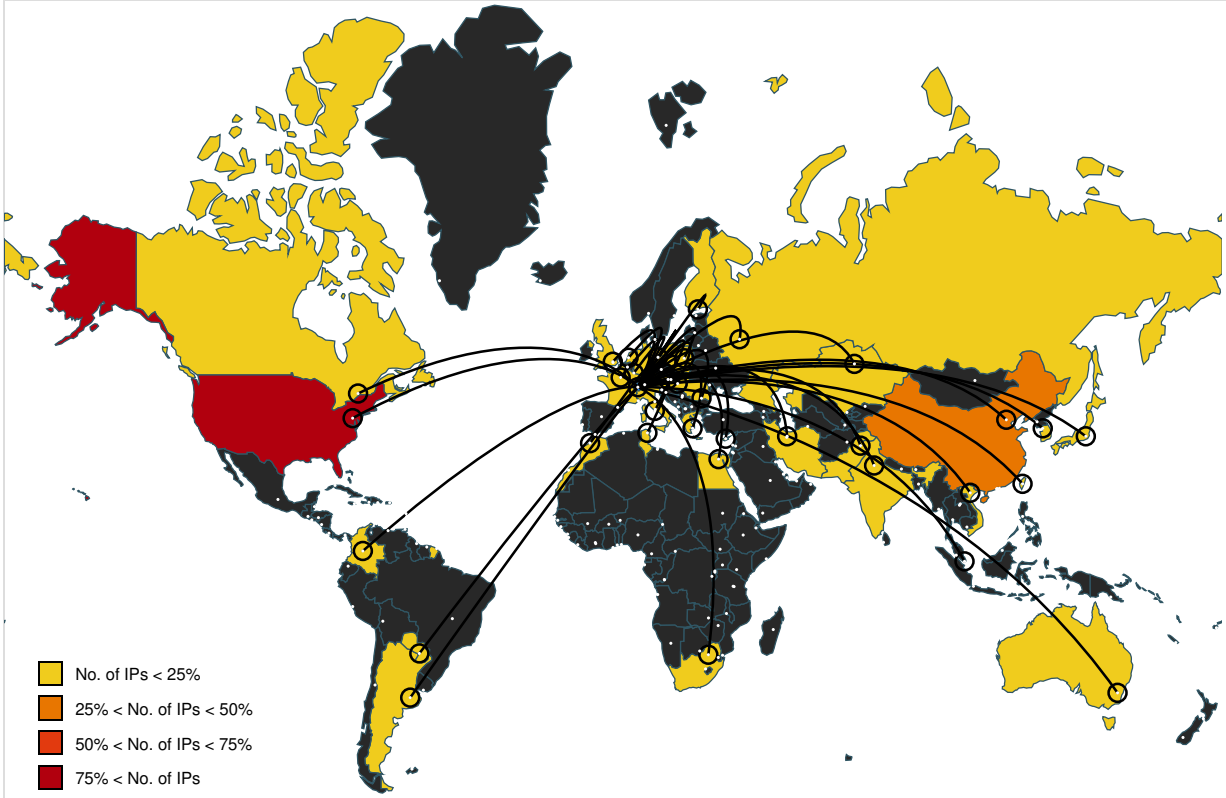
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	162.213.35.24	true	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
58.202.177.142	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
159.64.241.190	unknown	United States		32982	DOE-HQUS	false
212.52.175.99	unknown	Hungary		28924	INTEGRITY-HU-ASHU	false
63.39.143.10	unknown	United States		3356	LEVEL3US	false
249.14.196.103	unknown	Reserved		unknown	unknown	false
42.192.16.243	unknown	China		4249	LILLY-ASUS	false
5.12.90.139	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
98.232.70.184	unknown	United States		7922	COMCAST-7922US	false
105.140.212.239	unknown	Morocco		6713	IAM-ASMA	false
192.207.58.154	unknown	United States		32082	BSC-20041102US	false
31.185.231.183	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
146.220.114.141	unknown	Luxembourg		204590	SWISS-ASCH	false
80.107.96.109	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
110.39.166.129	unknown	Pakistan		38264	WATEEN-IMS-PK-AS-APNationalWiMAXIMSenvironmentPK	false
218.220.155.239	unknown	Japan		9617	ZAQJupiterTelecommunicationsCoLtdJP	false
102.222.82.226	unknown	unknown		36926	CKL1-ASNKE	false
150.1.78.94	unknown	Japan		6400	CompaniaDominicanadeTelefonosSADO	false
67.58.124.128	unknown	United States		14615	ROCK-HILL-TELEPHONEUS	false
88.134.156.126	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
79.218.100.138	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
85.128.200.52	unknown	Poland		15967	NAZWAPL	false
190.23.45.125	unknown	Paraguay		27866	COPACOPY	false
91.130.14.11	unknown	Austria		1257	TELE2EU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
164.0.143.52	unknown	Kazakhstan		29355	KCELL-ASKZ	false
223.216.154.47	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
145.31.212.219	unknown	Netherlands		42894	MINVENW-RWSMinVenW-RijkswaterstaatBackboneNL	false
4.254.167.35	unknown	United States		3356	LEVEL3US	false
84.143.2.211	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
168.75.155.164	unknown	United States		14135	NAVISITE-EAST-2US	false
197.12.199.97	unknown	Tunisia		37703	ATLAXTN	false
141.44.15.196	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
149.106.157.56	unknown	United States		19999	UNIONASNUS	false
35.219.213.175	unknown	United States		19527	GOOGLE-2US	false
117.255.236.149	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
142.64.238.6	unknown	Canada		5769	VIDEOTRONCA	false
206.222.200.40	unknown	United States		15108	ALLO-COMMUS	false
145.242.154.40	unknown	France		1101	IP-EEND-ASIP-EENDBVNL	false
68.250.134.115	unknown	United States		7018	ATT-INTERNET4US	false
116.162.104.215	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
58.170.22.167	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
241.50.76.188	unknown	Reserved		unknown	unknown	false
172.57.85.118	unknown	United States		21928	T-MOBILE-AS21928US	false
165.237.183.16	unknown	United States		3456	TWC-3456-ITUS	false
251.234.67.51	unknown	Reserved		unknown	unknown	false
243.126.76.164	unknown	Reserved		unknown	unknown	false
35.184.93.84	unknown	United States		15169	GOOGLEUS	false
175.227.77.64	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
91.174.79.10	unknown	France		12322	PROXADFR	false
100.17.25.113	unknown	United States		701	UUNETUS	false
101.14.115.233	unknown	Taiwan; Republic of China (ROC)		24158	TAIWANMOBILE-ASTaiwanMobileCoLtdTW	false
76.241.14.39	unknown	United States		7018	ATT-INTERNET4US	false
118.144.228.44	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
2.187.183.239	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
203.117.119.34	unknown	Singapore		4657	STARHUB-INTERNETStarHubLtdSG	false
104.44.147.151	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
19.167.223.34	unknown	United States		3	MIT-GATEWAYSUS	false
66.29.186.182	unknown	United States		32808	UTAHBROADBAND-AS1US	false
14.4.246.118	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
151.109.8.118	unknown	United States		1218	NCUBE-BELMONT-ASUS	false
220.162.96.250	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
17.111.180.131	unknown	United States		714	APPLE-ENGINEERINGUS	false
218.9.165.51	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
77.92.31.121	unknown	Cyprus		43356	COMTECH-ASTR	false
77.47.59.205	unknown	Germany		35244	KMS-DE_ASDE	false
44.168.122.170	unknown	United States		20473	AS-CHOOPAUS	false
250.136.198.230	unknown	Reserved		unknown	unknown	false
200.9.212.10	unknown	Argentina		263249	MasterBaseSACL	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
171.234.17.145	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
220.182.67.5	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
146.227.250.160	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
148.200.235.46	unknown	Netherlands		33915	TNF-ASNL	false
158.205.145.129	unknown	Japan		4694	IDCFIDCFrontierIncJP	false
46.84.168.31	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
169.192.200.41	unknown	United States		37611	AfrihostZA	false
46.132.103.37	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
249.162.127.113	unknown	Reserved		unknown	unknown	false
43.160.156.32	unknown	Japan		4249	LILLY-ASUS	false
196.74.72.240	unknown	Morocco		36903	MT-MPLSMA	false
206.50.62.34	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
63.90.62.225	unknown	United States		701	UUNETUS	false
76.50.164.153	unknown	United States		18494	CENTURYLINK-LEGACY-EMBARQ-WRBGUS	false
181.157.10.239	unknown	Colombia		26611	COMCELSACO	false
9.108.199.206	unknown	United States		3356	LEVEL3US	false
123.217.96.216	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
45.62.135.63	unknown	United States		31882	ABS-AS1US	false
145.202.2.222	unknown	Netherlands		1101	IP-EEND-ASIP-EENDBVNL	false
119.2.4.202	unknown	China		23724	CHINANET-IDC-BJ-APIDCChinaTelecommunicationsCorporation	false
141.224.226.177	unknown	United States		18454	AUGSBURGUS	false
186.85.150.225	unknown	Colombia		10620	TelmexColombiaSACO	false
154.114.47.243	unknown	South Africa		2018	TENET-1ZA	false
36.144.68.134	unknown	China		56044	CMNET-AS-LIAONINGChinaMobilecommunicationscorporationC	false
111.36.229.194	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	false
93.48.179.248	unknown	Italy		12874	FASTWEBIT	false
91.229.112.4	unknown	Russian Federation		56957	IX-2-ASRU	false
203.23.142.162	unknown	Australia		9749	GPKNET-AS-AUGPKComputersPtyLtdInternetServiceProvide	false
173.164.129.216	unknown	United States		7922	COMCAST-7922US	false
154.136.21.106	unknown	Egypt		37069	MOBINILEG	false
128.12.130.141	unknown	United States		32	STANFORDUS	false
64.236.200.12	unknown	United States		7029	WINDSTREAMUS	false
70.57.201.106	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	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 LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.785090824309155
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	sora.sh4.elf
File size:	63'772 bytes
MD5:	ddd7c47a4422d6bd5d4e8c0f7b5176c2
SHA1:	4a4d85fe96503e2471ef85dde9ede9fa1b7936d9
SHA256:	591d03ac5bade653f673e1aaaea02bf4bbdce88734618db775251d53c6e2272f
SHA512:	0c1d639f69b008eafd2625ed818db7dcb6ce341331ae1188821bef4c36a034aa42a7449c17951a9d8c5d6edf68bff88326c9c188d533cf056e6dbacdb03f85ab
SSDEEP:	1536:PaAtVnz1/mUUNztiYmW6ihiYLTofs3wfpWIDNEJ7JC7:P/tVz1eUUfwN0T0f+whWONEJ7J
TLSH:	41539FA5C5ACAE58C71441B8B654CD398723F408A5A76EFBD646C796800BEFCF0187F2
File Content Preview:	.ELF.....*.....@.4.....4. ...(.....@...@.$...$.....(...(.A. (.A.$.....Q.td....././"O.n.....#.*@.....#.*@.....o&O.n...l....././.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	63372
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

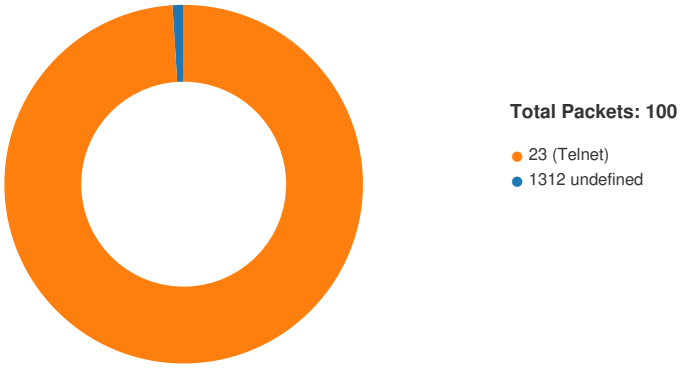
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xe3e0	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40e4c0	0xe4c0	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40e4e4	0xe4e4	0x1040	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41f528	0xf528	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41f530	0xf530	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41f53c	0xf53c	0x210	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x41f74c	0xf74c	0x280	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf74c	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	0x400000	0x400000	0xf524	0xf524	6.8204	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xf528	0x41f528	0x41f528	0x224	0x4a4	2.9997	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 28, 2024 20:00:54.252039909 CET	192.168.2.14	8.8.8.8	0xc987	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)	false
Nov 28, 2024 20:00:54.252087116 CET	192.168.2.14	8.8.8.8	0x4ebd	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2024 20:00:55.337229013 CET	8.8.8.8	192.168.2.14	0xc987	No error (0)	daisy.ubuntu.com		162.213.35.24	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2024 20:00:55.337229013 CET	8.8.8.8	192.168.2.14	0xc987	No error (0)	daisy.ubuntu.com		162.213.35.25	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: sora.sh4.elf PID: 5534, Parent PID: 5452

General

Start time (UTC):	18:58:06
Start date (UTC):	28/11/2024
Path:	/tmp/sora.sh4.elf
Arguments:	/tmp/sora.sh4.elf
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: sora.sh4.elf PID: 5537, Parent PID: 5534

General

Start time (UTC):	18:58:07
Start date (UTC):	28/11/2024
Path:	/tmp/sora.sh4.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: sora.sh4.elf PID: 5539, Parent PID: 5534

General

Start time (UTC):	18:58:07
Start date (UTC):	28/11/2024
Path:	/tmp/sora.sh4.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: sora.sh4.elf PID: 5540, Parent PID: 5534

General

Start time (UTC):	18:58:07
Start date (UTC):	28/11/2024
Path:	/tmp/sora.sh4.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: sora.sh4.elf PID: 5543, Parent PID: 5540

General

Start time (UTC):	18:58:07
Start date (UTC):	28/11/2024
Path:	/tmp/sora.sh4.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: sora.sh4.elf PID: **5544**, Parent PID: **5540**

General

Start time (UTC):	18:58:07
Start date (UTC):	28/11/2024
Path:	/tmp/sora.sh4.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: sora.sh4.elf PID: **5546**, Parent PID: **5540**

General

Start time (UTC):	18:58:07
Start date (UTC):	28/11/2024
Path:	/tmp/sora.sh4.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9