ID: 831207
Sample Name: sora.x86.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:35:09
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

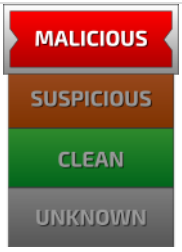
sora.x86.elf

Overview

General Information

Sample Name:	sora.x86.elf
Analysis ID:	831207
MD5:	ed1472168cde…
SHA1:	647657a97916…
SHA256:	17492e1447ec…
Tags:	elf mirai
Infos:	

Detection



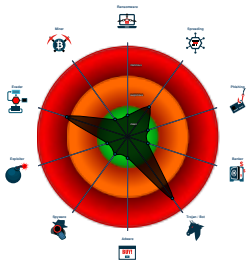
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample contains only a LOAD segm…
- Yara signature match
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831207
Start date and time:	2023-03-21 09:35:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
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 file name:	sora.x86.elf
Detection:	MAL
Classification:	mal80.troj.evad.linELF@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/sora.x86.elf
PID:	6222
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- sora.x86.elf (PID: 6222, Parent: 6124, MD5: ed1472168cdeb8c93dd3f03c3c8fdba8) Arguments: /tmp/sora.x86.elf
  - sora.x86.elf New Fork (PID: 6224, Parent: 6222)
    - sora.x86.elf New Fork (PID: 6317, Parent: 6224)
    - sora.x86.elf New Fork (PID: 6319, Parent: 6224)
      - sora.x86.elf New Fork (PID: 6320, Parent: 6319)
        - sora.x86.elf New Fork (PID: 6326, Parent: 6320)
        - sora.x86.elf New Fork (PID: 6327, Parent: 6320)
      - sora.x86.elf New Fork (PID: 6321, Parent: 6319)
      - sora.x86.elf New Fork (PID: 6322, Parent: 6319)
  - sora.x86.elf New Fork (PID: 6225, Parent: 6222)
  - sora.x86.elf New Fork (PID: 6226, Parent: 6222)
    - sora.x86.elf New Fork (PID: 6227, Parent: 6226)
      - sora.x86.elf New Fork (PID: 6316, Parent: 6227)
      - sora.x86.elf New Fork (PID: 6318, Parent: 6227)
    - sora.x86.elf New Fork (PID: 6228, Parent: 6226)
    - sora.x86.elf New Fork (PID: 6229, Parent: 6226)
- **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

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
6316.1.0000000008048000.0000000008057000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6316.1.0000000008048000.0000000008057000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xd2a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd2b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd2c8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd2dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd2f0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd304:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd318:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd32c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd340:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd354:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd368:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd37c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd390:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3cc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3f4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd408:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd41c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd430:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6316.1.0000000008048000.0000000008057000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xd7f8:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64
6316.1.0000000008048000.0000000008057000.r-x.sdmp	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	• 0x5710:$a: 53 31 DB 8B 4C 24 0C 8B 54 24 08 83 F9 01 76 15 66 8B 02 83 E9 02 25 FF FF 00 00 83 C2 02 01 C3 83 F9 01 77 EB 49 75 05 0F BE 02 01 C3
6316.1.0000000008048000.0000000008057000.r-x.sdmp	Linux_Trojan_Mirai_88de437f	unknown	unknown	• 0xa482:$a: 24 08 8B 4C 24 04 85 D2 74 0D 31 C0 89 F6 C6 04 08 00 40 39 D0
Click to see the 67 entries				

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

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

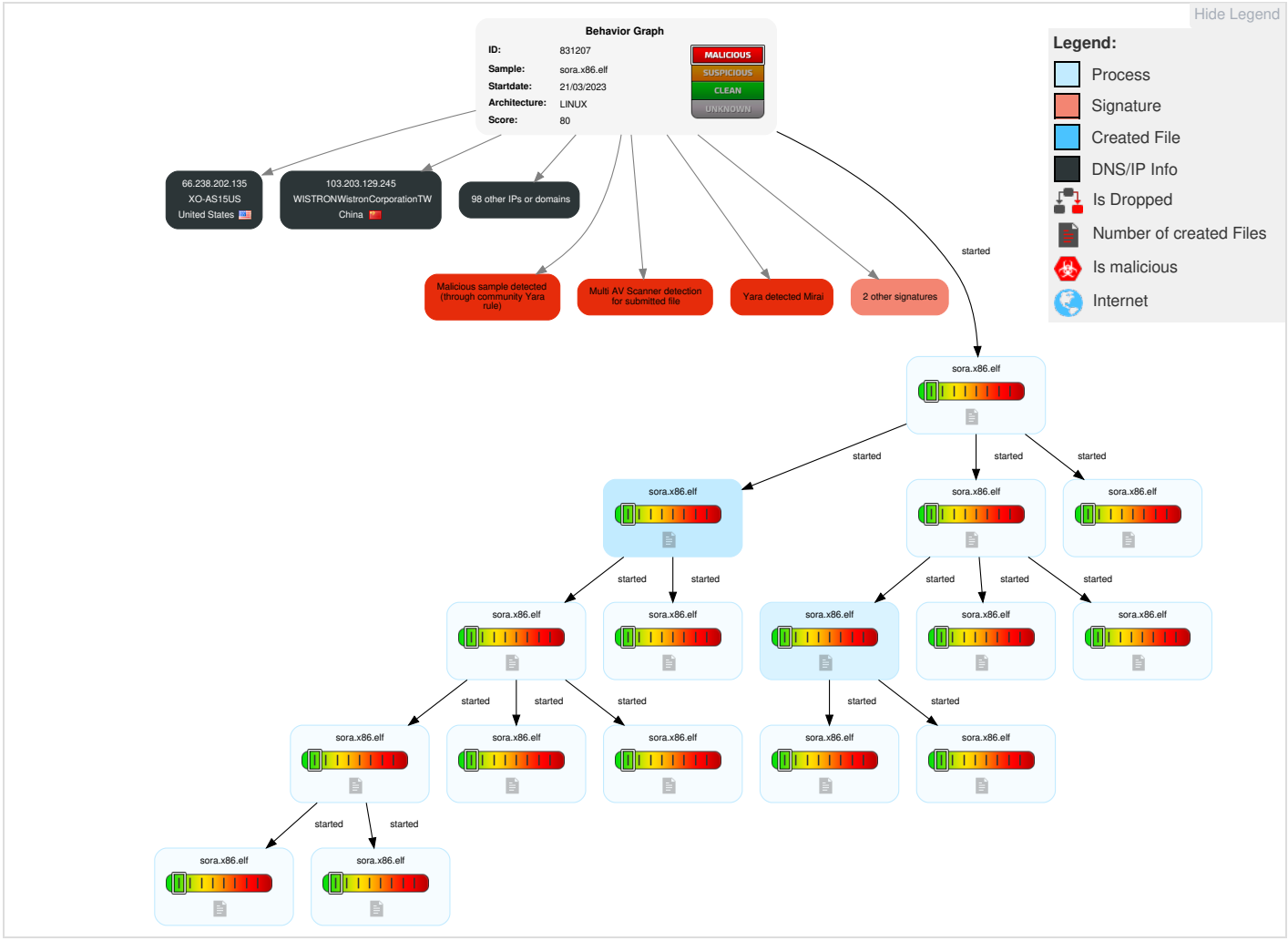
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 1 Obfuscated Files or Information	1 OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	1 1 Non-Standard Port	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	1 Application Layer Protocol	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
sora.x86.elf	69%	ReversingLabs	Linux.Trojan.Mirai	
sora.x86.elf	58%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

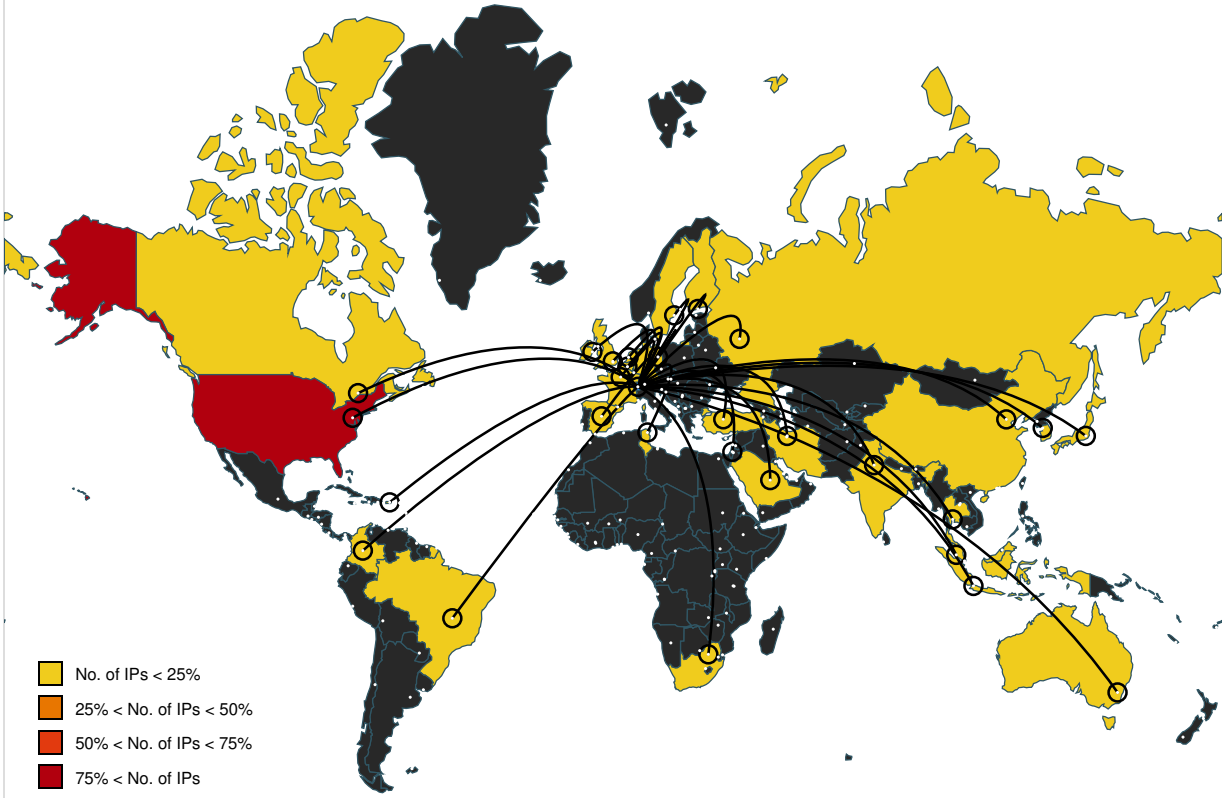
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.81.141.6	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
41.163.216.179	unknown	South Africa		36937	Neotel-ASZA	false
176.136.170.99	unknown	France		5410	BOUYGTEL-ISPFR	false
250.135.211.9	unknown	Reserved		unknown	unknown	false
48.10.80.145	unknown	United States		2686	ATGS-MMD-ASUS	false
177.110.72.108	unknown	Brazil		26615	TIMSABR	false
243.144.74.220	unknown	Reserved		unknown	unknown	false
106.129.53.72	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
222.12.163.124	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
70.89.111.222	unknown	United States		7922	COMCAST-7922US	false
38.71.40.64	unknown	United States		39988	INTELLIGENT-TECHNOLOGY-SOLUTIONSUS	false
105.217.152.42	unknown	South Africa		16637	MTNNS-ASZA	false
157.15.9.149	unknown	unknown		2512	TCP-NETTCPIncJP	false
201.43.167.94	unknown	Brazil		27699	TELEFONICABRASILSABR	false
188.67.250.32	unknown	Finland		16086	DNAFI	false
151.219.242.165	unknown	unknown		11003	PANDGUS	false
92.150.193.36	unknown	France		3215	FranceTelecom-OrangeFR	false
23.161.244.109	unknown	Reserved		19575	ISPNETUS	false
38.54.7.61	unknown	United States		174	COGENT-174US	false
142.106.230.185	unknown	Canada		808	GONET-ASN-1CA	false
5.73.143.151	unknown	Iran (ISLAMIC Republic Of)		57218	RIGHTELIR	false
118.16.75.14	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
247.179.52.153	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.73.176.86	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
8.112.113.215	unknown	United States		3356	LEVEL3US	false
101.201.216.175	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
57.86.163.61	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
170.201.22.99	unknown	United States		10995	PNCBANKUS	false
92.111.42.8	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
23.1.146.96	unknown	United States		6762	SEABONE-NETTELECOMITALIASPARKLESpAIT	false
39.192.61.38	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
101.172.43.74	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
38.0.95.145	unknown	United States		174	COGENT-174US	false
34.199.228.243	unknown	United States		14618	AMAZON-AESUS	false
91.178.248.238	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
36.194.65.150	unknown	China		24138	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
23.21.46.155	unknown	United States		14618	AMAZON-AESUS	false
116.40.18.47	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
194.218.130.135	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
24.95.80.235	unknown	United States		10796	TWC-10796-MIDWESTUS	false
110.170.33.208	unknown	Thailand		7470	TRUEINTERNET-AS-APTRUEINTERNETCoLtdTH	false
251.188.124.217	unknown	Reserved		unknown	unknown	false
103.133.113.47	unknown	India		138310	JUBILANT-ASJubilantFoodworksLimitedIN	false
44.53.238.50	unknown	United States		7377	UCSDUS	false
114.133.53.33	unknown	Malaysia		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
68.54.35.223	unknown	United States		7922	COMCAST-7922US	false
174.140.121.36	unknown	United States		11776	ATLANTICBB-JOHNSTOWNUS	false
223.248.70.160	unknown	China		9812	CNNIC-CN-COLNETOrientalCableNetworkCoLtdCN	false
189.86.165.247	unknown	Brazil		4230	CLAROSABR	false
206.60.118.7	unknown	United States		8014	BATELNETBS	false
19.94.4.107	unknown	United States		3	MIT-GATEWAYSUS	false
176.65.3.11	unknown	Palestinian Territory Occupied		12975	PALTEL-ASPALTELAutonomousSystemPS	false
19.1.83.123	unknown	United States		3	MIT-GATEWAYSUS	false
143.39.115.88	unknown	United States		11003	PANDGUS	false
75.9.72.27	unknown	United States		7018	ATT-INTERNET4US	false
150.29.19.108	unknown	Japan		23793	AISTNationalInstituteofAdvancedIndustrialScienceandT	false
84.188.59.211	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
145.197.157.97	unknown	Netherlands		1101	IP-EEND-ASIP-EENDBVNL	false
78.165.175.187	unknown	Turkey		9121	TTNETTR	false
103.203.129.245	unknown	China		131599	WISTRONWistronCorporationTW	false
155.154.166.84	unknown	United States		1488	DNIC-ASBLK-01488-01489US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
255.146.64.5	unknown	Reserved		unknown	unknown	false
181.52.29.241	unknown	Colombia		10620	TelmexColombiaSACO	false
58.178.161.35	unknown	Australia		9443	VOCUS-RETAIL-AUVocusRetailAU	false
75.146.144.230	unknown	United States		7922	COMCAST-7922US	false
254.14.158.74	unknown	Reserved		unknown	unknown	false
72.152.89.188	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
38.89.204.125	unknown	United States		174	COGENT-174US	false
152.248.210.113	unknown	Brazil		26599	TELEFONICABRASILSABR	false
98.243.159.97	unknown	United States		7922	COMCAST-7922US	false
97.195.200.70	unknown	United States		6167	CELLCO-PARTUS	false
2.203.197.72	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
143.16.24.77	unknown	United States		264008	LANCAMANTOANISERVICOSDEINFORMATICALTDA-MEBR	false
244.239.113.91	unknown	Reserved		unknown	unknown	false
150.108.123.75	unknown	United States		32531	FORDHAM-UNIVERSITYUS	false
147.134.215.195	unknown	United States		30569	CREIGHTON-ASUS	false
168.241.199.152	unknown	United States		21943	ASN-ITG-072618US	false
13.107.141.165	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
203.226.15.246	unknown	Korea Republic of		45385	DAELIMDAELIMCorporationKR	false
70.45.115.227	unknown	Puerto Rico		14638	LCPRLUS	false
145.240.163.248	unknown	France		1101	IP-EEND-ASIP-EENDBVNL	false
253.45.18.214	unknown	Reserved		unknown	unknown	false
82.127.24.59	unknown	France		3215	FranceTelecom-OrangeFR	false
249.181.214.51	unknown	Reserved		unknown	unknown	false
185.220.10.223	unknown	Spain		205390	TECTIQOM-ASDE	false
90.126.139.54	unknown	France		3215	FranceTelecom-OrangeFR	false
251.214.54.12	unknown	Reserved		unknown	unknown	false
254.194.255.52	unknown	Reserved		unknown	unknown	false
38.229.203.83	unknown	United States		23028	TEAM-CYMRUUS	false
213.33.211.152	unknown	Russian Federation		3216	SOVAM-ASRU	false
203.228.150.224	unknown	Korea Republic of		4664	HIT-KR-APShinbiroKR	false
145.103.13.187	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
125.252.63.134	unknown	Korea Republic of		17608	ABN-AS-KRABNKR	false
157.190.234.164	unknown	Ireland		1213	HEANETIE	false
196.178.177.179	unknown	Tunisia		37693	TUNISIANATN	false
166.242.49.101	unknown	United States		6614	USCC-ASNUS	false
253.196.194.66	unknown	Reserved		unknown	unknown	false
66.238.202.135	unknown	United States		2828	XO-AS15US	false
210.37.185.91	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
148.37.24.17	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	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, Intel 80386, version 1 (GNU/Linux), statically linked, no section header
Entropy (8bit):	7.869234697100542
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	sora.x86.elf
File size:	27704
MD5:	ed1472168cdeb8c93dd3f03c3c8fdba8
SHA1:	647657a97916d4db8ade0115a6fb5b3de3c02f77
SHA256:	17492e1447ec32d450601db269a687e058fab102b0bd35763e93483c755921cd
SHA512:	298f355d1a894695b13a11f0de55f56d90b9f98ea568e0f7de280ad9da8feba50af74abb3c5505479af99c8b6e617f933a5e08391b4e089c3dcc8e689708175f
SSDEEP:	384:MRG/9WXUx5+bkbRaliVErjrL9VD9jPwrSaf5cwd/DyZTYHHJC8oytPFnAqV/LITf:/5+Kcrb9VDJeIwkTYTlPFnz/Qe
TLSH:	01C2E1A3A4E5CD15C863413B6F1F1AAB61386524134DEE1E323BEBDC63460B4A176DC7
File Content Preview:	.ELF.....@s..4.....4. ...(.....;k..;k.....~...~.....Q.td.....UPX!.....P...P....._.....?d..ELF.....d.....4....4. (.....k.-.#. .....sw....$..w..\.\..A.

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	

ELF header

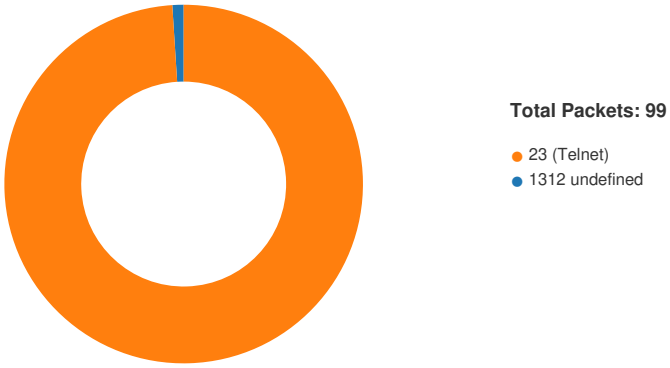
Header String Table Index:	

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0xc01000	0xc01000	0x6b3b	0x6b3b	7.8740	0x5	R E	0x1000		
LOAD	0xe80	0x8057e80	0x8057e80	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: sora.x86.elf PID: 6222, Parent PID: 6124

General

Start time:	09:35:53
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	/tmp/sora.x86.elf
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: 6224, Parent PID: 6222

General

Start time:	09:35:53
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

File Activities

File Read

Directory Enumerated

Analysis Process: sora.x86.elf PID: **6317**, Parent PID: **6224**

General

Start time:	09:38:45
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6319**, Parent PID: **6224**

General

Start time:	09:38:45
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6320**, Parent PID: **6319**

General

Start time:	09:38:45
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6326**, Parent PID: **6320**

General

Start time:	09:38:50
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6327**, Parent PID: **6320**

General

Start time:	09:38:50
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6321**, Parent PID: **6319**

General

Start time:	09:38:45
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf

Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6322**, Parent PID: **6319**

General

Start time:	09:38:45
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6225**, Parent PID: **6222**

General

Start time:	09:35:53
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6226**, Parent PID: **6222**

General

Start time:	09:35:53
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6227**, Parent PID: **6226**

General

Start time:	09:35:53
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

File Activities

File Read

Directory Enumerated

Analysis Process: sora.x86.elf PID: **6316**, Parent PID: **6227**

General

Start time:	09:38:45
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6318**, Parent PID: **6227**

General	
Start time:	09:38:45
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6228**, Parent PID: **6226**

General	
Start time:	09:35:53
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8

Analysis Process: sora.x86.elf PID: **6229**, Parent PID: **6226**

General	
Start time:	09:35:53
Start date:	21/03/2023
Path:	/tmp/sora.x86.elf
Arguments:	n/a
File size:	27704 bytes
MD5 hash:	ed1472168cdeb8c93dd3f03c3c8fdba8