ID: 507393
Sample Name: sora.arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:51:14
Date: 22/10/2021
Version: 33.0.0 White Diamond

Table of Contents

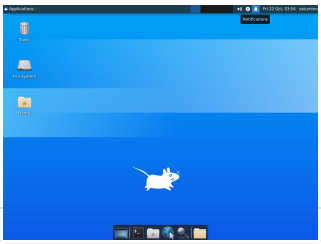
Linux Analysis Report sora.arm

Overview

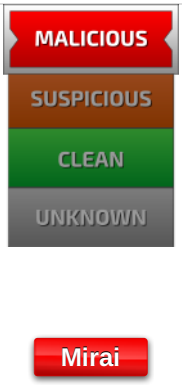
General Information

Sample Name:	sora.arm
Analysis ID:	507393
MD5:	be53dbd9067ec4..
SHA1:	2542023e69a80e..
SHA256:	50aa5219ad1080..
Infos:	

Most interesting Screenshot:



Detection



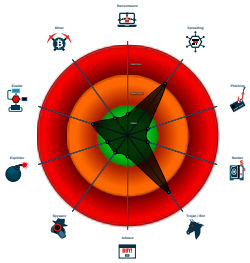
Mirai

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:	507393
Start date:	22.10.2021
Start time:	03:51:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sora.arm
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.linARM@0/2@0/0
Warnings:	Show All

Process Tree

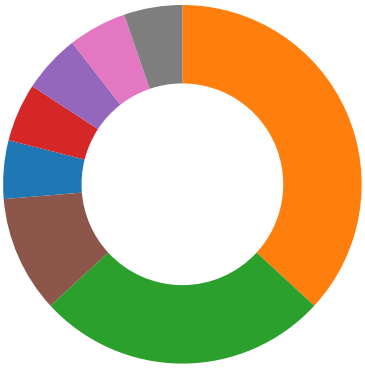
- **system is lnxubuntu20**
- sora.arm (PID: 5247, Parent: 5117, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/sora.arm
  - sora.arm New Fork (PID: 5249, Parent: 5247)
  - sora.arm New Fork (PID: 5250, Parent: 5247)
  - sora.arm New Fork (PID: 5252, Parent: 5247)
    - sora.arm New Fork (PID: 5255, Parent: 5252)
    - sora.arm New Fork (PID: 5257, Parent: 5252)
    - sora.arm New Fork (PID: 5258, Parent: 5252)
- systemd New Fork (PID: 5281, Parent: 1)
  - sshd (PID: 5281, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5282, Parent: 1)
  - sshd (PID: 5282, 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



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

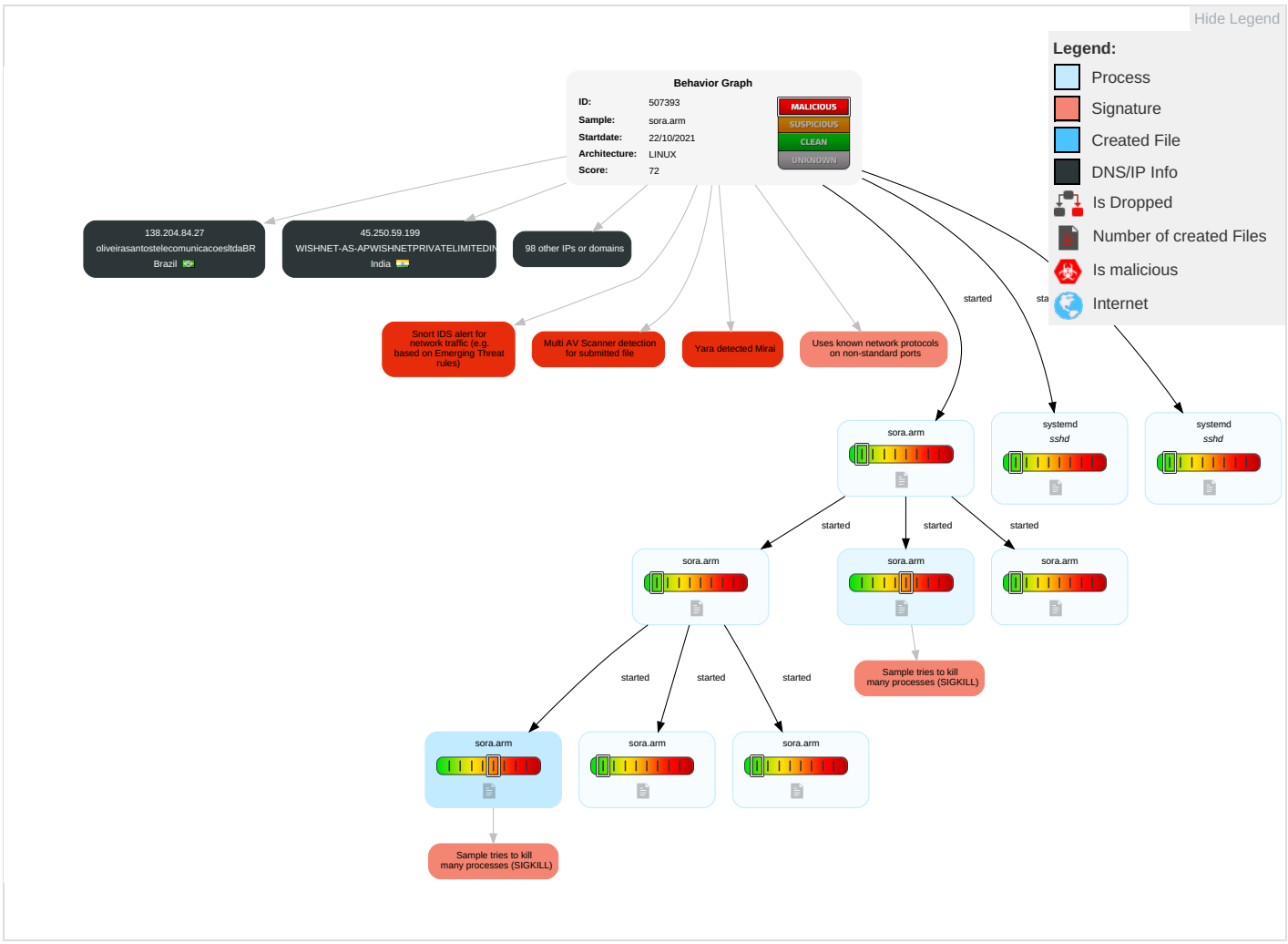
Mitre Att&ck Matrix

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

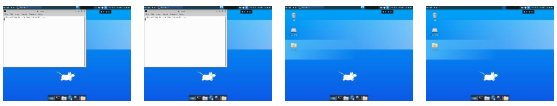
Behavior Graph

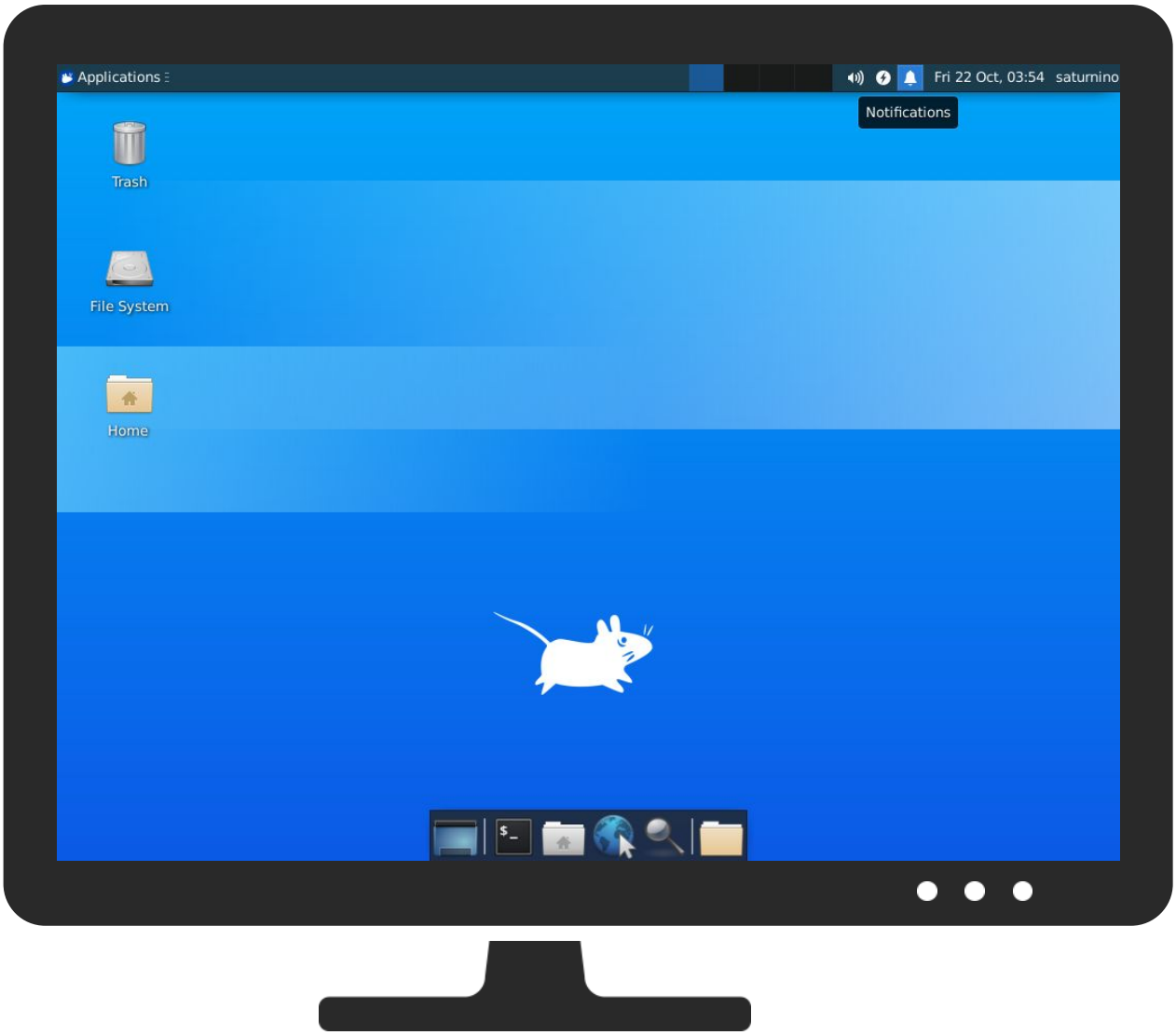


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
sora.arm	51%	Virustotal		Browse

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
4.55.11.241	unknown	United States		3356	LEVEL3US	false
84.117.68.253	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
167.187.21.223	unknown	United States		26529	HILTON-EUS	false
242.255.56.220	unknown	Reserved		unknown	unknown	false
161.80.220.44	unknown	United States		14298	EPA-NETUS	false
117.27.105.202	unknown	China		133776	CHINATELECOM-FUJIAN-QUANZHOU-IDC1QuanzhouCN	false
14.178.101.117	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
155.103.35.42	unknown	United States		17055	UTAHUS	false
43.28.51.144	unknown	Japan		4249	LILLY-ASUS	false
99.255.50.46	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
138.204.84.27	unknown	Brazil		263886	oliveirasantostelecomunicacoesltdaBR	false
218.237.30.108	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
198.38.244.233	unknown	United States		8038	6CONNECTUS	false
113.112.200.78	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
70.171.195.170	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
31.31.135.149	unknown	Belgium		199095	CITYMESH-ASBE	false
27.61.12.140	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
248.214.159.198	unknown	Reserved		unknown	unknown	false
90.76.221.211	unknown	France		3215	FranceTelecom-OrangeFR	false
164.10.127.115	unknown	Sweden		59807	SWEDBANK-ASSE	false
196.248.26.0	unknown	South Africa		2018	TENET-1ZA	false
79.10.129.189	unknown	Italy		3269	ASN-IBSNAZIT	false
121.148.29.153	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
57.138.213.143	unknown	Belgium		2686	ATGS-MMD-ASUS	false
120.212.187.165	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
206.206.98.0	unknown	United States		13332	HYPEENT-SJUS	false
19.129.114.112	unknown	United States		3	MIT-GATEWAYSUS	false
168.98.201.162	unknown	United States		17130	JONESDAYUS	false
88.141.109.122	unknown	France		8228	CEGETEL-ASFR	false
47.46.55.100	unknown	United States		20115	CHARTER-20115US	false
168.235.188.142	unknown	United States		22925	ALLIED-TELECOMUS	false
97.108.2.149	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
34.45.16.134	unknown	United States		2686	ATGS-MMD-ASUS	false
78.66.23.17	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
45.250.59.199	unknown	India		45775	WISHNET-AS-APWISHNETPRIVATELIMITEDIN	false
84.0.112.232	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	false
86.96.126.175	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
18.38.79.125	unknown	United States		3	MIT-GATEWAYSUS	false
47.76.139.3	unknown	United States		9500	VODAFONE-TRANSIT-ASVodafoneNZLtdNZ	false
58.126.77.117	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
182.241.248.253	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
183.125.207.61	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
93.130.191.52	unknown	Germany		6805	TDDE-ASN1DE	false
57.70.235.20	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
101.233.126.238	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
254.218.41.67	unknown	Reserved		unknown	unknown	false
158.209.127.74	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
95.167.9.132	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
201.31.3.43	unknown	Brazil		4230	CLAROSABR	false
13.151.196.62	unknown	United States		7018	ATT-INTERNET4US	false
217.83.112.79	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
178.171.248.203	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
174.239.21.252	unknown	United States		22394	CELLCOUS	false
185.42.139.195	unknown	Sweden		8674	NETNOD-IXNetnodInternetExchangeSverigeABSE	false
193.70.144.166	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
124.51.246.28	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
176.11.44.226	unknown	Norway		12929	NETCOM-ASOsloNorwayNO	false
171.212.68.22	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
252.7.153.45	unknown	Reserved		unknown	unknown	false
8.138.112.156	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
250.159.208.197	unknown	Reserved		unknown	unknown	false
96.53.0.135	unknown	Canada		6327	SHAWCA	false
146.252.65.231	unknown	United States		25400	TELIA-NORWAY-ASTeliaNorwayCoreNetworksNO	false
207.128.45.33	unknown	United States		6289	AHM-CORPUS	false
96.102.137.10	unknown	United States		7922	COMCAST-7922US	false
124.36.206.242	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
195.149.138.21	unknown	Sweden		3257	GTT-BACKBONEGTTDE	false
162.179.208.125	unknown	United States		21928	T-MOBILE-AS21928US	false
170.22.45.118	unknown	United States		18540	RECOVERYPOINTSYSTEMSUS	false
110.242.6.176	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
115.99.154.231	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	false
62.195.46.122	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
173.161.184.194	unknown	United States		7922	COMCAST-7922US	false
191.82.133.18	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
68.45.115.70	unknown	United States		7922	COMCAST-7922US	false
251.35.55.52	unknown	Reserved		unknown	unknown	false
84.220.234.180	unknown	Italy		8612	TISCALI-IT	false
107.18.39.9	unknown	United States		14654	WAYPORTUS	false
24.154.154.217	unknown	United States		27364	ACS-INTERNETUS	false
198.27.93.15	unknown	Canada		16276	OVHFR	false
182.203.239.166	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
185.138.105.250	unknown	France		39405	FULLSAVE-ASFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.99.43.137	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
114.156.131.62	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
111.104.212.232	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
196.122.13.10	unknown	Morocco		36925	ASMediMA	false
250.27.96.100	unknown	Reserved		unknown	unknown	false
145.62.30.67	unknown	Netherlands		201204	GFIS-AS-DE	false
87.243.148.188	unknown	Austria		35370	AINET-ASAT	false
115.127.175.5	unknown	Bangladesh		24342	BRAC-BDMAIL-AS-BDBRACNetLimitedBD	false
189.78.86.126	unknown	Brazil		27699	TELEFONICABRASILSABR	false
249.212.143.196	unknown	Reserved		unknown	unknown	false
151.188.183.20	unknown	United States		21984	FCPSUS	false
184.247.40.201	unknown	United States		10507	SPCSUS	false
86.255.245.37	unknown	France		3215	FranceTelecom-OrangeFR	false
200.248.129.243	unknown	Brazil		4230	CLAROSABR	false
70.9.189.25	unknown	United States		10507	SPCSUS	false
82.193.159.74	unknown	Russian Federation		5563	URALUralRegionalNetRU	false
243.151.79.213	unknown	Reserved		unknown	unknown	false
147.112.122.32	unknown	Norway		766	REDIRISRedIRISAutonomousSystemES	false

Runtime Messages

Command:	/tmp/sora.arm
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
45.250.59.199	dBmJXcsqS4	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEVEL3US	DPJPYxGxfI	Get hash	malicious	Browse	• 4.217.42.190
	4RBTXTxBnt	Get hash	malicious	Browse	• 75.103.49.234
	g22kPe2LIc	Get hash	malicious	Browse	• 9.63.47.20
	cosvgegE1S	Get hash	malicious	Browse	• 4.249.28.35
	gKCq4VLpjL	Get hash	malicious	Browse	• 205.195.40.149
	uK570ZEpyQ	Get hash	malicious	Browse	• 4.95.242.117
	mkRkjGXjDJ	Get hash	malicious	Browse	• 4.219.160.57
	fzkfNBkz1C	Get hash	malicious	Browse	• 4.226.238.87
	UYnpKcFZ2s	Get hash	malicious	Browse	• 9.200.100.99
	jvilYCvWBc	Get hash	malicious	Browse	• 8.63.125.96
	zYMp3detVO	Get hash	malicious	Browse	• 4.100.150.137
	oH6qNmnFRP	Get hash	malicious	Browse	• 9.135.21.252

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Tf9ATzpdKR	Get hash	malicious	Browse	• 206.44.210.185
	b3astmode.arm	Get hash	malicious	Browse	• 9.55.241.26
	b3astmode.arm7	Get hash	malicious	Browse	• 4.250.42.57
	b3astmode.x86	Get hash	malicious	Browse	• 9.198.27.0
	yFbmGHoONE	Get hash	malicious	Browse	• 4.10.26.13
	zju8TB277l	Get hash	malicious	Browse	• 4.58.123.133
	JYWllP5wHP	Get hash	malicious	Browse	• 4.134.233.155
	FWsCarsq8Q	Get hash	malicious	Browse	• 4.9.109.233
LIBERTYGLOBALLibertyGlobalformerly UPCBroadbandHolding	SecuriteInfo.com.Linux.Mirai.1429.15365.3177	Get hash	malicious	Browse	• 178.202.32.7
	R9kV5GcwPz	Get hash	malicious	Browse	• 213.126.148.53
	bqrHRKVNod	Get hash	malicious	Browse	• 87.207.131.229
	g22kPe2LIc	Get hash	malicious	Browse	• 178.84.62.104
	hWT9RJDotD	Get hash	malicious	Browse	• 213.126.148.21
	uK570ZEpyQ	Get hash	malicious	Browse	• 109.255.18 1.171
	mkRkjGXjDJ	Get hash	malicious	Browse	• 109.255.38.18
	ggtS1fKIqX	Get hash	malicious	Browse	• 213.164.252.4
	oH6qNmnFRP	Get hash	malicious	Browse	• 213.126.24 8.234
	b3astmode.arm7	Get hash	malicious	Browse	• 62.143.241.202
	JYWllP5wHP	Get hash	malicious	Browse	• 78.44.174.129
	uwgXkY20gB	Get hash	malicious	Browse	• 84.118.167.187
	sora.arm7	Get hash	malicious	Browse	• 46.140.33.66
	BMP4Nk5TTq	Get hash	malicious	Browse	• 178.84.158.124
	B6WwgS8sUq	Get hash	malicious	Browse	• 212.187.76.144
	PFD33mzc5l	Get hash	malicious	Browse	• 213.126.148.53
	buiodawbdawbuiopdw.x86	Get hash	malicious	Browse	• 62.3.12.42
	hNsTaM2BAu	Get hash	malicious	Browse	• 81.89.1.20
	iSdOB1UKQv	Get hash	malicious	Browse	• 94.171.49.21
	dAhGa49Lql	Get hash	malicious	Browse	• 80.110.209.43

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5282/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

/run/sshd.pid	
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:CF:CF
MD5:	77E31130E90E9883A9065686679D54C0
SHA1:	9EB2EFEC6EC51EAA639F2D599C5EC6DBEC86364A
SHA-256:	EBCC6D4C0E3D89DCD951179B37A6B54CE9B4BB2F26A4E8EF448BAE0C67B074B2
SHA-512:	B92DC2F240498F724A465012B966B0E71911714970CFC01D244F01B9C39DF182C362E24FE3A8A8B2571342A81E185369095326FB7B8AA6A1D4A79B75B95A8162
Malicious:	false
Reputation:	low
Preview:	5282.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), s tatically linked, stripped
Entropy (8bit):	5.973009415949496
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	sora.arm
File size:	56880
MD5:	be53dbd9067ec4960a79a5a273d98fab
SHA1:	2542023e69a80e86a1f9c1af3bb4a0c09c81f46a
SHA256:	50aa5219ad1080a17954597f9370aff75b579f8e550ca19 6fd4d298ff860a67b
SHA512:	b3413bd5e7c7b69a54784d6fae5c4ce69482903deed620 27d661d8ab442a4e4f895e9ef69674be77a5a9229131d8 5c7e07732ed70d7a703b6d848a06229b8bf
SSDEEP:	768:30ESWRYSaG0wBXAy9abThYrB2dPsnjVB5uEBw LRzqmPrqYhH8qkJSULwCVy/rCxE:dSaP0waejVMqY/c J8fhWfM5tMd7oHm
File Content Preview:	.ELF...a.....(.....4.....4. ...(..... .....t.....Q.td.....-...L."....4 .....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	56480
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

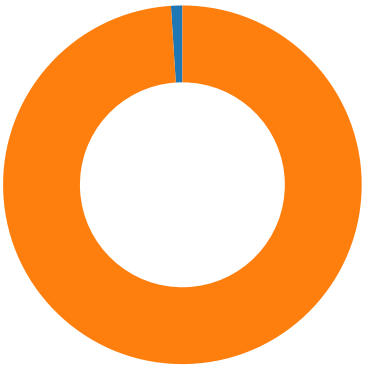
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0xd430	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x154e0	0xd4e0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x154f4	0xd4f4	0x5f4	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1daec	0xdaec	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1daf4	0xdaf4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1db00	0xdb00	0x160	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1dc60	0xdc60	0x280	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xdc60	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	0x8000	0x8000	0xdae8	0xdae8	3.1511	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0xdaec	0x1daec	0x1daec	0x174	0x3f4	0.4351	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



Total Packets: 98

- 23 (Telnet)
- 1312 undefined

TCP Packets

System Behavior

Analysis Process: sora.arm PID: 5247 Parent PID: 5117

General

Start time:	03:51:55
Start date:	22/10/2021
Path:	/tmp/sora.arm
Arguments:	/tmp/sora.arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: sora.arm PID: 5249 Parent PID: 5247

General

Start time:	03:51:55
Start date:	22/10/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: sora.arm PID: 5250 Parent PID: 5247

General

Start time:	03:51:55
Start date:	22/10/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5252 Parent PID: 5247

General

Start time:	03:51:55
Start date:	22/10/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5255 Parent PID: 5252

General

Start time:	03:51:55
Start date:	22/10/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: sora.arm PID: 5257 Parent PID: 5252

General

Start time:	03:51:55
Start date:	22/10/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5258 Parent PID: 5252

General

Start time:	03:51:55
Start date:	22/10/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5281 Parent PID: 1

General

Start time:	03:52:06
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5281 Parent PID: 1

General

Start time:	03:52:06
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: 5282 Parent PID: 1

General

Start time:	03:52:07
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5282 Parent PID: 1

General

Start time:	03:52:07
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