ID: 626479
Sample Name: sora.arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:30:53
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

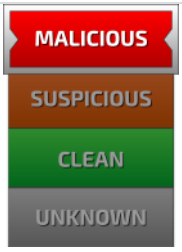
sora.arm

Overview

General Information

Sample Name:	sora.arm
Analysis ID:	626479
MD5:	7799db04192fa3..
SHA1:	15dbc1cc83b869..
SHA256:	600656d40c1543..
Infos:	

Detection



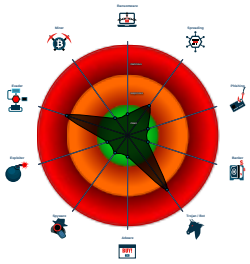
Mirai

Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- 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
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626479
Start date and time: 14/05/202204:30:53	2022-05-14 04:30:53 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
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:	mal60.troj.evad.linARM@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/sora.arm
PID:	6226
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- sora.arm (PID: 6226, Parent: 6123, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/sora.arm
  - sora.arm New Fork (PID: 6228, Parent: 6226)
    - sora.arm New Fork (PID: 6326, Parent: 6228)
    - sora.arm New Fork (PID: 6330, Parent: 6228)
      - sora.arm New Fork (PID: 6333, Parent: 6330)
        - sora.arm New Fork (PID: 6344, Parent: 6333)
        - sora.arm New Fork (PID: 6346, Parent: 6333)
      - sora.arm New Fork (PID: 6335, Parent: 6330)
      - sora.arm New Fork (PID: 6336, Parent: 6330)
    - sora.arm New Fork (PID: 6230, Parent: 6226)
    - sora.arm New Fork (PID: 6231, Parent: 6226)
      - sora.arm New Fork (PID: 6234, Parent: 6231)
        - sora.arm New Fork (PID: 6325, Parent: 6234)
        - sora.arm New Fork (PID: 6328, Parent: 6234)
      - sora.arm New Fork (PID: 6235, Parent: 6231)
      - sora.arm New Fork (PID: 6237, Parent: 6231)
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

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

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Data Obfuscation

Sample is packed with UPX

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

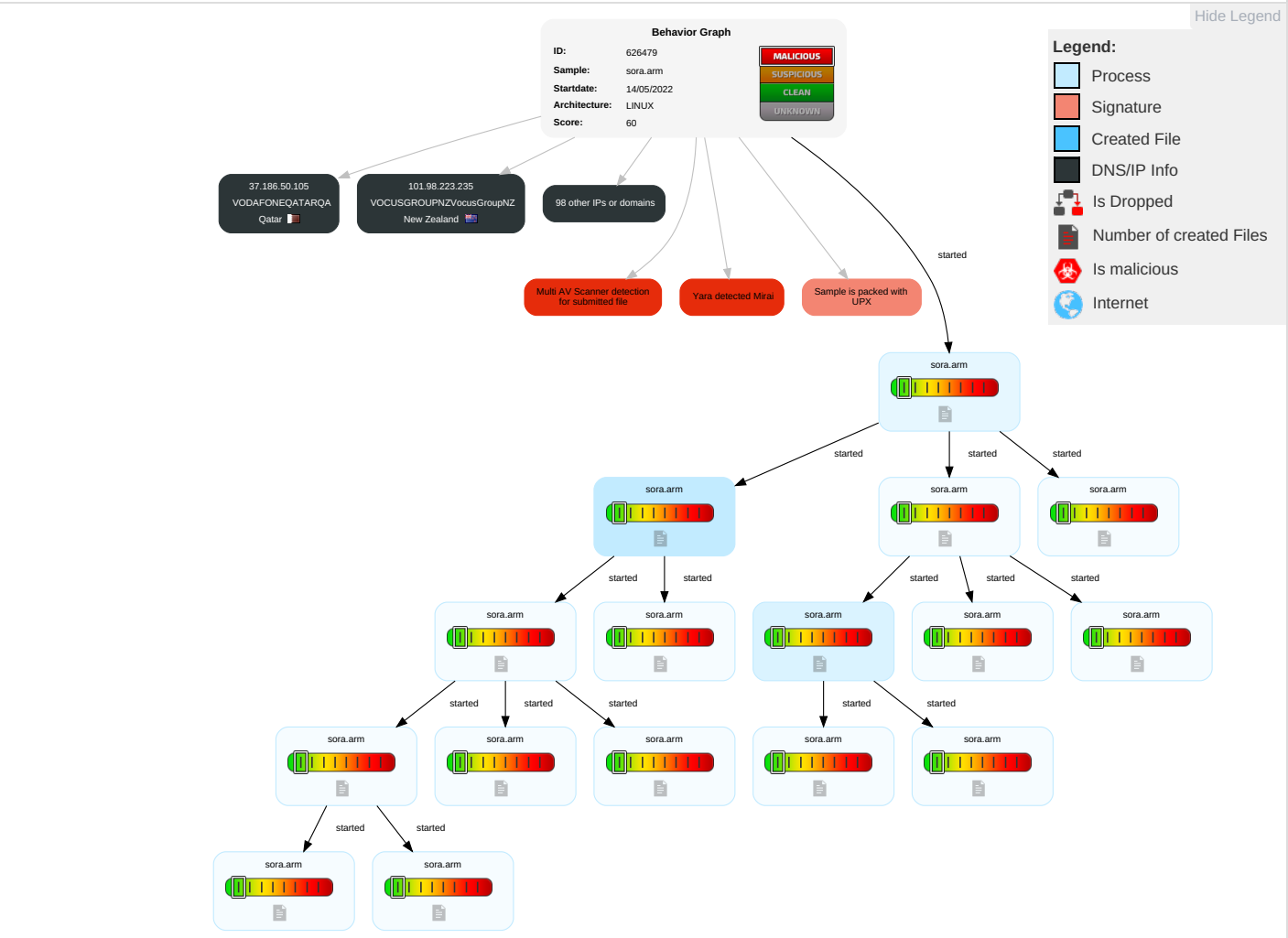
Mitre Att&ck Matrix

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 Obfuscated Files or Information	1 OS Credential Dumping	1 1 Security Software 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 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.arm	43%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

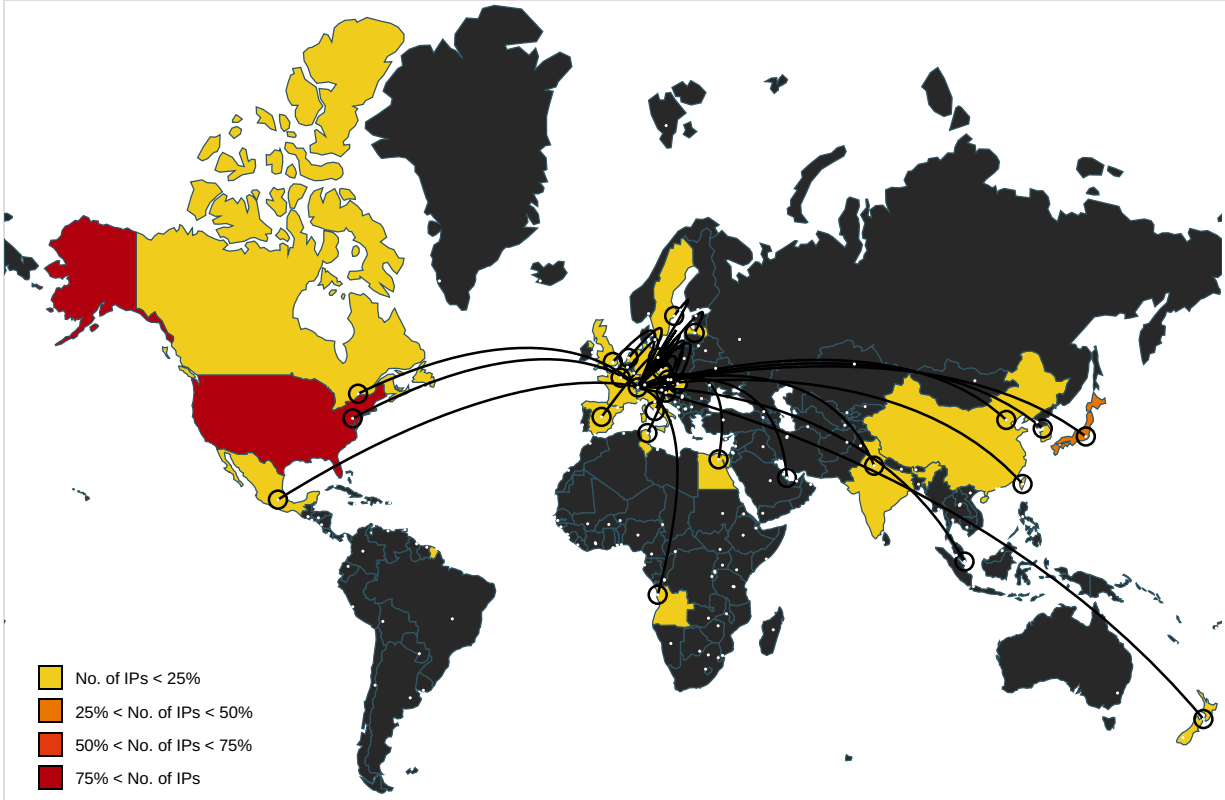
Domains and IPs

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
192.132.79.178	unknown	United States		367	DNIC-ASBLK-00306-00371US	false
17.88.248.1	unknown	United States		714	APPLE-ENGINEERINGUS	false
108.34.195.20	unknown	United States		701	UUNETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.158.231.141	unknown	Austria		8692	BRZAT	false
197.166.142.74	unknown	Egypt		24863	LINKdotNET-ASEG	false
243.142.109.8	unknown	Reserved		unknown	unknown	false
154.28.148.110	unknown	United States		174	COGENT-174US	false
223.110.109.215	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
242.105.215.220	unknown	Reserved		unknown	unknown	false
89.3.43.196	unknown	France		21502	ASN-NUMERICABLEFR	false
248.65.0.12	unknown	Reserved		unknown	unknown	false
16.46.151.36	unknown	United States		unknown	unknown	false
45.140.216.1	unknown	Switzerland		62075	LANNERTDE	false
147.24.192.227	unknown	United States		10796	TWC-10796-MIDWESTUS	false
135.148.11.249	unknown	United States		18676	AVAYAUS	false
253.179.7.5	unknown	Reserved		unknown	unknown	false
187.247.165.44	unknown	Mexico		13999	MegaCableSAdeCVMX	false
37.90.202.181	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
161.53.142.82	unknown	Croatia (LOCAL Name: Hrvatska)		2108	CARNET-ASJMarohnica510000ZagrebHR	false
201.173.227.169	unknown	Mexico		11888	TelevisionInternacionalSAdeCVMX	false
126.89.187.159	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
133.124.154.5	unknown	Japan		2522	PPP-EXPJapanNetworkInformationCenterJP	false
13.165.162.234	unknown	United States		7018	ATT-INTERNET4US	false
218.235.146.189	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
250.183.216.13	unknown	Reserved		unknown	unknown	false
48.6.146.179	unknown	United States		2686	ATGS-MMD-ASUS	false
105.179.193.81	unknown	unknown		37228	Olleh-Rwanda-NetworksRW	false
243.114.158.2	unknown	Reserved		unknown	unknown	false
223.184.95.212	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
108.103.78.32	unknown	United States		10507	SPCSUS	false
75.43.169.89	unknown	United States		7018	ATT-INTERNET4US	false
99.2.51.118	unknown	United States		7018	ATT-INTERNET4US	false
99.188.69.140	unknown	United States		7018	ATT-INTERNET4US	false
160.224.24.100	unknown	Angola		11259	ANGOLATELECOMAO	false
124.54.163.211	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
198.217.52.158	unknown	United States		3354	THENET-AS-3354US	false
46.109.74.153	unknown	Latvia		12578	APOLLO-ASLatviaLV	false
23.254.189.224	unknown	United States		54290	HOSTWINDSUS	false
197.13.57.208	unknown	Tunisia		37504	MeninxTN	false
83.191.157.210	unknown	Sweden		39651	COMHEM-SWEDENSE	false
156.191.147.95	unknown	Egypt		36992	ETISALAT-MISREG	false
95.120.78.125	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
141.231.140.12	unknown	United Kingdom		12701	BARCAPLondonGB	false
66.74.196.104	unknown	United States		20001	TWC-20001-PACWESTUS	false
242.47.204.113	unknown	Reserved		unknown	unknown	false
88.0.190.253	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
222.4.209.248	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
101.98.223.235	unknown	New Zealand		9790	VOCUSGROUPNZVocusGroupNZ	false
246.182.65.69	unknown	Reserved		unknown	unknown	false
197.32.129.167	unknown	Egypt		8452	TE-ASTE-ASEG	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.48.194.60	unknown	United States		20001	TWC-20001-PACWESTUS	false
43.145.165.142	unknown	Japan		4249	LILLY-ASUS	false
246.118.168.83	unknown	Reserved		unknown	unknown	false
24.115.243.251	unknown	United States		3737	AS-PTDUS	false
35.63.96.23	unknown	United States		397797	CITYOFMARSHALL-01US	false
195.199.39.146	unknown	Hungary		1955	HBONE-ASHUNGARNETHU	false
36.107.69.251	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
194.14.131.55	unknown	Sweden		35041	NET-BINERO-STHLM1SE	false
70.96.75.254	unknown	United States		7385	ALLSTREAMUS	false
247.246.7.44	unknown	Reserved		unknown	unknown	false
246.104.145.143	unknown	Reserved		unknown	unknown	false
68.179.33.30	unknown	Canada		20161	TRGOCA	false
109.219.227.142	unknown	France		3215	FranceTelecom-OrangeFR	false
104.208.173.193	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
187.204.147.54	unknown	Mexico		8151	UninetSAdeCVMX	false
48.16.103.121	unknown	United States		2686	ATGS-MMD-ASUS	false
251.189.114.109	unknown	Reserved		unknown	unknown	false
40.61.159.230	unknown	United States		4249	LILLY-ASUS	false
140.207.43.149	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	false
219.29.178.11	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
39.115.115.171	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
78.79.205.44	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
101.13.247.74	unknown	Taiwan; Republic of China (ROC)		24158	TAIWANMOBILE-ASTaiwanMobileCoLtdTW	false
8.173.77.185	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
180.15.127.156	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
108.143.162.126	unknown	United States		16509	AMAZON-02US	false
178.188.243.188	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
86.82.71.136	unknown	Netherlands		1136	KPNKPNNationalEU	false
19.76.79.165	unknown	United States		3	MIT-GATEWAYSUS	false
106.250.8.227	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
180.114.49.216	unknown	China		137702	CHINATELECOM-JIANGSU-NANJING-IDCNanjingJiangsuProvince	false
159.247.172.170	unknown	United States		3481	STOFCT-DOITUS	false
149.9.143.181	unknown	United States		14987	RETHEMHOSTINGUS	false
220.24.38.227	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
95.177.81.60	unknown	United Kingdom		8190	MDNXGB	false
82.184.182.41	unknown	Italy		3269	ASN-IBSNAZIT	false
85.71.236.132	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	false
240.117.204.14	unknown	Reserved		unknown	unknown	false
24.31.202.210	unknown	United States		11426	TWC-11426-CAROLINASUS	false
37.186.50.105	unknown	Qatar		48728	VODAFONEQATARQA	false
210.212.47.194	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
145.225.247.175	unknown	Germany		25039	ASN-LINDEKlosterhofstrasse1DE	false
195.122.185.77	unknown	United Kingdom		3356	LEVEL3US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
220.219.163.179	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
16.85.23.211	unknown	United States		unknown	unknown	false
183.19.172.132	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
158.26.60.160	unknown	United States		1766	ASN-EXXONMOBIL-US	false
59.3.178.43	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
221.213.227.182	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
94.38.206.221	unknown	Italy		8612	TISCALI-IT	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, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	7.930945027439013
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	sora.arm
File size:	24648
MD5:	7799db04192fa39c4d8d2986fbc472a8
SHA1:	15dbc1cc83b869cd3eab35cd02c994507d4d0604
SHA256:	600656d40c15432fe35987fec3d346cf9f34ee9b1ae1d23706925d6c8b6e57b8
SHA512:	11058cc551c7ee141b26b66edaf5ef3f01e3ca6aaf3af8fef5b0edd556213f92695922f52735ffa8c5062cd119c0d51aca5598217f35c9980fec36bf3128b678
SSDEEP:	768:y9MhmNhHXqPpY5IpXetXpsIifmqrs3UozV:y9QmNhHXqxRpXgXpUfwzV
TLSH:	90B2E01179AC5DE2E5748C739F5C8383A30713BAD0DD654015265E289DCE83B21F7AAF

File Content Preview:	.ELF...a.....(.....4.....4. ... (.....__.__.....t[..t...t.....Q.td.....CvUPX!.....Q.....?.E.h;.}...^.....enQ.e.....j.....3.....w..q@5.rN.>^.(.W...

Static ELF Info

ELF header

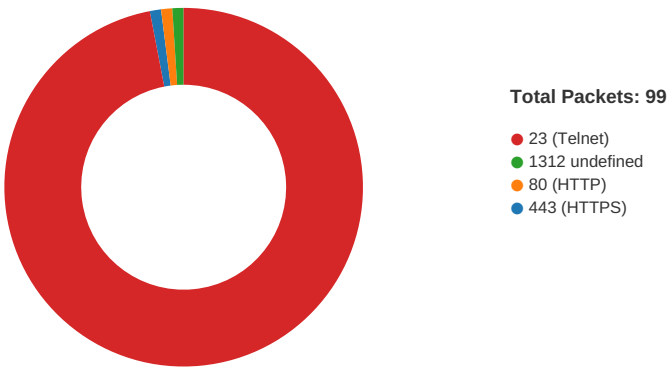
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0xcdb0
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
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	0x8000	0x8000	0x5f5f	0x5f5f	4.0313	0x5	R E	0x8000		
LOAD	0x5b74	0x1db74	0x1db74	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: sora.arm PID: **6226**, Parent PID: **6123**

General

Start time:	04:31:41
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	/tmp/sora.arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: sora.arm PID: **6228**, Parent PID: **6226**

General

Start time:	04:31:41
Start date:	14/05/2022
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: **6326**, Parent PID: **6228**

General

Start time:	04:34:32
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6330**, Parent PID: **6228**

General

Start time:	04:34:32
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6333**, Parent PID: **6330**

General

Start time:	04:34:32
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6344**, Parent PID: **6333**

General

Start time:	04:34:37
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6346**, Parent PID: **6333**

General

Start time:	04:34:37
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6335**, Parent PID: **6330**

General

Start time:	04:34:32
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6336**, Parent PID: **6330**

General

Start time:	04:34:32
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6230**, Parent PID: **6226**

General

Start time:	04:31:41
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6231**, Parent PID: **6226**

General

Start time:	04:31:41
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6234**, Parent PID: **6231**

General

Start time:	04:31:41
Start date:	14/05/2022
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: **6325**, Parent PID: **6234**

General

Start time:	04:34:32
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6328**, Parent PID: **6234**

General

Start time:	04:34:32
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6235**, Parent PID: **6231**

General

Start time:	04:31:41
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: **6237**, Parent PID: **6231**

General

Start time:	04:31:41
Start date:	14/05/2022
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1