ID: 513630
Sample Name: sora.arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:58:06
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

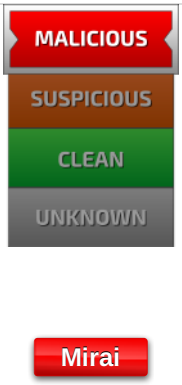
Linux Analysis Report sora.arm

Overview

General Information

Sample Name:	sora.arm
Analysis ID:	513630
MD5:	146e69dbf3fa2b5..
SHA1:	49df0f19985dc93..
SHA256:	48d4f466e1ef7e2..
Infos:	

Detection

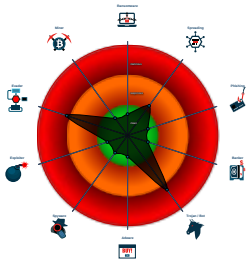


Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- 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 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:	34.0.0 Boulder Opal
Analysis ID:	513630
Start date:	02.11.2021
Start time:	11:58:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 57s
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:	mal68.troj.evad.linARM@0/2@0/0
Warnings:	Show All

Process Tree

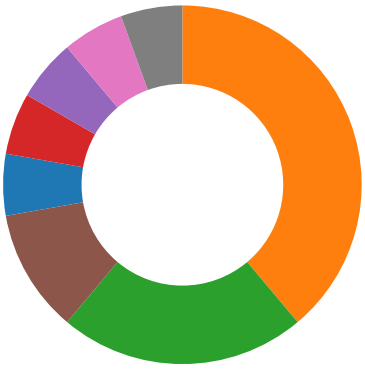
- **system is lnxubuntu20**
- sora.arm (PID: 5245, Parent: 5117, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/sora.arm
  - sora.arm New Fork (PID: 5247, Parent: 5245)
    - sora.arm New Fork (PID: 5389, Parent: 5247)
    - sora.arm New Fork (PID: 5391, Parent: 5247)
      - sora.arm New Fork (PID: 5393, Parent: 5391)
        - sora.arm New Fork (PID: 5406, Parent: 5393)
        - sora.arm New Fork (PID: 5408, Parent: 5393)
      - sora.arm New Fork (PID: 5395, Parent: 5391)
      - sora.arm New Fork (PID: 5396, Parent: 5391)
  - sora.arm New Fork (PID: 5248, Parent: 5245)
  - sora.arm New Fork (PID: 5251, Parent: 5245)
    - sora.arm New Fork (PID: 5253, Parent: 5251)
      - sora.arm New Fork (PID: 5398, Parent: 5253)
      - sora.arm New Fork (PID: 5401, Parent: 5253)
    - sora.arm New Fork (PID: 5255, Parent: 5251)
    - sora.arm New Fork (PID: 5258, Parent: 5251)
- systemd New Fork (PID: 5285, Parent: 1)
- sshd (PID: 5285, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5288, Parent: 1)
- sshd (PID: 5288, 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
- Data Obfuscation
- Persistence and Installation Behavior
- 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)

Data Obfuscation:

Sample is packed with UPX

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

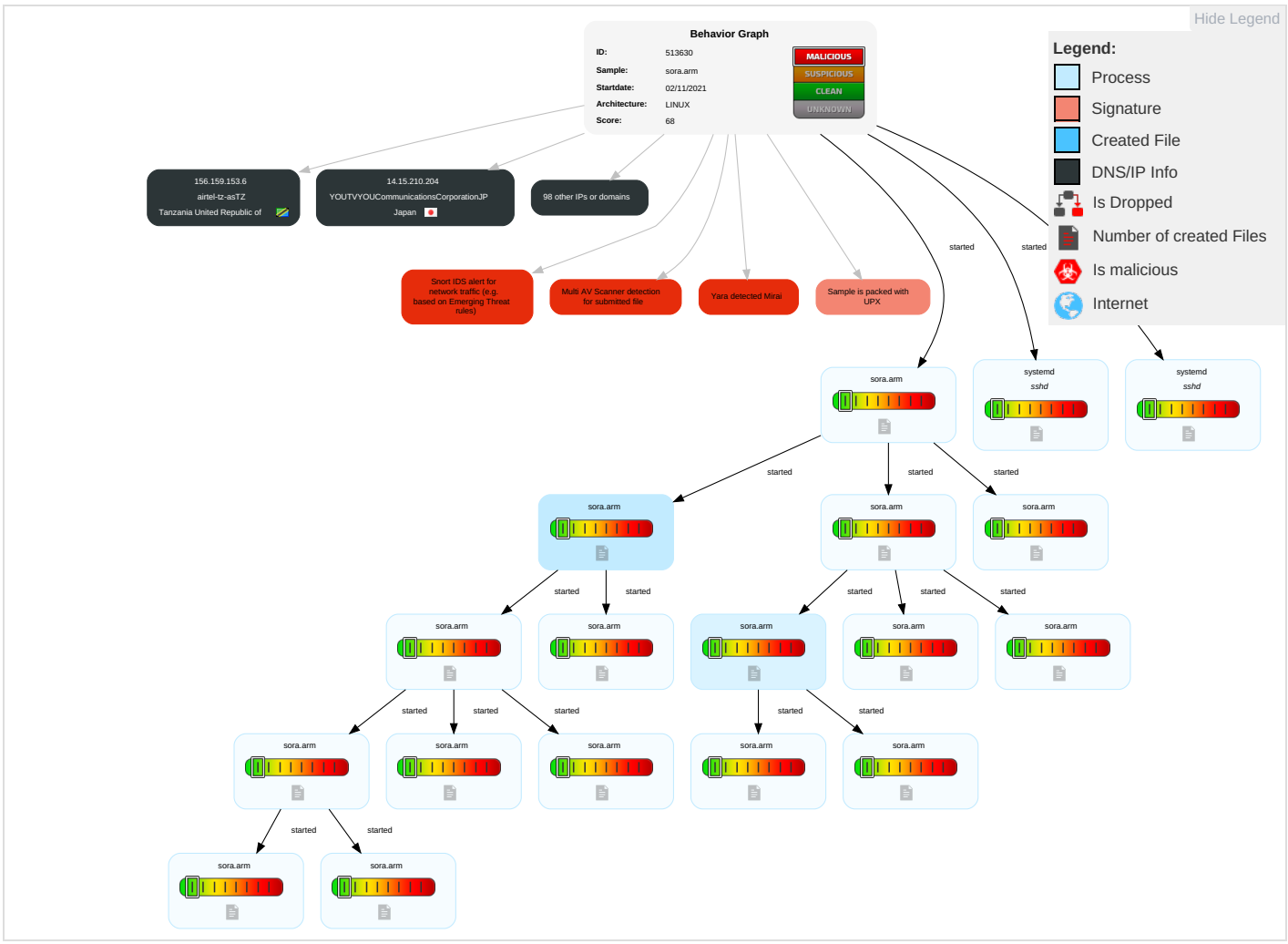
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated Files or Information 1	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	Mod Syst Parti
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	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devi Lock
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	Dele Devi 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	41%	Virustotal		Browse
sora.arm	42%	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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
163.229.182.74	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
246.252.30.75	unknown	Reserved		unknown	unknown	false
179.219.28.171	unknown	Brazil		28573	CLAROSABR	false
83.45.140.219	unknown	Spain		3352	TELEFONICA_DE_ESPANA ES	false
71.64.206.178	unknown	United States		10796	TWC-10796-MIDWESTUS	false
23.210.22.144	unknown	United States		7679	QTNETQTnetIncJP	false
144.48.249.155	unknown	India		55933	CLOUDIE-AS-APCloudieLimitedHK	false
124.21.97.181	unknown	China		7497	CSTNET-AS-APComputerNetworkInformationCenterCN	false
86.239.217.40	unknown	France		3215	FranceTelecom-OrangeFR	false
154.181.108.71	unknown	Egypt		8452	TE-ASTE-ASEG	false
170.72.212.15	unknown	United States		16761	FEDMOG-ASN-01US	false
182.219.30.94	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
2.27.129.117	unknown	United Kingdom		12576	EELtdGB	false
210.33.92.41	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
119.5.222.246	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
124.109.98.255	unknown	China		9797	NEXONASIAPACIFIC-AS-APNexonAsiaPacificPLAU	false
68.65.216.68	unknown	Virgin Islands (BRITISH)		396357	BVI-DIGVG	false
180.187.140.120	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
18.253.84.71	unknown	United States		16509	AMAZON-02US	false
184.100.122.186	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
72.225.180.234	unknown	United States		12271	TWC-12271-NYCUS	false
212.196.181.181	unknown	United Kingdom		49392	ASBAXETNRU	false
182.115.198.192	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
156.159.153.6	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
208.39.209.106	unknown	United States		4997	AFS-WESTUS	false
246.114.129.2	unknown	Reserved		unknown	unknown	false
115.229.163.223	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
172.115.149.230	unknown	United States		20001	TWC-20001-PACWESTUS	false
207.31.98.5	unknown	United States		174	COGENT-174US	false
147.116.44.110	unknown	United States		766	REDIRISRedIRISAutonomousSystemES	false
37.124.245.201	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
247.58.171.139	unknown	Reserved		unknown	unknown	false
245.115.229.68	unknown	Reserved		unknown	unknown	false
119.98.22.192	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
99.88.136.121	unknown	United States		7018	ATT-INTERNET4US	false
150.192.233.18	unknown	United States		1479	DNIC-ASBLK-01478-01479US	false
118.206.43.82	unknown	China		9506	SINGTEL-FIBRESingtelFibreBroadbandSG	false
125.88.53.63	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
76.150.114.42	unknown	United States		7922	COMCAST-7922US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.229.128.76	unknown	Ukraine		15895	KSNET-ASUA	false
77.104.249.197	unknown	Czech Republic		201476	WOLFNETCZ	false
153.213.227.95	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
58.234.32.238	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
80.193.176.131	unknown	United Kingdom		5089	NTLGB	false
162.187.22.173	unknown	United States		21928	T-MOBILE-AS21928US	false
48.192.4.195	unknown	United States		2686	ATGS-MMD-ASUS	false
91.223.243.22	unknown	Estonia		9130	HMS-ASRU	false
77.65.71.9	unknown	Poland		13110	INEA-ASPL	false
108.133.219.246	unknown	United States		16509	AMAZON-02US	false
107.127.53.157	unknown	United States		7018	ATT-INTERNET4US	false
157.228.56.168	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
114.211.192.180	unknown	China		9595	XEPHIONNTT-MECorporationJP	false
19.236.11.170	unknown	United States		3	MIT-GATEWAYSUS	false
189.174.190.60	unknown	Mexico		8151	UninetSAdeCVMX	false
165.76.65.179	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
20.209.235.125	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
73.22.72.159	unknown	United States		7922	COMCAST-7922US	false
87.199.107.137	unknown	Poland		41201	DOLSATulWojskaPolskiego23CPL	false
116.201.10.48	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
152.75.141.108	unknown	United States		20137	USAGM-LANUS	false
12.127.242.59	unknown	United States		7018	ATT-INTERNET4US	false
255.43.156.57	unknown	Reserved		unknown	unknown	false
95.205.130.30	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
175.107.120.229	unknown	Korea Republic of		9765	VTOPIA-AS-KRVTOPIAKR	false
160.192.235.30	unknown	Japan		7670	CTNETEnergiaCommunicationsIncJP	false
108.116.201.123	unknown	United States		10507	SPCSUS	false
194.136.53.17	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
142.87.202.73	unknown	Canada		7950	HC-ASCA	false
103.38.51.243	unknown	India		131458	WILLIAMSLEA-AS-APWILLIAMSLEAINDIAPRIVATELIMITEDIN	false
149.19.144.212	unknown	United States		10250	DATAFIVEUS	false
106.196.252.131	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
209.168.181.190	unknown	United States		7029	WINDSTREAMUS	false
189.206.1.30	unknown	Mexico		11172	AlestraSdeRLdeCVMX	false
68.96.185.223	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
40.191.64.134	unknown	United States		4249	LILLY-ASUS	false
147.87.57.17	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
140.226.54.51	unknown	United States		16519	CUDENVERUS	false
61.145.158.23	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
14.15.210.204	unknown	Japan		131959	YOUTVYOUCommunicationsCorporationJP	false
248.162.216.115	unknown	Reserved		unknown	unknown	false
96.120.35.221	unknown	United States		7922	COMCAST-7922US	false
186.113.231.64	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
243.56.125.139	unknown	Reserved		unknown	unknown	false
93.84.149.187	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
73.116.116.165	unknown	United States		7922	COMCAST-7922US	false
208.143.213.251	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
197.116.147.77	unknown	Algeria		36947	ALGTEL-ASDZ	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.119.67.5	unknown	Poland		16298	INTERBOX-ASLubbersBoxTelematicaBVNL	false
222.185.3.25	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
145.62.19.138	unknown	Netherlands		201204	GFIS-AS-DE	false
82.94.34.56	unknown	Netherlands		3265	XS4ALL-NLAmsterdamNL	false
144.92.74.22	unknown	United States		59	WISC-MADISON-ASUS	false
122.229.132.149	unknown	China		134771	CHINATELECOM-ZHEJIANG-WENZHOU-IDCWENZHOUZHEJIANGProvince	false
53.123.238.100	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
153.135.73.184	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
244.16.241.122	unknown	Reserved		unknown	unknown	false
207.110.103.107	unknown	United States		2828	XO-AS15US	false
244.139.79.29	unknown	Reserved		unknown	unknown	false
247.191.182.142	unknown	Reserved		unknown	unknown	false
18.102.91.87	unknown	United States		3	MIT-GATEWAYSUS	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
118.206.43.82	re2.arm	Get hash	malicious	Browse	
124.21.97.181	CDcUegnLSd	Get hash	malicious	Browse	
99.88.136.121	re.a1rmv4l	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLAROSABR	6A9RyJXCd7	Get hash	malicious	Browse	• 200.247.239.133
	mipsel	Get hash	malicious	Browse	• 186.205.151.110
	arm-20211102-0937	Get hash	malicious	Browse	• 201.56.243.74
	sora.x86	Get hash	malicious	Browse	• 200.255.254.171
	sora.mips	Get hash	malicious	Browse	• 200.172.238.27
	EWTeT0uzHW	Get hash	malicious	Browse	• 201.56.255.64
	eFsSvDKams	Get hash	malicious	Browse	• 189.93.133.5
	L831wSjET5	Get hash	malicious	Browse	• 177.82.174.209
	Hilix.x86	Get hash	malicious	Browse	• 200.229.10.213
	aTQ4RalkUs	Get hash	malicious	Browse	• 191.63.86.246

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	o6aMoZKsIK	Get hash	malicious	Browse	• 200.255.254.166
	8VANaS473t	Get hash	malicious	Browse	• 179.153.48.23
	yVbcX1sEtS	Get hash	malicious	Browse	• 187.29.148.245
	7DoAjWX5uZ	Get hash	malicious	Browse	• 187.38.101.60
	FGVOkw9did	Get hash	malicious	Browse	• 179.209.253.117
	P8AVd483d7	Get hash	malicious	Browse	• 187.38.211.243
	Yoshi.arm	Get hash	malicious	Browse	• 189.100.152.239
	mips	Get hash	malicious	Browse	• 189.60.206.59
	w66OTKGVFv	Get hash	malicious	Browse	• 200.231.97.12
	00hZyjOhZA	Get hash	malicious	Browse	• 179.156.250.213
TELEFONICA_DE_ESPANAES	sora.mips	Get hash	malicious	Browse	• 95.121.137.238
	BsXhlyIHzC	Get hash	malicious	Browse	• 80.36.33.66
	L831wSjET5	Get hash	malicious	Browse	• 95.121.185.136
	JVHk2b1Yd5	Get hash	malicious	Browse	• 95.127.124.196
	WhFNix8BoE	Get hash	malicious	Browse	• 95.121.19.91
	yVbcX1sEtS	Get hash	malicious	Browse	• 83.32.29.93
	8PRjJeUifB	Get hash	malicious	Browse	• 176.80.242.237
	7DoAjWX5uZ	Get hash	malicious	Browse	• 176.80.154.240
	1Y2rsDBP9s	Get hash	malicious	Browse	• 81.41.247.123
	Ko84iLip1u	Get hash	malicious	Browse	• 83.40.96.83
	arH2Af5qoc	Get hash	malicious	Browse	• 83.34.180.127
	t7WU0JjLAR	Get hash	malicious	Browse	• 80.27.241.201
	P8AVd483d7	Get hash	malicious	Browse	• 79.156.169.224
	mRQwOz6Oit	Get hash	malicious	Browse	• 81.43.163.120
	Yoshi.arm7	Get hash	malicious	Browse	• 193.152.99.121
	Yoshi.x86	Get hash	malicious	Browse	• 194.224.122.99
	mipsel	Get hash	malicious	Browse	• 88.16.182.168
	arm	Get hash	malicious	Browse	• 95.125.208.148
	mips	Get hash	malicious	Browse	• 80.37.48.128
	anWxzNav9N	Get hash	malicious	Browse	• 83.46.177.108
KIXS-AS-KRKoreaTelecomKR	6A9RyJXCd7	Get hash	malicious	Browse	• 27.236.140.73
	mipsel	Get hash	malicious	Browse	• 121.177.161.98
	arm-20211102-0937	Get hash	malicious	Browse	• 175.207.154.237
	sora.arm7	Get hash	malicious	Browse	• 220.116.135.254
	sora.x86	Get hash	malicious	Browse	• 124.198.74.66
	mips-20211102-0937	Get hash	malicious	Browse	• 175.207.27.27
	zJk9UEOnQ7	Get hash	malicious	Browse	• 59.1.116.39
	EWTeT0uzHW	Get hash	malicious	Browse	• 110.68.135.133
	oraENsAq4i	Get hash	malicious	Browse	• 210.223.80.230
	MePwVTNRoA	Get hash	malicious	Browse	• 222.97.213.124
	MkyxPXGeTq	Get hash	malicious	Browse	• 218.151.252.36
	eFsSvDKams	Get hash	malicious	Browse	• 118.234.3.34
	KHSQ48GkGn	Get hash	malicious	Browse	• 220.94.246.139
	Hilix.arm	Get hash	malicious	Browse	• 59.27.2.25
	BsXhlyIHzC	Get hash	malicious	Browse	• 211.226.150.150
	L831wSjET5	Get hash	malicious	Browse	• 112.173.38.251
	WhFNix8BoE	Get hash	malicious	Browse	• 121.141.70.237
	Hilix.x86	Get hash	malicious	Browse	• 175.215.45.91
	wt5i2fAcF0	Get hash	malicious	Browse	• 14.97.81.159
	aTQ4RalkUs	Get hash	malicious	Browse	• 128.134.200.251

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5288/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):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:CH:CH
MD5:	646DBD75E4679C90C338B332DCE60B73
SHA1:	7DAAB161D12D83004F8ECDAB11F8F3967D4D1589
SHA-256:	08A99E3191F4A6D2244473F5549F3EA3DDFE3CBD59937583C620D7CC11C9F6FF
SHA-512:	81164F7647D20E1242EA5404A3A76131EB8D44BC03CD994E68FBBE5DA11D5E09422B3C4E72B6570EDAC5EAD3C3B6F7760592CD78038A24C74C9EA6CE37FA4CB
Malicious:	false
Reputation:	low
Preview:	5288.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	7.929459447179547
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	sora.arm
File size:	25004
MD5:	146e69dbf3fa2b51093964f087c9be01
SHA1:	49df0f19985dc9369426d2445560f4346c52e8c3
SHA256:	48d4f466e1ef7e2872a2ad032ca98e8ea161c3fd25f6eda3ef5cf271f23dd557
SHA512:	a941247f2a6be938aa4a2b83d80962aa78326975ced590dd96a2673689f1705b7e8644ecf32c88a413c39ec18a4bca9b4c6ddd562c423473b07b1ac03b080f50
SSDEEP:	384:cZ0X9nxn8o9ir/nSdoijsN2e4JQkCD2EjKb3pLLhymdGUop5hi:5X9nxn8o9wnBoWzEQf2EjKb3p3s3UozQ
File Content Preview:	.ELF...a.....(.....4.....4. ...(.....`...`.....^.....Q.td.....CvUPX!.....0...0.....R.....?.E.h;.}...^.....f.Z.6..(fw....&.x:.E.....oe.`.S..T.....n..

Static ELF Info

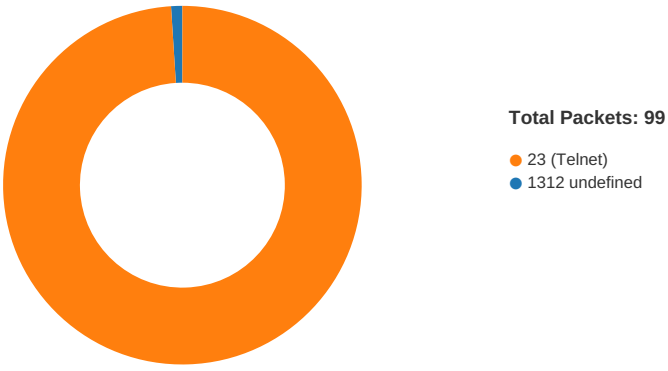
ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0xcf10
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program 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	0x60bf	0x60bf	4.0455	0x5	R E	0x8000		
LOAD	0x5ee0	0x1dee0	0x1dee0	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: 5245 Parent PID: 5117

General

Start time:	11:58:49
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	/tmp/sora.arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: sora.arm PID: 5247 Parent PID: 5245

General

Start time:	11:58:49
Start date:	02/11/2021
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: 5389 Parent PID: 5247

General

Start time:	12:01:48
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5391 Parent PID: 5247

General

Start time:	12:01:48
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5393 Parent PID: 5391

General

Start time:	12:01:48
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5406 Parent PID: 5393

General

Start time:	12:01:53
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5408 Parent PID: 5393

General

Start time:	12:01:53
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5395 Parent PID: 5391

General

Start time:	12:01:48
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5396 Parent PID: 5391

General

Start time:	12:01:48
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5248 Parent PID: 5245

General

Start time:	11:58:49
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5251 Parent PID: 5245

General

Start time:	11:58:49
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5253 Parent PID: 5251

General

Start time:	11:58:49
Start date:	02/11/2021
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: 5398 Parent PID: 5253

General

Start time:	12:01:48
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5401 Parent PID: 5253

General

Start time:	12:01:48
Start date:	02/11/2021
Path:	/tmp/sora.arm

Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5255 Parent PID: 5251

General

Start time:	11:58:49
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm PID: 5258 Parent PID: 5251

General

Start time:	11:58:49
Start date:	02/11/2021
Path:	/tmp/sora.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5285 Parent PID: 1

General

Start time:	11:58:59
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5285 Parent PID: 1

General

Start time:	11:58:59
Start date:	02/11/2021
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: 5288 Parent PID: 1

General

Start time:	11:59:00
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5288 Parent PID: 1

General

Start time:	11:59:00
Start date:	02/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated