ID: 518886
Sample Name: sora.arm7
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:52:22
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

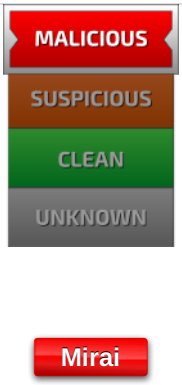
Linux Analysis Report sora.arm7

Overview

General Information

Sample Name:	sora.arm7
Analysis ID:	518886
MD5:	c0530dfd3766a32.
SHA1:	a45fb3c938ed307.
SHA256:	8a6e72fa60a5be3.
Tags:	Mirai
Infos:	

Detection

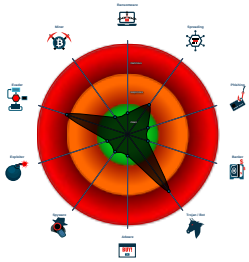


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample is packed with UPX
- Uses known network protocols on no...
- Sample contains only a LOAD segm...
- Yara signature match
- 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

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:	518886
Start date:	10.11.2021
Start time:	03:52:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sora.arm7
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.troj.evad.linARM7@0/2@0/0
Warnings:	Show All

Process Tree

Copyright Joe Security LLC 2021

- **system is lnxubuntu20**
- sora.arm7 (PID: 5240, Parent: 5119, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/sora.arm7
  - sora.arm7 New Fork (PID: 5242, Parent: 5240)
    - sora.arm7 New Fork (PID: 5374, Parent: 5242)
    - sora.arm7 New Fork (PID: 5375, Parent: 5242)
      - sora.arm7 New Fork (PID: 5378, Parent: 5375)
        - sora.arm7 New Fork (PID: 5391, Parent: 5378)
        - sora.arm7 New Fork (PID: 5392, Parent: 5378)
      - sora.arm7 New Fork (PID: 5380, Parent: 5375)
      - sora.arm7 New Fork (PID: 5381, Parent: 5375)
  - sora.arm7 New Fork (PID: 5243, Parent: 5240)
  - sora.arm7 New Fork (PID: 5245, Parent: 5240)
    - sora.arm7 New Fork (PID: 5248, Parent: 5245)
      - sora.arm7 New Fork (PID: 5385, Parent: 5248)
      - sora.arm7 New Fork (PID: 5387, Parent: 5248)
    - sora.arm7 New Fork (PID: 5249, Parent: 5245)
    - sora.arm7 New Fork (PID: 5252, Parent: 5245)
- systemd New Fork (PID: 5273, Parent: 1)
- sshd (PID: 5273, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5274, Parent: 1)
- sshd (PID: 5274, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

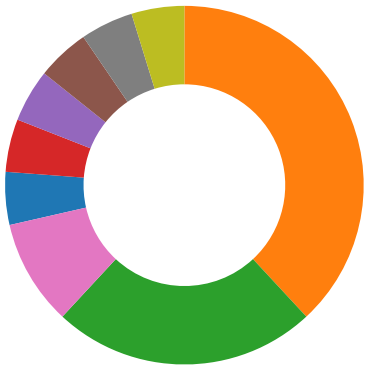
Initial Sample

Source	Rule	Description	Author	Strings
sora.arm7	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x7c94:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x7d03:$s2: $Id: UPX • 0x7cb4:$s3: $Info: This file is packed with the UPX executable packer

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
- Hooking and other Techniques for Hiding and Protection
- 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)

Copyright Joe Security LLC 2021

Uses known network protocols on non-standard ports

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

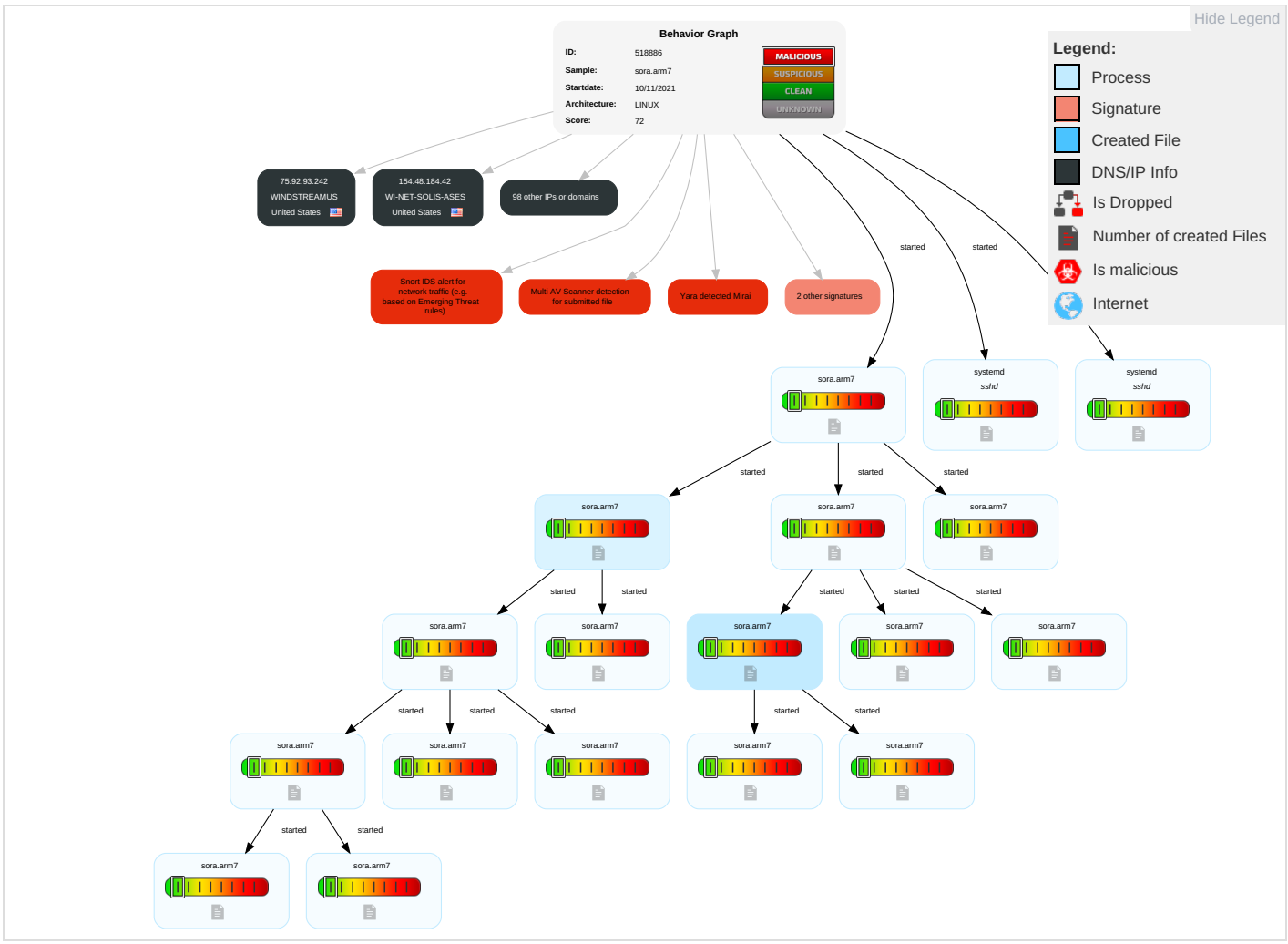
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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 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.arm7	42%	Virustotal		Browse
sora.arm7	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

Copyright Joe Security LLC 2021

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
105.180.23.20	unknown	Egypt		37069	MOBINILEG	false
38.5.198.77	unknown	United States		174	COGENT-174US	false
44.244.125.175	unknown	United States		16509	AMAZON-02US	false
108.198.1.171	unknown	United States		7018	ATT-INTERNET4US	false
213.60.85.253	unknown	Spain		12334	Galicia-SpainES	false
38.3.136.25	unknown	United States		174	COGENT-174US	false
250.29.133.144	unknown	Reserved		unknown	unknown	false
157.6.233.117	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
157.145.44.94	unknown	United States		719	ELISA-ASHelsinkiFinlandEU	false
73.198.119.83	unknown	United States		7922	COMCAST-7922US	false
162.65.245.129	unknown	United States		35893	ACPCA	false
152.43.75.176	unknown	United States		33401	CPCCUS	false
68.107.216.54	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
216.61.47.73	unknown	United States		7018	ATT-INTERNET4US	false
196.224.103.15	unknown	Tunisia		37492	ORANGE-TN	false
32.193.220.66	unknown	United States		2686	ATGS-MMD-ASUS	false
197.109.134.94	unknown	South Africa		37168	CELL-CZA	false
81.180.199.188	unknown	Romania		8953	ASN-ORANGE-ROMANIARO	false
147.48.140.172	unknown	United States		2852	CESNET2CZ	false
211.14.115.244	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
147.105.169.59	unknown	United States		22522	ULALAUNCHUS	false
220.232.49.252	unknown	Singapore		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
96.195.125.71	unknown	United States		7922	COMCAST-7922US	false
107.157.7.1	unknown	United States		7065	SONOMAUS	false
154.48.184.42	unknown	United States		203499	WI-NET-SOLIS-ASES	false
244.203.2.250	unknown	Reserved		unknown	unknown	false
253.241.166.61	unknown	Reserved		unknown	unknown	false
125.178.123.148	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
76.227.191.165	unknown	United States		7018	ATT-INTERNET4US	false
212.9.202.33	unknown	United Kingdom		8942	LondonOfficeGB	false
74.202.235.90	unknown	United States		395313	BRAINTREEUS	false
124.145.224.179	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
180.249.117.189	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
186.246.82.239	unknown	Brazil		7738	TelemarNorteLesteSABR	false
184.192.180.65	unknown	United States		10507	SPCSUS	false
180.145.69.198	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
171.99.205.149	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	false
111.196.171.136	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
43.74.235.99	unknown	Japan		4249	LILLY-ASUS	false
44.105.65.47	unknown	United States		7377	UCSDUS	false
218.181.74.77	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
53.191.190.220	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
152.241.29.184	unknown	Brazil		26599	TELEFONICABRASILSABR	false
91.186.75.42	unknown	Norway		56828	NORWEGIANHEALTHNETWORKNO	false
109.165.176.243	unknown	Bosnia and Herzegowina		25144	TELEKOM-SRPSKE-ASKraljaPetraIKaradjordjevica61aBA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.0.172.146	unknown	South Africa		328112	Linux-Based-Systems-Design-ASZA	false
93.87.57.249	unknown	Serbia		8400	TELEKOM-ASRS	false
82.25.98.22	unknown	United Kingdom		5089	NTLGB	false
40.178.220.70	unknown	United States		4249	LILLY-ASUS	false
70.34.47.248	unknown	United States		15830	EQUINIX-CONNECT-EMEAGB	false
110.109.134.165	unknown	China		134810	CMNET-JILIN-AS-APChinaMobileGroupJiLincommunicationsco	false
139.0.170.93	unknown	Indonesia		23700	FASTNET-AS-IDLinknet-FastnetASNID	false
35.2.238.241	unknown	United States		36375	UMICH-AS-5US	false
183.109.40.165	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
161.58.199.192	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
189.181.107.156	unknown	Mexico		8151	UninetSAdeCVMX	false
248.38.186.19	unknown	Reserved		unknown	unknown	false
136.69.43.77	unknown	United States		60311	ONEFMCH	false
80.155.119.168	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
82.39.27.145	unknown	United Kingdom		5089	NTLGB	false
199.81.85.172	unknown	United States		7726	FITC-ASUS	false
163.109.89.198	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
90.158.71.173	unknown	Turkey		9021	ISNETTR	false
32.148.111.173	unknown	United States		2686	ATGS-MMD-ASUS	false
84.87.28.28	unknown	Netherlands		1136	KPNKPNNationalEU	false
78.152.92.58	unknown	Austria		35370	AINET-ASAT	false
187.51.205.102	unknown	Brazil		10429	TELEFONICABRASILSABR	false
36.75.177.224	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
142.166.65.11	unknown	Canada		855	CANET-ASN-4CA	false
70.210.207.227	unknown	United States		6167	CELLCO-PARTUS	false
18.102.226.164	unknown	United States		3	MIT-GATEWAYSUS	false
75.92.93.242	unknown	United States		7029	WINDSTREAMUS	false
84.73.147.144	unknown	Switzerland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
60.126.184.178	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
144.44.178.235	unknown	European Union		21286	KPN-CORPORATE-MARKETNL	false
109.115.234.55	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
253.85.73.245	unknown	Reserved		unknown	unknown	false
17.242.50.87	unknown	United States		714	APPLE-ENGINEERINGUS	false
251.59.93.2	unknown	Reserved		unknown	unknown	false
138.226.133.196	unknown	Switzerland		12980	EMEAHostingAutonomousSystemEU	false
247.52.50.28	unknown	Reserved		unknown	unknown	false
40.193.69.189	unknown	United States		4249	LILLY-ASUS	false
109.239.104.154	unknown	United Kingdom		33920	AQLGB	false
112.255.242.110	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
178.244.73.50	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
87.143.226.17	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
84.187.248.166	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
190.79.134.140	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
246.57.16.99	unknown	Reserved		unknown	unknown	false
126.97.154.254	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
48.235.60.188	unknown	United States		2686	ATGS-MMD-ASUS	false
43.143.51.89	unknown	Japan		4249	LILLY-ASUS	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
169.111.169.161	unknown	United States		37611	AfrihostZA	false
167.128.242.202	unknown	United States		25899	LSNETUS	false
110.53.232.225	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
93.47.218.64	unknown	Italy		12874	FASTWEBIT	false
45.205.88.180	unknown	Seychelles		54600	PEGTECHINCUS	false
58.162.208.60	unknown	Australia		1221	ASN-TELSTRATelstraCorporation LtdAU	false
247.160.162.94	unknown	Reserved		unknown	unknown	false
162.104.193.5	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false

Runtime Messages

Command:	/tmp/sora.arm7
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MOBINILEG	Heri2RE17I	Get hash	malicious	Browse	• 45.96.249.224
	v9o2vinbUj	Get hash	malicious	Browse	• 45.106.6.129
	QaCRsRGMyb	Get hash	malicious	Browse	• 45.104.148.59
	QSjpGBd7Gv	Get hash	malicious	Browse	• 45.97.8.6
	fbXTgwatuJ	Get hash	malicious	Browse	• 45.96.114.49
	27xJuvcfMM	Get hash	malicious	Browse	• 45.104.67.13
	2b6XF36zQq	Get hash	malicious	Browse	• 197.223.62.23
	EwSjOP120s	Get hash	malicious	Browse	• 154.136.91.73
	s4Qw9YZtjr	Get hash	malicious	Browse	• 197.222.170.112
	Zhh51946Eq	Get hash	malicious	Browse	• 102.13.166.47
	DvwfkRaTRo	Get hash	malicious	Browse	• 105.33.240.3
	IYcCOLfGT7	Get hash	malicious	Browse	• 102.13.129.64
	bZ3EzTJKiD	Get hash	malicious	Browse	• 102.15.192.80
	X8q5ELI79g	Get hash	malicious	Browse	• 102.13.154.34
	sora.arm7	Get hash	malicious	Browse	• 45.104.148.38
	3Htna329pC	Get hash	malicious	Browse	• 154.136.21.109
	mipsel	Get hash	malicious	Browse	• 154.134.132.111
	zJk9UEOnQ7	Get hash	malicious	Browse	• 45.104.148.70
	MePwVTNRoA	Get hash	malicious	Browse	• 45.104.148.60
	MkyxPXGeTq	Get hash	malicious	Browse	• 45.106.6.109
COGENT-174US	arm	Get hash	malicious	Browse	• 149.120.38.179

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order confirmation.exe	Get hash	malicious	Browse	• 143.244.146.182
	mips	Get hash	malicious	Browse	• 38.198.158.164
	arm	Get hash	malicious	Browse	• 149.113.158.20
	Shipping Documents.exe	Get hash	malicious	Browse	• 206.237.226.3
	BS0Dxmu2go	Get hash	malicious	Browse	• 38.142.176.60
	Kz2SeJpaxw	Get hash	malicious	Browse	• 38.30.199.60
	RrK5IgZ6gZ	Get hash	malicious	Browse	• 154.60.6.214
	BKyU0T5xcw	Get hash	malicious	Browse	• 38.238.192.108
	skonwRkAlJ	Get hash	malicious	Browse	• 38.50.252.69
	jyTZMJKPD2	Get hash	malicious	Browse	• 149.44.189.199
	P8NtIPe7f0	Get hash	malicious	Browse	• 38.169.130.58
	OoeA4dABtV	Get hash	malicious	Browse	• 38.171.134.157
	gFn4iz8ygL	Get hash	malicious	Browse	• 38.185.170.70
	b8xw7rKh8F	Get hash	malicious	Browse	• 62.73.8.76
	Zhh51946Eq	Get hash	malicious	Browse	• 149.52.186.146
	FAuA0G2obM	Get hash	malicious	Browse	• 38.212.157.134
	Order No. AU-L0475-500.exe	Get hash	malicious	Browse	• 154.23.204.55
	fCca2FJVXG	Get hash	malicious	Browse	• 38.173.137.250
	DDgJHmrtcG	Get hash	malicious	Browse	• 149.110.24.45
AMAZON-02US	v9o2vinbUj	Get hash	malicious	Browse	• 34.254.55.151
	QSjpGBd7Gv	Get hash	malicious	Browse	• 108.152.25.10
	fbXTgwatuJ	Get hash	malicious	Browse	• 13.225.123.90
	27xJuvcfMM	Get hash	malicious	Browse	• 54.250.225.134
	E4438FE55AD506189992ED8BFA402449106E5C7D0AE3A.exe	Get hash	malicious	Browse	• 3.13.191.225
	rEOqCaa9fM.apk	Get hash	malicious	Browse	• 52.92.163.216
	Passcode_for_jsartori_451_6.html	Get hash	malicious	Browse	• 52.34.207.165
	DevInstallerBeta.exe	Get hash	malicious	Browse	• 104.192.141.1
	DevInstallerBeta.exe	Get hash	malicious	Browse	• 52.217.129.129
	Devoncs-Attachment 2021-11-09 File - 5849057.html	Get hash	malicious	Browse	• 13.32.219.88
	PO_AMO_8100045923.exe	Get hash	malicious	Browse	• 50.18.238.17
	zuroq8.dll	Get hash	malicious	Browse	• 205.251.242.103
	zuroq1.dll	Get hash	malicious	Browse	• 176.32.103.205
	BSDs-4933.PZTOJFSSIFHXAAYTSKOMYAGCHTHAOF#U00f1.msi	Get hash	malicious	Browse	• 13.249.13.93
	8557527948257.html	Get hash	malicious	Browse	• 13.249.13.23
	SOA & INV FOR OCT'21.exe	Get hash	malicious	Browse	• 3.64.163.50
	Order confirmation.exe	Get hash	malicious	Browse	• 54.176.36.242
	vbc.exe	Get hash	malicious	Browse	• 44.227.65.245
	Vergi #U00f6deme faturas#U0131 9 Kas#U0131m 2021 Sal#U0131,pdf.exe	Get hash	malicious	Browse	• 75.2.115.196
	MV OCEANLADY.docx	Get hash	malicious	Browse	• 76.223.86.4

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5274/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

/proc/5274/oom_score_adj	
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):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Civ:CM
MD5:	399A14B7B28E9470E1BE6F272272890A
SHA1:	5B82D7F69C166B978FBFC8009876BE4797BAAC8D
SHA-256:	7C92CC37DF60EBCCC15A4175839687DD0EC20BD8FA9A730DD1C193473D3A5860
SHA-512:	01619BEF8D2ADA8E3EBF14DB84500B3F0D1F8C19AB9FE963C74C39168DB2719E21B8AA033FFA1B6FCE28C07D54B4B098CB5FBB255908170484C683DD1752CBD9
Malicious:	false
Reputation:	low
Preview:	5274.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.977264005957624
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	sora.arm7
File size:	48696
MD5:	c0530dfd3766a324673f37c1644de5bc
SHA1:	a45fb3c938ed307ed0f4a550bc17e460a0e5b661
SHA256:	8a6e72fa60a5be3c99b64bdbbf23839949e051dfaf9b975c040fa00c8edde1c6
SHA512:	bcdf869c6ab18916424f9c7d44202c8fab64c99a445afe1a1a6f5bb64d87cea28072bfc78f437e3cb8b91711154672ebffa0929d1347929f06e103073e19f824
SSDEEP:	768:lK7y1XGO1LCNgukEkvwtqPnH7u83nc0iFA9q3UELWt/iw+kvBGg6+fYtrBHM:N12O1LCNguovDPH7Tcr3LWhiw+kvBGgt
File Content Preview:	.ELF.....(.....4.....4. ...(..... ..... b.. b.. b.....Q.td.....OUPX!.....p...p.....h.....?.E.h;....#..$...o.....=..B.*...5N&"a..mk.c.....}<.....M.Q....[

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:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0xf1a0

ELF header

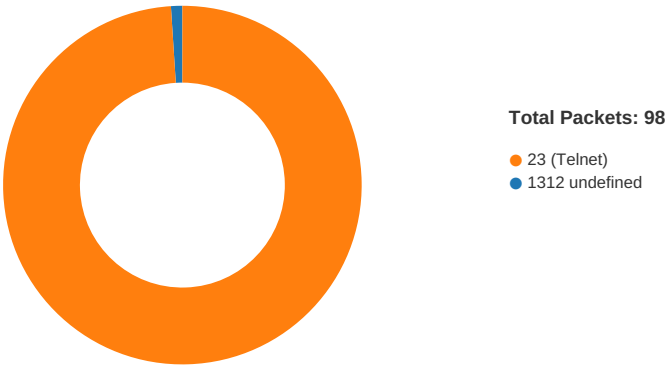
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

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	0x838d	0x838d	4.0392	0x5	R E	0x8000		
LOAD	0x6220	0x26220	0x26220	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.arm7 PID: 5240 Parent PID: 5119

General

Start time:	03:53:02
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	/tmp/sora.arm7
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

Copyright Joe Security LLC 2021

File Read

Analysis Process: sora.arm7 PID: 5242 Parent PID: 5240

General

Start time:	03:53:02
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: sora.arm7 PID: 5374 Parent PID: 5242

General

Start time:	03:56:04
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5375 Parent PID: 5242

General

Start time:	03:56:04
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5378 Parent PID: 5375

General

Start time:	03:56:04
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Copyright Joe Security LLC 2021

Analysis Process: sora.arm7 PID: 5391 Parent PID: 5378

General

Start time:	03:56:09
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5392 Parent PID: 5378

General

Start time:	03:56:09
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5380 Parent PID: 5375

General

Start time:	03:56:04
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5381 Parent PID: 5375

General

Start time:	03:56:04
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5243 Parent PID: 5240

General

Start time:	03:53:02
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Copyright Joe Security LLC 2021

Analysis Process: sora.arm7 PID: 5245 Parent PID: 5240

General

Start time:	03:53:02
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5248 Parent PID: 5245

General

Start time:	03:53:02
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: sora.arm7 PID: 5385 Parent PID: 5248

General

Start time:	03:56:04
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5387 Parent PID: 5248

General

Start time:	03:56:04
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5249 Parent PID: 5245

General

Start time:	03:53:02
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sora.arm7 PID: 5252 Parent PID: 5245

General

Start time:	03:53:02
Start date:	10/11/2021
Path:	/tmp/sora.arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5273 Parent PID: 1

General

Start time:	03:53:16
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5273 Parent PID: 1

General

Start time:	03:53:16
Start date:	10/11/2021
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: 5274 Parent PID: 1

General

Start time:	03:53:16
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

Copyright Joe Security LLC 2021

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5274 Parent PID: 1

General

Start time:	03:53:16
Start date:	10/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Copyright Joe Security LLC 2021