ID: 513591
Sample Name: sora.mips
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:17:27
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

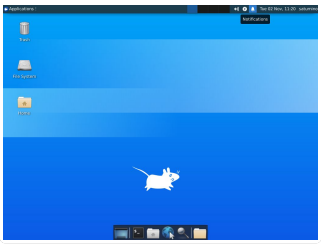
Linux Analysis Report sora.mips

Overview

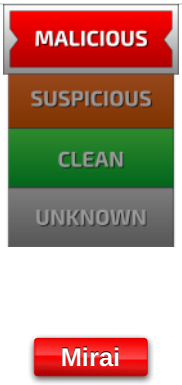
General Information

Sample Name:	sora.mips
Analysis ID:	513591
MD5:	f541ee6ca94d92d.
SHA1:	46100ebb28ef32d.
SHA256:	119853ec87c7bc…
Infos:	

Most interesting Screenshot:



Detection



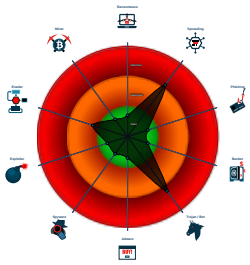
Mirai

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 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:	34.0.0 Boulder Opal
Analysis ID:	513591
Start date:	02.11.2021
Start time:	11:17:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sora.mips
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.spre.troj.linMIPS@0/6@0/0
Warnings:	Show All

Process Tree

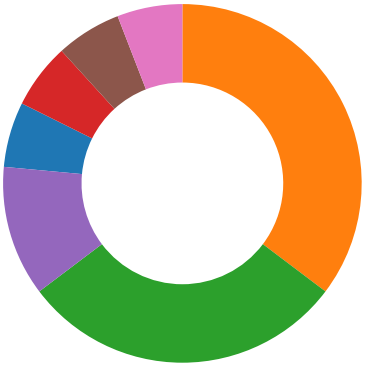
- **system is lnxubuntu20**
  - sora.mips (PID: 5235, Parent: 5111, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/sora.mips
    - sora.mips New Fork (PID: 5237, Parent: 5235)
    - sora.mips New Fork (PID: 5238, Parent: 5235)
    - sora.mips New Fork (PID: 5239, Parent: 5235)
      - sora.mips New Fork (PID: 5243, Parent: 5239)
      - sora.mips New Fork (PID: 5245, Parent: 5239)
      - sora.mips New Fork (PID: 5247, Parent: 5239)
- systemd New Fork (PID: 5275, Parent: 1)
  - sshd (PID: 5275, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5276, Parent: 1)
  - sshd (PID: 5276, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5386, Parent: 1)
  - sshd (PID: 5386, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5387, Parent: 1)
  - sshd (PID: 5387, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5390, Parent: 1)
  - sshd (PID: 5390, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5391, Parent: 1)
  - sshd (PID: 5391, 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
- 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)

System Summary:

Sample tries to kill many processes (SIGKILL)

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

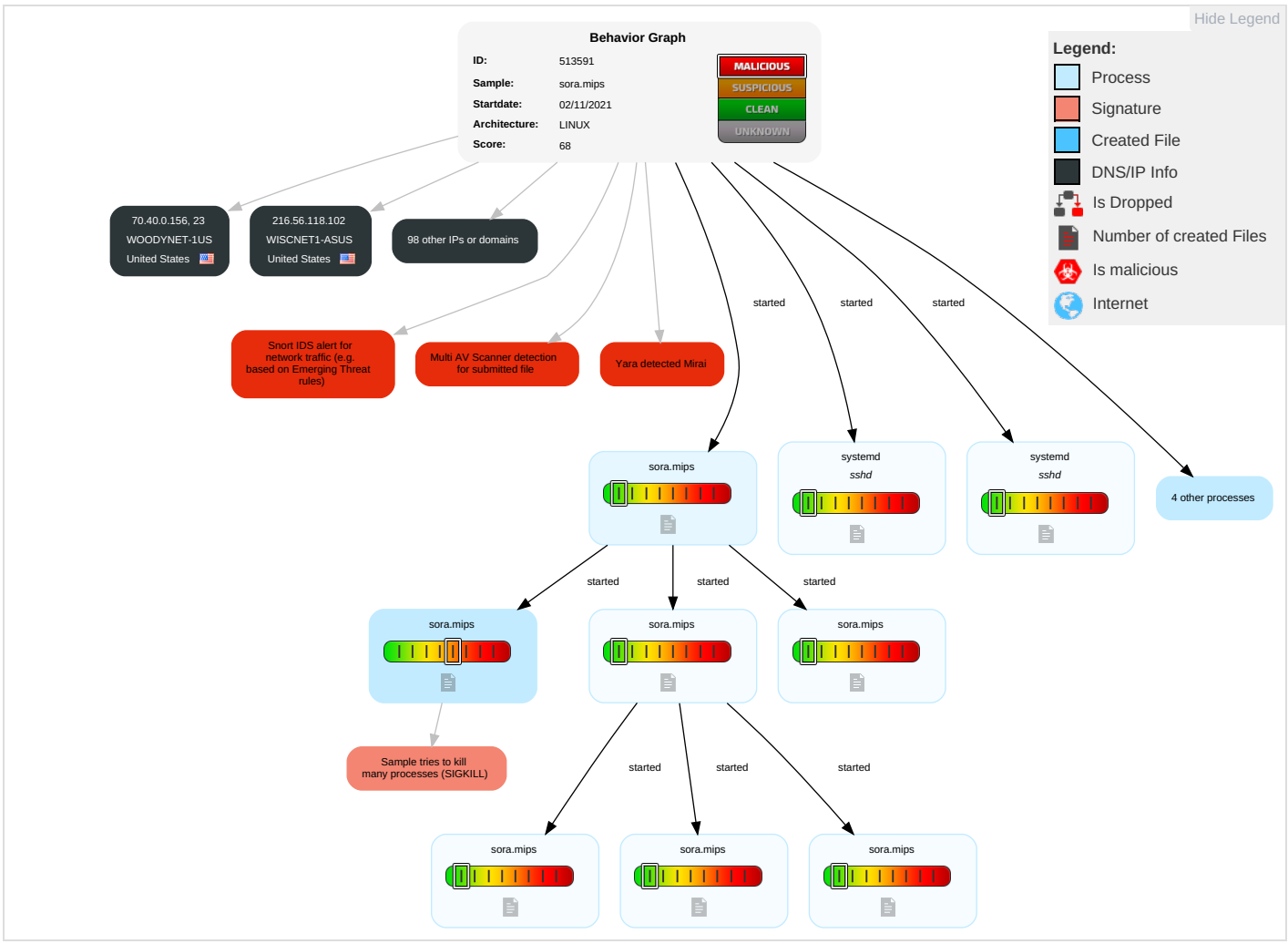
Mitre Att&ck Matrix

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	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

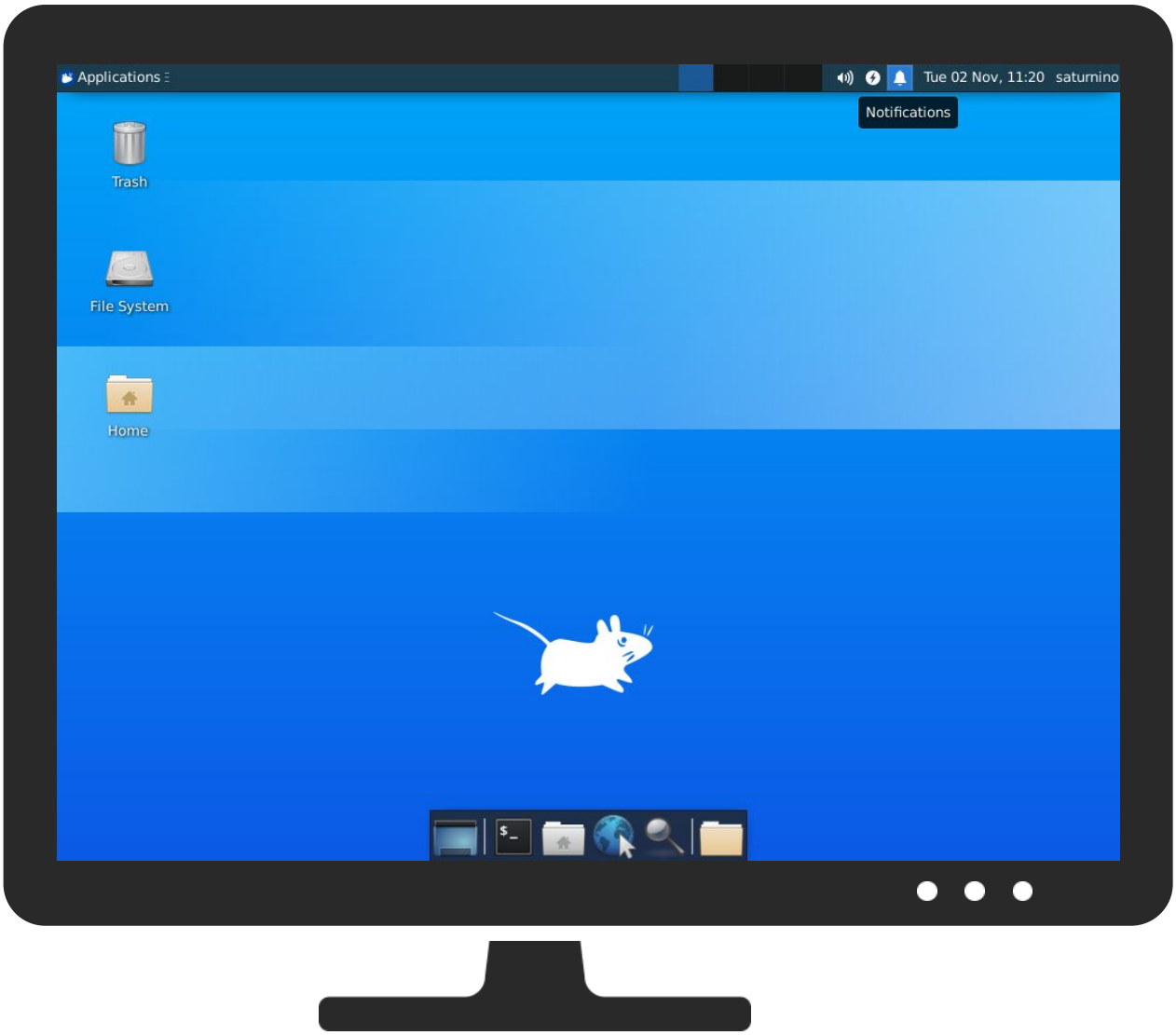
Behavior Graph



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.mips	52%	Virustotal		Browse
sora.mips	56%	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

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
71.107.202.139	unknown	United States		701	UUNETUS	false
80.24.160.20	unknown	Spain		3352	TELEFONICA_DE_ESPANA ES	false
70.40.0.156	unknown	United States		42	WOODYNET-1US	false
78.227.140.86	unknown	France		12322	PROXADFR	false
67.57.110.53	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
91.174.80.19	unknown	France		12322	PROXADFR	false
172.246.244.217	unknown	United States		18978	ENZUINC-US	false
245.171.55.96	unknown	Reserved		unknown	unknown	false
63.148.160.73	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
142.245.30.182	unknown	Canada		19416	RBC-NYUS	false
255.148.57.230	unknown	Reserved		unknown	unknown	false
111.6.69.190	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
31.137.239.105	unknown	Netherlands		15480	VFNL-ASVodafoneNLAutonomousSystemNL	false
34.229.108.227	unknown	United States		14618	AMAZON-AESUS	false
24.64.127.6	unknown	Canada		6327	SHAWCA	false
76.8.118.210	unknown	Canada		25636	ONTL-2002CA	false
203.176.190.38	unknown	Pakistan		45195	CDCPAK-PKCDCHouse99-BBlockBPK	false
41.193.111.37	unknown	South Africa		11845	Vox-TelecomZA	false
59.109.98.212	unknown	China		18245	FOUNDERBNCNNICCN	false
121.77.143.181	unknown	China		9812	CNNIC-CN-COLNETOrientalCableNetworkCoLtdCN	false
254.167.189.62	unknown	Reserved		unknown	unknown	false
241.15.185.185	unknown	Reserved		unknown	unknown	false
120.224.137.159	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	false
44.96.244.86	unknown	United States		7377	UCSDUS	false
114.37.39.155	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
37.91.93.228	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
149.150.154.242	unknown	United States		2494	MUWNETMUWNETAutonomousSystemAT	false
248.155.90.26	unknown	Reserved		unknown	unknown	false
31.31.135.149	unknown	Belgium		199095	CITYMESH-ASBE	false
251.82.161.94	unknown	Reserved		unknown	unknown	false
167.238.223.149	unknown	United States		36092	CENTENEUS	false
153.128.122.143	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
151.142.10.141	unknown	United States		10967	HOMEDEPOTNETUS	false
158.73.140.99	unknown	United States		19050	TIC-DHHS-INTERIORUS	false
64.28.69.73	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
106.128.236.235	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
140.210.162.31	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
216.81.240.141	unknown	United States		11320	LIGHTEDGE-AS-02US	false
200.172.238.27	unknown	Brazil		4230	CLAROSABR	false
95.121.137.238	unknown	Spain		3352	TELEFONICA_DE_ESPANA ES	false
17.160.100.84	unknown	United States		714	APPLE-ENGINEERINGUS	false
164.183.202.166	unknown	United States		37717	EL-KhawarizmiTN	false
240.85.62.5	unknown	Reserved		unknown	unknown	false
104.35.143.179	unknown	United States		20001	TWC-20001-PACWESTUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
175.34.81.13	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
16.229.239.174	unknown	United States		unknown	unknown	false
86.90.140.115	unknown	Netherlands		1136	KPNKPNNationalEU	false
43.112.78.251	unknown	Japan		4249	LILLY-ASUS	false
255.123.99.53	unknown	Reserved		unknown	unknown	false
195.20.246.157	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
36.132.101.91	unknown	China		56044	CMNET-AS-LIAONINGChinaMobilecommunicationscorporationC	false
191.254.53.60	unknown	Brazil		27699	TELEFONICABRASILSABR	false
45.124.201.45	unknown	Australia		134067	UNITI-AS-APUnitiWirelessPtyLtdAU	false
163.40.82.221	unknown	United States		226	LOS-NETTOS-ASUS	false
96.201.7.12	unknown	United States		7922	COMCAST-7922US	false
189.181.178.68	unknown	Mexico		8151	UninetSAdeCVMX	false
57.147.55.165	unknown	Belgium		2686	ATGS-MMD-ASUS	false
92.233.183.89	unknown	United Kingdom		5089	NTLGB	false
244.107.176.234	unknown	Reserved		unknown	unknown	false
246.55.8.155	unknown	Reserved		unknown	unknown	false
96.38.83.249	unknown	United States		20115	CHARTER-20115US	false
120.1.84.157	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
60.6.178.183	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
172.74.68.185	unknown	United States		11426	TWC-11426-CAROLINASUS	false
245.166.238.106	unknown	Reserved		unknown	unknown	false
112.251.95.212	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
210.110.112.139	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
169.164.169.125	unknown	United States		37611	AfrihostZA	false
68.144.38.185	unknown	Canada		6327	SHAWCA	false
12.69.103.16	unknown	United States		7018	ATT-INTERNET4US	false
255.96.93.6	unknown	Reserved		unknown	unknown	false
136.254.214.173	unknown	United States		72	SCHLUMBERGER-ASUS	false
219.69.54.175	unknown	Taiwan; Republic of China (ROC)		9416	MULTIMEDIA-AS-APHoshinMultimediaCenterIncTW	false
90.142.192.22	unknown	Sweden		1257	TELE2EU	false
99.215.192.252	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
167.134.52.44	unknown	Venezuela		10405	UPRR-ASN-01US	false
189.194.242.73	unknown	Mexico		13999	MegaCableSAdeCVMX	false
90.35.131.168	unknown	France		3215	FranceTelecom-OrangeFR	false
205.182.104.37	unknown	United States		3356	LEVEL3US	false
250.109.197.189	unknown	Reserved		unknown	unknown	false
157.204.30.231	unknown	United States		54216	GORE-NETWORKUS	false
167.234.69.231	unknown	United States		3525	ALBERTSONSUS	false
83.97.114.71	unknown	Germany		209854	SURFSHARKVG	false
142.67.215.102	unknown	Canada		22636	NOVA-SCOTIA-POWERCA	false
159.206.56.242	unknown	Canada		16793	DATA-TRONICSUS	false
80.110.234.46	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
83.208.201.84	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	false
102.236.71.235	unknown	unknown		36926	CKL1-ASNKE	false
65.1.40.107	unknown	United States		16509	AMAZON-02US	false
172.116.65.63	unknown	United States		20001	TWC-20001-PACWESTUS	false
151.158.166.126	unknown	unknown		205664	VATTENFALL-ABSE	false
216.56.118.102	unknown	United States		2381	WISCNET1-ASUS	false
67.211.159.82	unknown	United States		26161	TMEIC-AUS	false
250.85.29.212	unknown	Reserved		unknown	unknown	false
13.176.170.242	unknown	United States		7018	ATT-INTERNET4US	false
169.147.23.233	unknown	United States		11659	KUMCUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
53.99.133.165	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
174.146.255.210	unknown	United States		10507	SPCSUS	false
60.0.108.165	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
111.142.109.142	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false

Runtime Messages

Command:	/tmp/sora.mips
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
31.31.135.149	sora.arm	Get hash	malicious	Browse	
95.121.137.238	EtNIxD2GSD	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UUNETUS	arm5-20211102-0937	Get hash	malicious	Browse	• 193.99.20.99
	wNrhZyq41N	Get hash	malicious	Browse	• 71.245.10.212
	eFsSvDKams	Get hash	malicious	Browse	• 72.74.241.117
	KHSQ48GkGn	Get hash	malicious	Browse	• 207.24.250.131
	Hilix.arm	Get hash	malicious	Browse	• 173.70.19.34
	JVHk2b1Yd5	Get hash	malicious	Browse	• 108.54.12.29
	vRjXKh3l4n	Get hash	malicious	Browse	• 68.133.8.110
	WhFNix8BoE	Get hash	malicious	Browse	• 207.247.179.228
	wt5i2fAcF0	Get hash	malicious	Browse	• 65.233.206.198
	aTQ4RalkUs	Get hash	malicious	Browse	• 100.41.247.191
	o6aMoZKsIK	Get hash	malicious	Browse	• 208.192.217.76
	dUW6YG1Tdv	Get hash	malicious	Browse	• 210.80.9.164
	RPov9E0iot	Get hash	malicious	Browse	• 63.9.179.107
	8VANaS473t	Get hash	malicious	Browse	• 108.37.65.106
	uohdbohpYb	Get hash	malicious	Browse	• 207.24.67.100
	yVbcX1sEtS	Get hash	malicious	Browse	• 108.3.69.246
	8PRjJeUifB	Get hash	malicious	Browse	• 162.84.87.96
	SZAYTvvY9Y	Get hash	malicious	Browse	• 145.4.3.12
	1Y2rsDBP9s	Get hash	malicious	Browse	• 108.3.70.173
	Ko84iLip1u	Get hash	malicious	Browse	• 207.68.36.75
TELEFONICA_DE_ESPANAES	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	ydZLm6GD56	Get hash	malicious	Browse	• 88.28.74.111

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5276/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.

/proc/5387/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.

/proc/5391/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):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Dc2n:p
MD5:	EBC3FCE3183D08458EA683E4EA2AE38B
SHA1:	34674DDE2892AB7D2354F95DAB7D442B44E42431
SHA-256:	60015F8BF398A9443CACC8139E72C56EF7B5DCCA1518B134617D7EC546BFF5F2
SHA-512:	6C626D79B58FD4C023DBDB3018EC06C5D78E75D2D79C210138A8F8C02A18C619DB798AD163E3827A4BCCC80919827B6DD57C23B812CADFD821A9E899DAE38AB
Malicious:	false
Reputation:	low
Preview:	5391.

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.296543702857597
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	sora.mips
File size:	71764
MD5:	f541ee6ca94d92d5c8da35fce228bb46
SHA1:	46100ebb28ef32d9895277b26db0705cdb4a5729
SHA256:	119853ec87c7bc15674fa8beaf375979d963c5fd763d08a32ef555041e053d04
SHA512:	8efd86b742eaf71e845f4abe47282f993fd62c4d45c4fd63b8f1ac9014a8a7c3e04242f1ecb292256ce38c36b3354ac1ceb15f86da52870fc501cb6e9921d914
SSDEEP:	1536:WkvDSnAd6mYoPdd8QVs1o0vB1tA0iLuYw2+O/8p:WkLSA3vbko0pTAmYw2+OEp
File Content Preview:	.ELF.....@.`...4...L....4. ...(.....@...@.....E...E.....dt.Q.....<...'....!'.....<...'.....!.. ....'9... .....<...'.....!.....'9.

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)

ELF header

Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	71244
Section Header Size:	40
Number of Section Headers:	13
Header String Table Index:	12

Sections

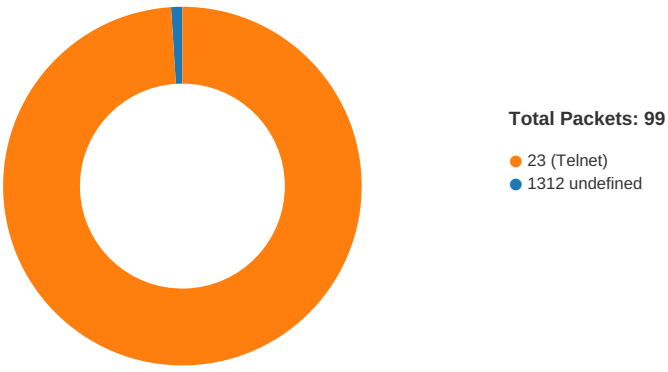
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0xffe0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x410100	0x10100	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x410160	0x10160	0x660	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x451000	0x11000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x451008	0x11008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x451020	0x11020	0x190	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4511b0	0x111b0	0x444	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x4515f4	0x115f4	0x24	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x451620	0x115f4	0x2a0	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x72c	0x115f4	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x115f4	0x57	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	0x400000	0x400000	0x107c0	0x107c0	3.3492	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x11000	0x451000	0x451000	0x5f4	0x8c0	1.8117	0x6	RW	0x10000		.ctors .dtors .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: sora.mips PID: 5235 Parent PID: 5111

General

Start time:	11:18:13
Start date:	02/11/2021
Path:	/tmp/sora.mips
Arguments:	/tmp/sora.mips
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: sora.mips PID: 5237 Parent PID: 5235

General

Start time:	11:18:13
Start date:	02/11/2021
Path:	/tmp/sora.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: sora.mips PID: 5238 Parent PID: 5235

General

Start time:	11:18:13
Start date:	02/11/2021
Path:	/tmp/sora.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sora.mips PID: 5239 Parent PID: 5235

General

Start time:	11:18:13
Start date:	02/11/2021
Path:	/tmp/sora.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sora.mips PID: 5243 Parent PID: 5239

General

Start time:	11:18:13
Start date:	02/11/2021
Path:	/tmp/sora.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: sora.mips PID: 5245 Parent PID: 5239

General

Start time:	11:18:14
Start date:	02/11/2021
Path:	/tmp/sora.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: sora.mips PID: 5247 Parent PID: 5239

General

Start time:	11:18:14
Start date:	02/11/2021
Path:	/tmp/sora.mips
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: systemd PID: 5275 Parent PID: 1

General

Start time:	11:18:26
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5275 Parent PID: 1

General

Start time:	11:18:26
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: 5276 Parent PID: 1

General

Start time:	11:18:27
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5276 Parent PID: 1

General

Start time:	11:18:27
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

Analysis Process: systemd PID: 5386 Parent PID: 1

General

Start time:	11:21:08

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

Analysis Process: sshd PID: 5386 Parent PID: 1

General

Start time:	11:21:08
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: 5387 Parent PID: 1

General

Start time:	11:21:09
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5387 Parent PID: 1

General

Start time:	11:21:09
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

Analysis Process: systemd PID: 5390 Parent PID: 1

General

Start time:	11:21:11
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5390 Parent PID: 1

General

Start time:	11:21:11
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: 5391 Parent PID: 1

General

Start time:	11:21:11
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5391 Parent PID: 1

General

Start time:	11:21:11
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