ID: 513641
Sample Name: sora.x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 12:12:50
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

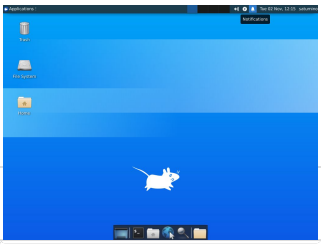
Linux Analysis Report sora.x86

Overview

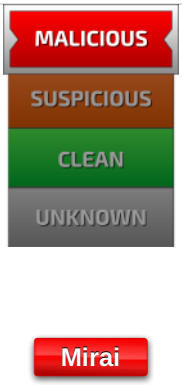
General Information

Sample Name:	sora.x86
Analysis ID:	513641
MD5:	ec0785f99de2a1e.
SHA1:	bdabfc4ef8c6e05..
SHA256:	30ad105f506c59e.
Tags:	Mirai
Infos:	

Most interesting Screenshot:



Detection

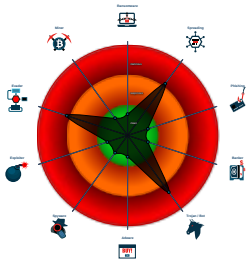


Score:	76
Range:	0 - 100
Whitelisted:	false

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 tries to kill many processes...
- Sample contains only a LOAD segm...
- 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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	513641
Start date:	02.11.2021
Start time:	12:12:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sora.x86
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:	mal76.spre.troj.evad.linX86@0/6@0/0
Warnings:	Show All

Process Tree

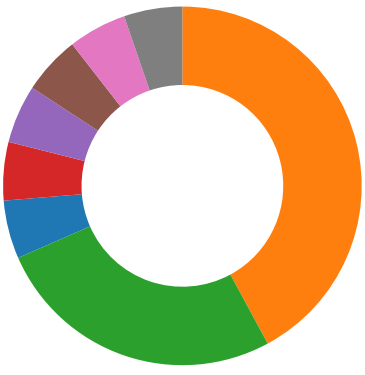
- **system is lnxubuntu20**
  - sora.x86 (PID: 5233, Parent: 5111, MD5: ec0785f99de2a1ea900d48a9bb26bf1c) Arguments: /tmp/sora.x86
    - sora.x86 New Fork (PID: 5234, Parent: 5233)
      - sora.x86 New Fork (PID: 5389, Parent: 5234)
      - sora.x86 New Fork (PID: 5390, Parent: 5234)
        - sora.x86 New Fork (PID: 5391, Parent: 5390)
          - sora.x86 New Fork (PID: 5401, Parent: 5391)
          - sora.x86 New Fork (PID: 5402, Parent: 5391)
        - sora.x86 New Fork (PID: 5392, Parent: 5390)
        - sora.x86 New Fork (PID: 5393, Parent: 5390)
    - sora.x86 New Fork (PID: 5235, Parent: 5233)
    - sora.x86 New Fork (PID: 5236, Parent: 5233)
      - sora.x86 New Fork (PID: 5237, Parent: 5236)
        - sora.x86 New Fork (PID: 5381, Parent: 5237)
        - sora.x86 New Fork (PID: 5382, Parent: 5237)
      - sora.x86 New Fork (PID: 5238, Parent: 5236)
      - sora.x86 New Fork (PID: 5239, Parent: 5236)
- systemd New Fork (PID: 5266, Parent: 1)
  - sshd (PID: 5266, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5267, Parent: 1)
  - sshd (PID: 5267, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5375, Parent: 1)
  - sshd (PID: 5375, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5376, Parent: 1)
  - sshd (PID: 5376, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5379, Parent: 1)
  - sshd (PID: 5379, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5380, Parent: 1)
  - sshd (PID: 5380, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

System Summary:

Sample tries to kill many processes (SIGKILL)

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

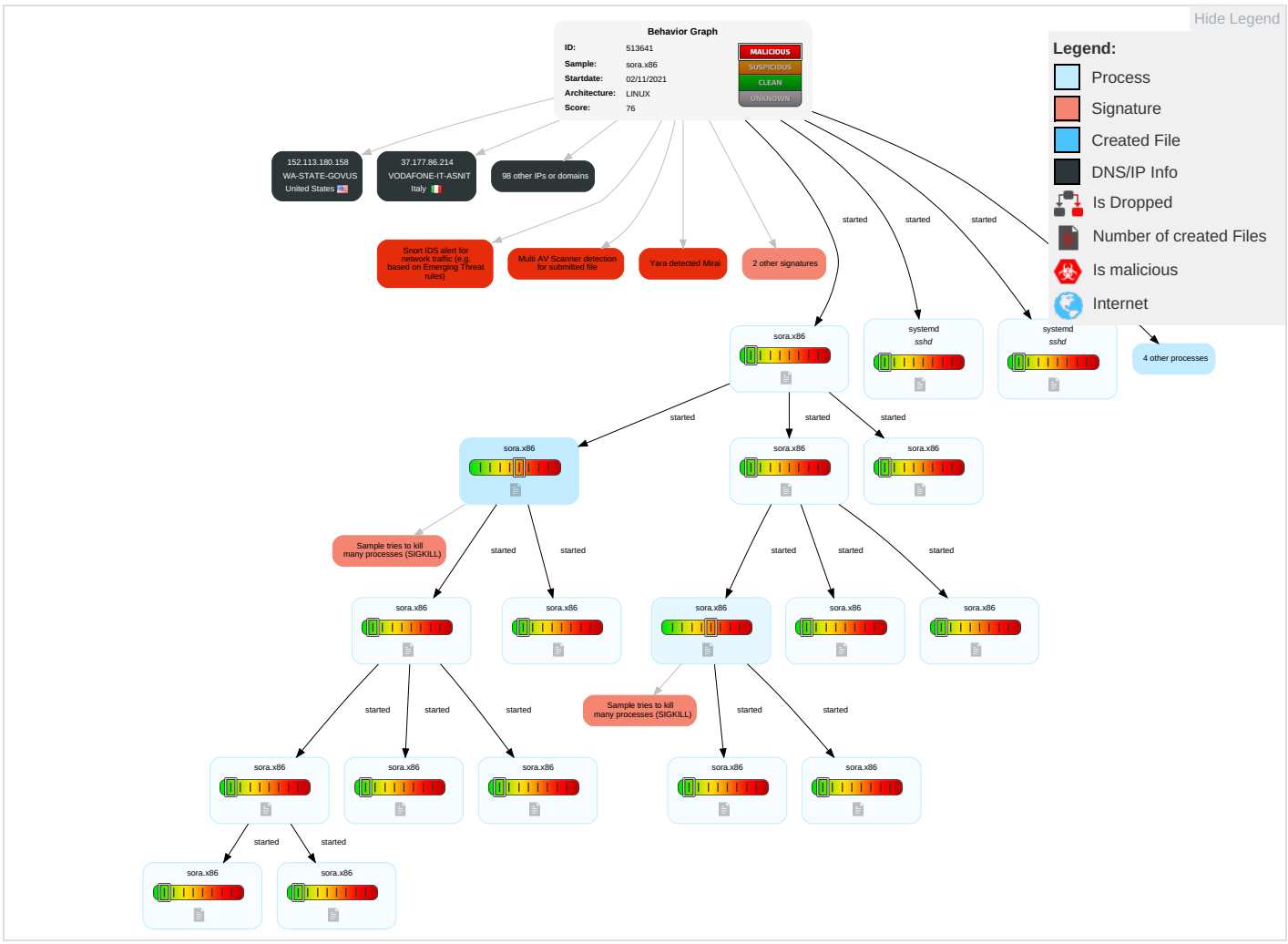
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated Files or Information 1	OS Credential Dumping 1	System Service Discovery	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 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	Non-Standard Port 1 1	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	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

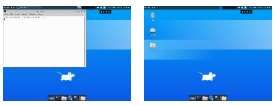
Behavior Graph

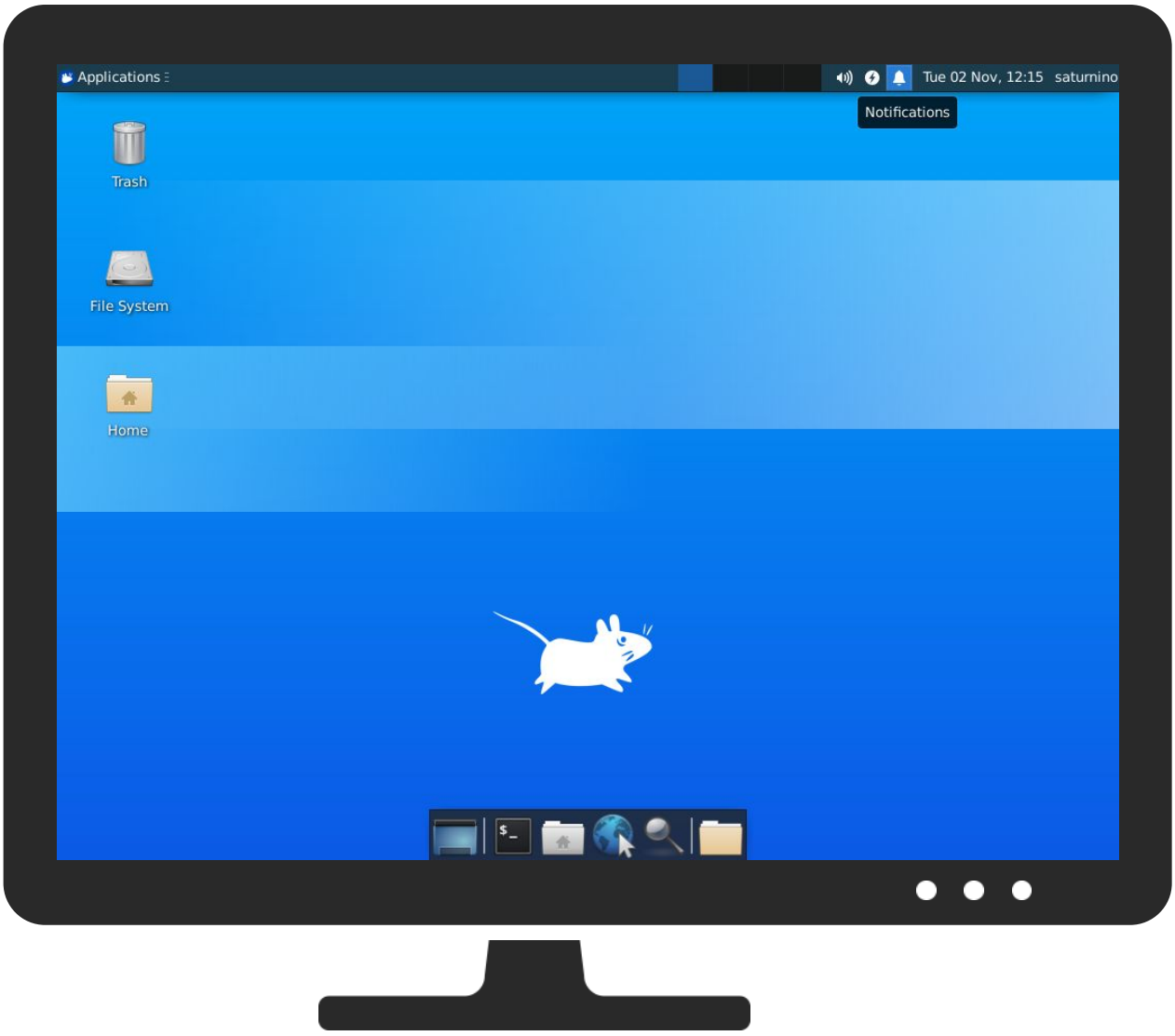


Screenshots

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.x86	38%	Virustotal		Browse
sora.x86	47%	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
165.14.150.75	unknown	Japan		18271	EVONETSojitzSystemsCorporationJP	false
2.98.202.30	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
1.241.64.41	unknown	Korea Republic of		38408	GOEAY-AS-KRGYEONGGIPROVINCIALANYANGOFFICEOFEDUCATION	false
126.27.223.237	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
167.244.146.157	unknown	United States		13325	STOMIUS	false
148.49.170.205	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
37.177.86.214	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
59.166.102.220	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
44.7.130.188	unknown	United States		7377	UCSDUS	false
113.54.159.201	unknown	China		24355	CNGI-CD-IX-AS-APCERNET2IXatUniversityofElectronicScie	false
146.15.235.153	unknown	United States		1467	DNIC-ASBLK-01467-01468US	false
166.203.133.216	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
251.188.124.239	unknown	Reserved		unknown	unknown	false
210.85.191.211	unknown	Taiwan; Republic of China (ROC)		7482	APOL-ASAsiaPacificOnlineServiceIncTW	false
204.62.73.110	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
114.239.158.155	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
41.14.214.51	unknown	South Africa		29975	VODACOM-ZA	false
113.124.222.249	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
210.110.95.218	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
162.30.206.148	unknown	United States		46483	RGHSUS	false
177.70.141.190	unknown	Brazil		266555	ISPNETTELECOMUNICACOESLTDA-EPPBR	false
219.240.106.33	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
172.215.195.50	unknown	United States		18747	IFX18747US	false
201.240.238.10	unknown	Peru		6147	TelefonicadelPeruSAAPE	false
31.67.116.133	unknown	United Kingdom		12576	EELtdGB	false
71.111.121.46	unknown	United States		701	UUNETUS	false
88.248.29.110	unknown	Turkey		9121	TTNETTR	false
38.93.85.255	unknown	United States		174	COGENT-174US	false
41.115.200.72	unknown	South Africa		16637	MTNNS-ASZA	false
4.54.18.94	unknown	United States		3356	LEVEL3US	false
16.85.71.175	unknown	United States		unknown	unknown	false
74.33.14.3	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
218.21.160.20	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
147.175.253.12	unknown	Slovakia (SLOVAK Republic)		2607	SANETSlovakAcademicNetworkSK	false
159.114.114.114	unknown	United Kingdom		32982	DOE-HQUS	false
18.68.25.132	unknown	United States		3	MIT-GATEWAYSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
133.80.8.221	unknown	Japan		55904	KOGAKUIN-ASKOGAKUINUniversityJP	false
118.14.181.61	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
119.59.136.138	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
24.150.2.237	unknown	Canada		7992	COGECOWAVECA	false
103.190.121.18	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
126.109.127.55	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
66.210.247.106	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
152.113.180.158	unknown	United States		4193	WA-STATE-GOVUS	false
121.81.167.8	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
12.10.152.124	unknown	United States		7018	ATT-INTERNET4US	false
217.4.22.110	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
44.100.131.207	unknown	United States		7377	UCSDUS	false
14.98.128.139	unknown	India		45820	TTSL-MEISISPTataTeleservicesISPASIN	false
20.95.97.146	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
1.109.50.131	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
68.15.246.54	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
59.121.20.32	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
34.26.63.252	unknown	United States		2686	ATGS-MMD-ASUS	false
92.203.254.252	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporationJP	false
97.110.251.226	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
203.175.188.145	unknown	Korea Republic of		9693	KFTCCA-ASKFTCKR	false
65.29.134.160	unknown	United States		10796	TWC-10796-MIDWESTUS	false
1.253.209.220	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
72.187.61.178	unknown	United States		33363	BHN-33363US	false
221.232.6.12	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
200.103.220.0	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
86.14.157.185	unknown	United Kingdom		5089	NTLGB	false
248.243.251.91	unknown	Reserved		unknown	unknown	false
213.29.127.118	unknown	Czech Republic		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
247.120.54.225	unknown	Reserved		unknown	unknown	false
101.163.182.162	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
191.234.39.21	unknown	Brazil		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
152.160.245.116	unknown	United States		54163	AHOSTINGUS	false
220.158.204.12	unknown	Bangladesh		134712	PIPEXNETWORK-BDPipexNetworkBD	false
192.198.234.232	unknown	United States		53468	FWLUS	false
73.94.134.111	unknown	United States		7922	COMCAST-7922US	false
251.234.221.195	unknown	Reserved		unknown	unknown	false
102.174.105.188	unknown	Tunisia		37693	TUNISIANATN	false
252.43.179.218	unknown	Reserved		unknown	unknown	false
13.233.103.202	unknown	United States		16509	AMAZON-02US	false
46.142.137.7	unknown	Germany		8881	VERSATELDE	false
90.134.166.190	unknown	Sweden		1257	TELE2EU	false
110.167.231.74	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.26.2.148	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
179.227.126.169	unknown	Brazil		26599	TELEFONICABRASILSABR	false
103.57.64.14	unknown	unknown		134179	RWN-AS-APRealWorldNetworksPtyLtdAU	false
94.16.9.82	unknown	Germany		42360	SSP-EUROPEpoweredbyANXDE	false
27.160.78.186	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
200.226.149.233	unknown	Brazil		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
16.97.163.5	unknown	United States		unknown	unknown	false
42.198.166.181	unknown	China		7497	CSTNET-AS-APComputerNetworkInformationCenterCN	false
71.112.18.152	unknown	United States		701	UUNETUS	false
112.219.5.116	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
59.28.140.225	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
158.198.246.29	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
254.122.33.192	unknown	Reserved		unknown	unknown	false
87.180.143.9	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
45.49.77.34	unknown	United States		20001	TWC-20001-PACWESTUS	false
153.49.4.136	unknown	United States		1226	CTA-42-AS1226US	false
98.39.201.51	unknown	United States		7922	COMCAST-7922US	false
110.203.9.8	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
146.20.63.85	unknown	United States		27357	RACKSPACEUS	false
96.59.177.46	unknown	United States		33363	BHN-33363US	false
70.84.162.139	unknown	United States		36351	SOFTLAYERUS	false

Runtime Messages

Command:	/tmp/sora.x86
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
EVONETSojitzSystemsCorporationJP	sora.arm7	Get hash	malicious	Browse	• 165.14.149.81
	4syAQhYxm8	Get hash	malicious	Browse	• 165.14.198.42
	sora.arm7	Get hash	malicious	Browse	• 165.14.73.241
	sora.arm7	Get hash	malicious	Browse	• 165.14.198.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	qJvDfzBXbs	Get hash	malicious	Browse	• 165.14.137.77
	wnwO8B1Wuy	Get hash	malicious	Browse	• 165.14.198.25
	AJK7j832D2	Get hash	malicious	Browse	• 165.14.150.39
	GMgREghUds	Get hash	malicious	Browse	• 165.14.160.111
	tMA66IeqHu	Get hash	malicious	Browse	• 165.14.168.212
	Vs7Vm7J1TR	Get hash	malicious	Browse	• 165.14.198.59
	ppc_unpacked	Get hash	malicious	Browse	• 165.14.174.79
OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	wt5i2fAcF0	Get hash	malicious	Browse	• 78.145.16.154
	8PRjJeUifB	Get hash	malicious	Browse	• 92.18.133.105
	Ko84iLip1u	Get hash	malicious	Browse	• 92.3.236.146
	S8G5z3pdHw	Get hash	malicious	Browse	• 92.24.64.128
	mP1pg0ryFA	Get hash	malicious	Browse	• 2.100.134.151
	032k4JmR0U	Get hash	malicious	Browse	• 92.13.106.251
	x86	Get hash	malicious	Browse	• 2.97.101.112
	T0uznhDXKw	Get hash	malicious	Browse	• 92.29.90.175
	ev1JsPbdMA	Get hash	malicious	Browse	• 92.24.16.217
	apep.arm	Get hash	malicious	Browse	• 92.7.19.93
	apep.x86	Get hash	malicious	Browse	• 92.16.44.106
	Ceji2MdFHD	Get hash	malicious	Browse	• 2.98.204.126
	Z7QqCH0bak	Get hash	malicious	Browse	• 92.14.197.224
	zouBbQwUTb	Get hash	malicious	Browse	• 92.24.15.58
	jJ6GK5qbZt	Get hash	malicious	Browse	• 92.26.100.228
	LCgNoeCOl6	Get hash	malicious	Browse	• 92.18.133.136
	x86_64	Get hash	malicious	Browse	• 2.98.162.217
	apep.x86	Get hash	malicious	Browse	• 92.24.40.60
	yOtRXukeq9	Get hash	malicious	Browse	• 92.21.79.215
	b3astmode.x86	Get hash	malicious	Browse	• 78.146.187.95
GOEAY-AS-KRGYEONGGIPROVINCIALANYANGOFFICEOFEDUCATION	ivImhRZqGa	Get hash	malicious	Browse	• 1.241.39.53
	dAhGa49Lql	Get hash	malicious	Browse	• 1.241.41.126
	qINZ8rxy9S	Get hash	malicious	Browse	• 61.77.19.135
	22kfSzInJi	Get hash	malicious	Browse	• 1.241.39.66
	O1qCIp2iQS	Get hash	malicious	Browse	• 1.241.64.50
	l6zn4l2gR0	Get hash	malicious	Browse	• 1.241.64.38
	WdyAWwF87e	Get hash	malicious	Browse	• 1.241.64.43

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5267/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/5376/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:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 -1000.

/proc/5380/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:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
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:DdVv:BVv
MD5:	2522E7CF829C2CEFC020B7B06A1C99C7
SHA1:	980DD56DC2FBFF129C6F3055C60599D46546A0B0
SHA-256:	E6CFA4E1AB3F5790C61A85FC6494DE44BB8D493753E3E3C31771A9C9AA7D1FB4
SHA-512:	DA266D5D96070400172644D2650ACF3EC3F52F48C1558C519E0A218A93B457B569B11917DD92C8B05144A79080BC53E1040576B0DC4E8D47B0AE4E0508CEA3E
Malicious:	false
Reputation:	low
Preview:	 5380.

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.8717761813776965
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	sora.x86
File size:	24728

General	
MD5:	ec0785f99de2a1ea900d48a9bb26bf1c
SHA1:	bdabfc4ef8c6e050ba2a88927ac9429bd71813c9
SHA256:	30ad105f506c59e85005c99f64fcfc577c2a51caf131bc9f57e5172a404654d3
SHA512:	4a3d6fba5292e86f1471b2d411954e950688522b891e6d827fd89aa621a087e953b544dd268aaacc9913807e036154568fb06115741ca71c85f8acb9d8e68cb1
SSDEEP:	384:M8DKKQOcRpmYLdn6RBOFRFt5rUFX1DiSllCo3AnupCFNqnrrd1NEZgO8UXWozPLu:R/QOC0Yhn6ROHWFlAcwNEFCnNBxcsce
File Content Preview:	.ELF.....g..4.....4. ...(....._..._.....W...W.....Q.td.....tUPX!.....Z.....?d..ELF.....d.....4.,..4. (.....k.-.#.`.....?..P.....d..l

Static ELF Info

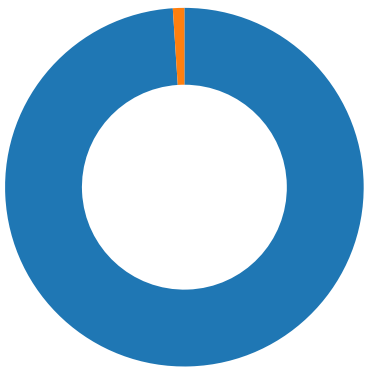
ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0xc067a0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number 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	0xc01000	0xc01000	0x5f9b	0x5f9b	4.5556	0x5	R E	0x1000		
LOAD	0x700	0x8055700	0x8055700	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



Total Packets: 97

- 1312 undefined
- 23 (Telnet)

TCP Packets

System Behavior

Analysis Process: sora.x86 PID: 5233 Parent PID: 5111

General

Start time:	12:13:38
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	/tmp/sora.x86
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5234 Parent PID: 5233

General

Start time:	12:13:38
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

File Activities

File Read

Directory Enumerated

Analysis Process: sora.x86 PID: 5389 Parent PID: 5234

General

Start time:	12:16:46
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5390 Parent PID: 5234

General

Start time:	12:16:46
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes

MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5391 Parent PID: 5390

General

Start time:	12:16:46
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5401 Parent PID: 5391

General

Start time:	12:16:51
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5402 Parent PID: 5391

General

Start time:	12:16:51
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5392 Parent PID: 5390

General

Start time:	12:16:46
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5393 Parent PID: 5390

General

Start time:	12:16:46
Start date:	02/11/2021
Path:	/tmp/sora.x86

Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5235 Parent PID: 5233

General

Start time:	12:13:38
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5236 Parent PID: 5233

General

Start time:	12:13:38
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5237 Parent PID: 5236

General

Start time:	12:13:38
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

File Activities

File Read

Directory Enumerated

Analysis Process: sora.x86 PID: 5381 Parent PID: 5237

General

Start time:	12:16:33
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5382 Parent PID: 5237

General

Start time:	12:16:33
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5238 Parent PID: 5236

General

Start time:	12:13:38
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: sora.x86 PID: 5239 Parent PID: 5236

General

Start time:	12:13:38
Start date:	02/11/2021
Path:	/tmp/sora.x86
Arguments:	n/a
File size:	24728 bytes
MD5 hash:	ec0785f99de2a1ea900d48a9bb26bf1c

Analysis Process: systemd PID: 5266 Parent PID: 1

General

Start time:	12:13:49
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5266 Parent PID: 1

General

Start time:	12:13:49
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: 5267 Parent PID: 1

General

Start time:	12:13:50
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5267 Parent PID: 1

General

Start time:	12:13:50
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: 5375 Parent PID: 1

General

Start time:	12:16:26
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5375 Parent PID: 1

General

Start time:	12:16:26
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: 5376 Parent PID: 1

General

Start time:	12:16:27
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5376 Parent PID: 1

General

Start time:	12:16:27
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: 5379 Parent PID: 1

General

Start time:	12:16:29
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5379 Parent PID: 1

General

Start time:	12:16:29
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: 5380 Parent PID: 1

General

Start time:	12:16:29
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5380 Parent PID: 1

General

Start time:	12:16:29
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