ID: 519593
Sample Name: sora.mpsl
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 22:57:03
Date: 10/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

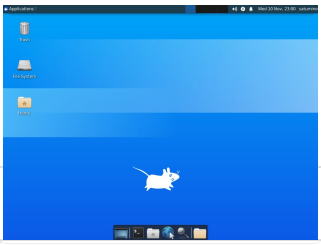
Linux Analysis Report sora.mpsl

Overview

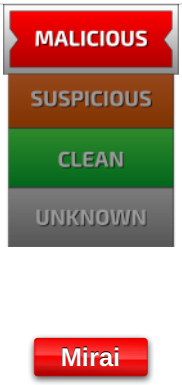
General Information

Sample Name:	sora.mpsl
Analysis ID:	519593
MD5:	42ac0f5f0fd0d4e…
SHA1:	12369aa6f5ffd2e…
SHA256:	2dfc8c4568d6a33..
Tags:	Mirai
Infos:	

Most interesting Screenshot:



Detection

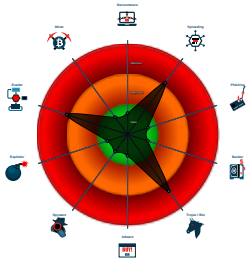


Score:	76
Range:	0 - 100
Whitelisted:	false

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…
- 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:	519593
Start date:	10.11.2021
Start time:	22:57:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sora.mpsl
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.linMPSL@0/2@0/0
Warnings:	Show All

Process Tree

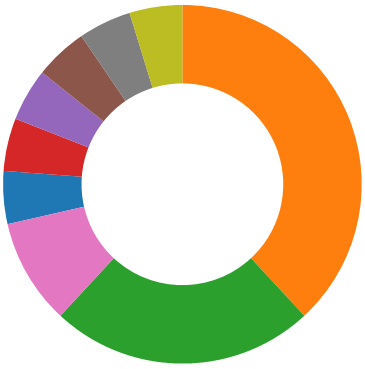
- **system is lnxubuntu20**
  - sora.mpsl (PID: 5240, Parent: 5118, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/sora.mpsl
    - sora.mpsl New Fork (PID: 5242, Parent: 5240)
    - sora.mpsl New Fork (PID: 5243, Parent: 5240)
    - sora.mpsl New Fork (PID: 5244, Parent: 5240)
      - sora.mpsl New Fork (PID: 5248, Parent: 5244)
      - sora.mpsl New Fork (PID: 5249, Parent: 5244)
      - sora.mpsl New Fork (PID: 5251, Parent: 5244)
  - systemd New Fork (PID: 5279, Parent: 1)
  - sshd (PID: 5279, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
  - systemd New Fork (PID: 5280, Parent: 1)
  - sshd (PID: 5280, 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
- 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)

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

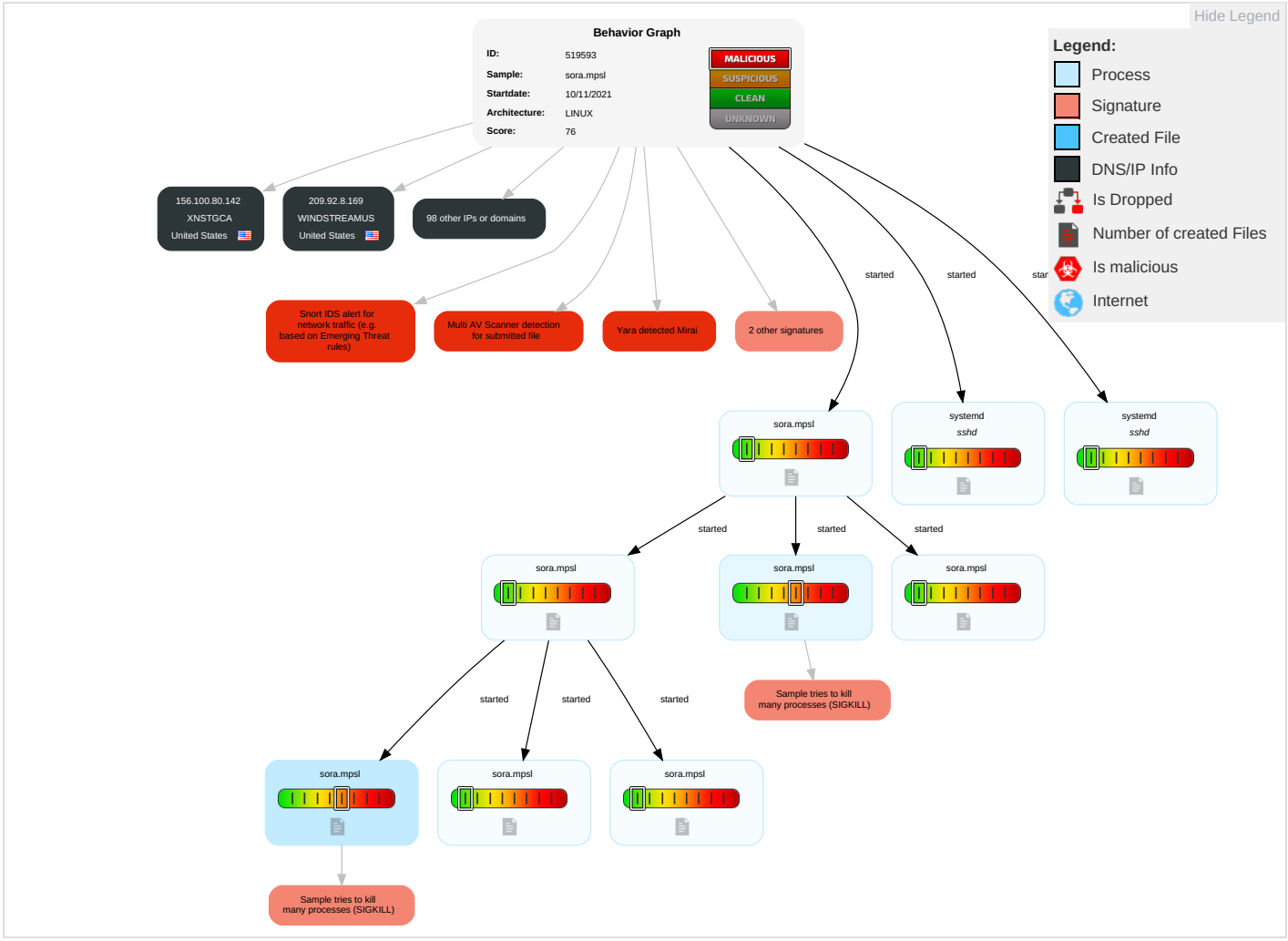
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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

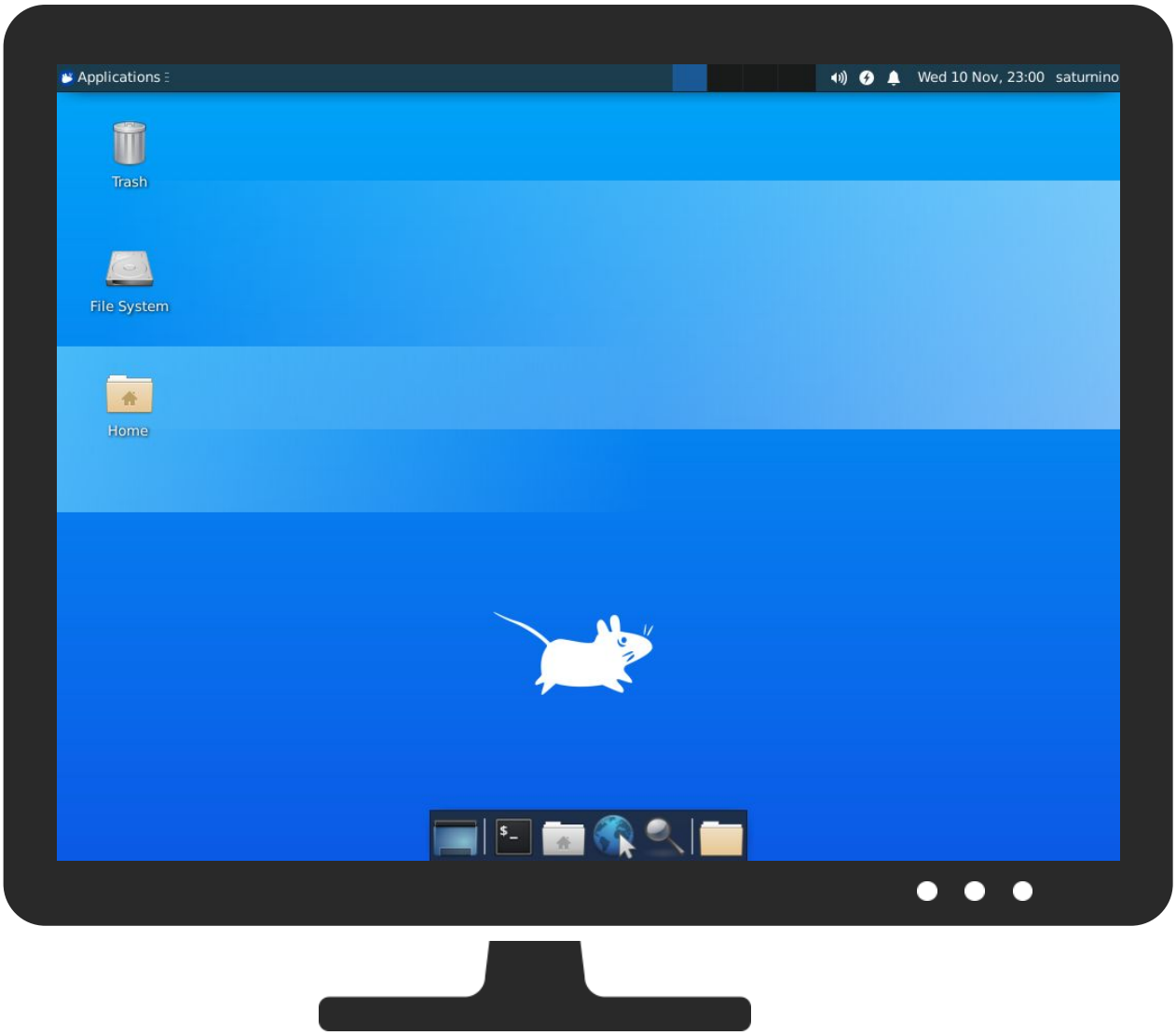
Behavior Graph



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.mpsl	39%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
148.57.98.39	unknown	United States		10753	LVLT-10753US	false
36.63.232.128	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
178.166.17.66	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	false
94.42.249.28	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
121.215.93.53	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
240.46.153.198	unknown	Reserved		unknown	unknown	false
202.126.161.125	unknown	Hong Kong		4637	ASN-TELSTRA-GLOBALTelstraGlobalHK	false
111.0.17.150	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
108.152.25.20	unknown	United States		16509	AMAZON-02US	false
141.205.80.8	unknown	United States		797	AMERITECH-ASUS	false
98.99.70.119	unknown	United States		62566	STARBUCKSUS	false
156.100.80.142	unknown	United States		393504	XNSTGCA	false
123.231.123.165	unknown	Sri Lanka		18001	DIALOG-ASDialogAxiataPLCLK	false
35.29.173.243	unknown	United States		36375	UMICH-AS-5US	false
108.17.85.21	unknown	United States		701	UUNETUS	false
222.226.56.23	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
94.62.51.199	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	false
148.129.11.201	unknown	United States		7764	CENSUSBUREAUUS	false
60.156.131.216	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
14.172.125.75	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
66.170.46.96	unknown	United States		16698	BRIGHTNETUS	false
121.98.221.38	unknown	New Zealand		9790	VOCUSGROUPNZVocusGroupNZ	false
44.80.188.194	unknown	United States		7377	UCSDUS	false
78.74.7.68	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
85.220.9.229	unknown	Iceland		6677	ICENET-AS1IS	false
79.149.221.198	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
116.31.232.129	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
209.92.8.169	unknown	United States		7029	WINDSTREAMUS	false
88.196.160.49	unknown	Estonia		3249	ESTPAKEE	false
165.104.225.187	unknown	United States		26305	ASN-SSMUS	false
204.120.93.14	unknown	United States		1239	SPRINTLINKUS	false
112.93.141.60	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
94.191.99.99	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
94.63.199.231	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	false
54.103.47.111	unknown	United States		16509	AMAZON-02US	false
160.38.70.93	unknown	United Kingdom		3450	UTKUS	false
68.54.35.217	unknown	United States		7922	COMCAST-7922US	false
202.65.72.220	unknown	Australia		38195	SUPERLOOP-AS-APSuperloopAU	false
1.45.25.239	unknown	China		45083	CHEERYZONEBeijingCheeryZoneScitechCoLtdCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
166.64.126.168	unknown	Australia		58681	NSWPOLSERV-AS-APNewSouthWalesPoliceAU	false
12.92.121.112	unknown	United States		7018	ATT-INTERNET4US	false
112.125.161.208	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
39.176.217.227	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
218.119.166.110	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
109.126.60.17	unknown	Russian Federation		42038	VLADLINK-ASRU	false
14.44.138.222	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
104.230.253.69	unknown	United States		10796	TWC-10796-MIDWESTUS	false
177.87.59.184	unknown	Brazil		262648	BRAVATELECOMUNICACOESPONTESELACERDALTDA-EPPBR	false
217.22.110.113	unknown	Spain		15711	IBERDROLABilbaoES	false
47.87.41.39	unknown	United States		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
65.66.253.159	unknown	United States		7018	ATT-INTERNET4US	false
112.96.183.188	unknown	China		17622	CNCGROUP-GZChinaUnicomGuangzhounetworkCN	false
102.136.132.185	unknown	Cote D'ivoire		36974	AFNET-ASCI	false
255.117.137.5	unknown	Reserved		unknown	unknown	false
242.184.151.122	unknown	Reserved		unknown	unknown	false
74.252.191.113	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
188.95.165.168	unknown	Saudi Arabia		34397	CYBERIA-RUHCyberiaRiyadhAutonomousSystemSA	false
191.237.129.95	unknown	Brazil		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
146.234.19.249	unknown	Germany		43857	FRAPORTDE	false
9.211.168.137	unknown	United States		3356	LEVEL3US	false
66.242.157.205	unknown	United States		13649	ASN-VINSUS	false
252.201.180.233	unknown	Reserved		unknown	unknown	false
146.153.203.105	unknown	United States		197938	TRAVIANGAMESDE	false
149.119.110.167	unknown	United States		11872	SYRACUSE-UNIVERSITYUS	false
85.138.67.230	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
191.80.153.165	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
116.204.165.44	unknown	Pakistan		23607	LEONET-AS-APLeoNetPvtLtdPK	false
5.101.107.41	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	false
221.83.33.106	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
24.71.77.191	unknown	Canada		6327	SHAWCA	false
193.252.45.35	unknown	France		3215	FranceTelecom-OrangeFR	false
32.93.232.170	unknown	United States		2686	ATGS-MMD-ASUS	false
243.100.129.203	unknown	Reserved		unknown	unknown	false
57.24.98.110	unknown	Belgium		2686	ATGS-MMD-ASUS	false
117.159.243.74	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
247.209.69.255	unknown	Reserved		unknown	unknown	false
160.247.147.135	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
93.126.14.252	unknown	Iran (ISLAMIC Republic Of)		44375	AISDPIR	false
190.95.251.255	unknown	Ecuador		27947	TelconetSAEC	false
62.222.102.220	unknown	Ireland		8918	CARRIER1-ASIE	false
178.161.16.206	unknown	Kuwait		42961	GPRS-ASZAINKW	false
89.246.41.40	unknown	Germany		8881	VERSATELDE	false
78.122.64.184	unknown	France		8228	CEGETEL-ASFR	false
23.68.48.214	unknown	United States		7922	COMCAST-7922US	false
65.133.167.221	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
164.137.70.99	unknown	United Kingdom		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
253.163.201.162	unknown	Reserved		unknown	unknown	false
101.79.180.5	unknown	Korea Republic of		38661	HCLC-AS-KRpurplestonesKR	false
208.98.29.101	unknown	United States		46844	ST-BGPUS	false
254.148.39.84	unknown	Reserved		unknown	unknown	false
198.164.10.40	unknown	Canada		395431	IGTCANSOLCA	false
183.183.7.155	unknown	Japan		45684	MIRAINETKyoceraCommunicationSystemsCoLtdJP	false
146.12.254.26	unknown	United States		197938	TRAVIANGAMESDE	false
199.45.249.232	unknown	United States		16618	FUC-AS-16618US	false
35.145.114.33	unknown	United States		394141	ROCKET-FIBERUS	false
63.154.17.178	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
118.117.199.51	unknown	China		139220	CHINANET-SICHUAN-CHUANXI-IDCSichuanChuanxnIDCCN	false
223.179.12.206	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
204.25.184.75	unknown	United States		13325	STOMIUS	false
158.30.134.23	unknown	United States		1504	DNIC-AS-01504US	false

Runtime Messages

Command:	/tmp/sora.mpsl
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
CHINANET-BACKBONENo31Jin-rongStreetCN	l0vNaPgd6f	Get hash	malicious	Browse	• 106.82.51.213
	8fVDxGRR8S	Get hash	malicious	Browse	• 121.234.206.186
	s36oh8l6l0	Get hash	malicious	Browse	• 59.48.199.216
	3ObdCtruss	Get hash	malicious	Browse	• 117.77.54.225
	uRQVqbl0sQ	Get hash	malicious	Browse	• 125.123.119.138
	63BjZ1IcIh	Get hash	malicious	Browse	• 1.193.195.217
	trynagetmybinsufucker98575.arm7	Get hash	malicious	Browse	• 183.151.71.1
	m-p.s-l.Sakura	Get hash	malicious	Browse	• 125.89.54.95
	QXFOZ3Cshc	Get hash	malicious	Browse	• 222.168.38.12
	sora.x86	Get hash	malicious	Browse	• 113.77.117.207
	sora.arm7	Get hash	malicious	Browse	• 182.98.40.207
	sora.arm	Get hash	malicious	Browse	• 182.244.34.68
	lDawzTbABc	Get hash	malicious	Browse	• 1.71.43.54
	DVHEnaPp2d	Get hash	malicious	Browse	• 119.126.143.146

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HwcNrhNfZg	Get hash	malicious	Browse	• 27.185.59.72
	X5bKvoLX1E	Get hash	malicious	Browse	• 42.203.201.215
	e9e6i5D2gK	Get hash	malicious	Browse	• 115.217.129.91
	19kG57P043	Get hash	malicious	Browse	• 123.175.36.144
	Smlp3eBtOI	Get hash	malicious	Browse	• 118.122.17.150
	eGH4d5FDoU	Get hash	malicious	Browse	• 27.28.94.97
LVLT-10753US	Kod7jprn7K.exe	Get hash	malicious	Browse	• 193.56.146.64
	44508.5578762732.dat.dll	Get hash	malicious	Browse	• 193.56.146.60
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 193.56.146.36
	2LG87UfOTH.exe	Get hash	malicious	Browse	• 193.56.146.64
	0A223AA68AF0C2AF0BAABDA61D82748629078720A017E.exe	Get hash	malicious	Browse	• 193.56.146.36
	951049989EB772C71EC4FA9F0685AB45CAE755CA5D34C.exe	Get hash	malicious	Browse	• 193.56.146.36
	C9DE02209482359466292BE7BC0464FC65037698B38C1.exe	Get hash	malicious	Browse	• 193.56.146.36
	setup_installer.exe	Get hash	malicious	Browse	• 193.56.146.36
	CB7D321954760DE22CCBF59ECE43D94E503350B18203D.exe	Get hash	malicious	Browse	• 193.56.146.36
	D1F610AF3C46FFF6C857BE0136C696604EB8E7466B4A7.exe	Get hash	malicious	Browse	• 193.56.146.36
	F1F6AEEE9A42004E68765A83E9CBD51BC878A0AFD7C80.exe	Get hash	malicious	Browse	• 193.56.146.36
	4Lkdxnkt9M.exe	Get hash	malicious	Browse	• 193.56.146.64
	22275B7C5A57111ACA919F6BBFAE171E5E99F5EF777D1.exe	Get hash	malicious	Browse	• 193.56.146.36
	4AE186F9A645695962B47F37C8B8E64C4D45F2B2A12AE.exe	Get hash	malicious	Browse	• 193.56.146.36
	O4eFetVyO4.exe	Get hash	malicious	Browse	• 193.56.146.36
	6PjJy5iOgU.exe	Get hash	malicious	Browse	• 193.56.146.36
	2FA81F4A4C64E5595C5D538062B4E8435E10FCCD9F81B.exe	Get hash	malicious	Browse	• 193.56.146.36
	t2E05q13ox.exe	Get hash	malicious	Browse	• 193.56.146.64
	I3O28Z5uqy.exe	Get hash	malicious	Browse	• 193.56.146.64
	Hf34l6qunJ.exe	Get hash	malicious	Browse	• 193.56.146.64

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5280/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:C/:C/
MD5:	0FB51AB07BECFCF5B764E59B0957E47B
SHA1:	07616041CD80AD91C6AA10FF67BFEBA563B7C869
SHA-256:	FB1A28528DCFF52E97348E800604313D3E228AAA6AE947D7204F6C1512A5DEC2
SHA-512:	25A69A478FB7B9E63A3748FCE192E292B14EF021A0ACBACAAAE672B7FCC04C41957EFC2177DF13CEB84B7A33D577913477A57CAAD949B49EA0A06C8B00789C0C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	5280.

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.879578898375912
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	sora.mpsl
File size:	27236
MD5:	42ac0f5f0fd0d4e42fb7254730e94632
SHA1:	12369aa6f5ffd2e251a1e8924eee602b0ef7b2df
SHA256:	2dfc8c4568d6a3392fcd4d1837e17d3b4c6a412c8b98bdd91ce91a58250afbca
SHA512:	76e5a2ba9a9576f3bedb6d2fcbef73e6b042471f5c8f537c99e1b43726ef32182eef1b69c29cd960b0ce1cb41f7fb8e0e10aecb27b7d3dcbe3a39367ccf58ae0
SSDEEP:	768:w9CUFskb2JgIs/E2+OocrfJiHNjfmQ2q7IoqdBhUWx:GCrJgHiOJrfwmQrctpj
File Content Preview:	.ELF.....V..4.....4. ...(.....=i..=i.....E...E.....tUPX!`.....T...T.....T.....?.E.h;....#.....b.L#4E..,....M..D{c...j;.D .A....~.....hE.:.O.....L..N.7g..\....R.....

Static ELF Info

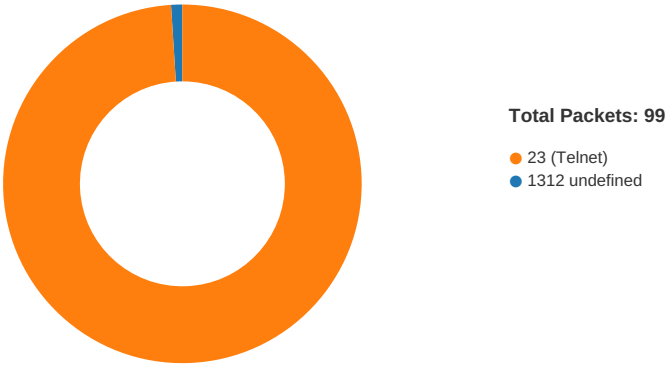
ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x105600
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
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	0x100000	0x100000	0x693d	0x693d	4.2069	0x5	R E	0x10000		
LOAD	0x18c0	0x4518c0	0x4518c0	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: sora.mpsl PID: 5240 Parent PID: 5118

General

Start time:	22:57:46
Start date:	10/11/2021
Path:	/tmp/sora.mpsl
Arguments:	/tmp/sora.mpsl
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

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

General

Start time:	22:57:47
Start date:	10/11/2021
Path:	/tmp/sora.mpsl
Arguments:	n/a
File size:	5773336 bytes

MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

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

General

Start time:	22:57:47
Start date:	10/11/2021
Path:	/tmp/sora.mpsl
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sora.mpsl PID: 5244 Parent PID: 5240

General

Start time:	22:57:47
Start date:	10/11/2021
Path:	/tmp/sora.mpsl
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sora.mpsl PID: 5248 Parent PID: 5244

General

Start time:	22:57:47
Start date:	10/11/2021
Path:	/tmp/sora.mpsl
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: sora.mpsl PID: 5249 Parent PID: 5244

General

Start time:	22:57:47
Start date:	10/11/2021
Path:	/tmp/sora.mpsl

Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sora.mpsl PID: 5251 Parent PID: 5244

General

Start time:	22:57:47
Start date:	10/11/2021
Path:	/tmp/sora.mpsl
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: systemd PID: 5279 Parent PID: 1

General

Start time:	22:58:02
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5279 Parent PID: 1

General

Start time:	22:58:02
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: 5280 Parent PID: 1

General

Start time:	22:58:02
Start date:	10/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5280 Parent PID: 1

General

Start time:	22:58:02
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