



ID: 635393
Sample Name: SBNGwWC7Wb
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 20:58:41
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report SBNGwWC7Wb 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
General Information 3
Warnings 3
Runtime Messages 3
Process Tree 4
Yara Signatures 4
Initial Sample 4
PCAP (Network Traffic) 4
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Networking 4
System Summary 4
Data Obfuscation 4
Hooking and other Techniques for Hiding and Protection 4
Stealing of Sensitive Information 5
Remote Access Functionality 5
Mitre Att&ck Matrix 5
Malware Configuration 5
Behavior Graph 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
URLs from Memory and Binaries 7
World Map of Contacted IPs 7
Public IPs 7
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
Static ELF Info 10
ELF header 10
Program Segments 10
Network Behavior 11
Network Port Distribution 11
TCP Packets 11
System Behavior 11
Analysis Process: SBNGwWC7Wb PID: 6224, Parent PID: 6122 11
General 11
File Activities 11
File Read 11
Analysis Process: SBNGwWC7Wb PID: 6226, Parent PID: 6224 11
General 11
Analysis Process: SBNGwWC7Wb PID: 6227, Parent PID: 6224 11
General 11
Analysis Process: SBNGwWC7Wb PID: 6234, Parent PID: 6227 12
General 12
File Activities 12
File Read 12
Directory Enumerated 12
Analysis Process: SBNGwWC7Wb PID: 6236, Parent PID: 6227 12
General 12
Analysis Process: SBNGwWC7Wb PID: 6238, Parent PID: 6236 12
General 12

Copyright Joe Security LLC 2022

Linux Analysis Report

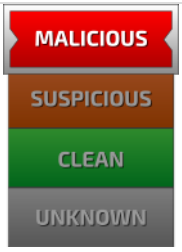
SBNGwWC7Wb

Overview

General Information

Sample Name:	SBNGwWC7Wb
Analysis ID:	635393
MD5:	275c6e393dcace..
SHA1:	64a8605d5f6914..
SHA256:	bb0fea23f67c783..
Tags:	32 elf mips mirai
Infos:	

Detection



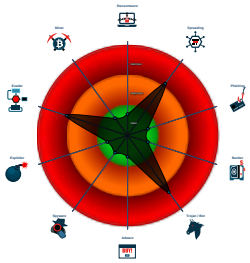
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- 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…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.

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

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635393
Start date and time: 27/05/202220:58:41	2022-05-27 20:58:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SBNGwWC7Wb
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.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/SBNGwWC7Wb
PID:	6224
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected

Copyright Joe Security LLC 2022

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- SBNGwWC7Wb (PID: 6224, Parent: 6122, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/SBNGwWC7Wb
  - SBNGwWC7Wb New Fork (PID: 6226, Parent: 6224)
  - SBNGwWC7Wb New Fork (PID: 6227, Parent: 6224)
    - SBNGwWC7Wb New Fork (PID: 6234, Parent: 6227)
    - SBNGwWC7Wb New Fork (PID: 6236, Parent: 6227)
      - SBNGwWC7Wb New Fork (PID: 6238, Parent: 6236)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SBNGwWC7Wb	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x9cf0:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x9d5f:$s2: $Id: UPX • 0x9d10:$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	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Networking



Uses known network protocols on non-standard ports

System Summary



Sample tries to kill multiple processes (SIGKILL)

Data Obfuscation



Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection



Copyright Joe Security LLC 2022

Uses known network protocols on non-standard ports

Stealing of Sensitive Information



Yara detected Mirai

Remote Access Functionality



Yara detected Mirai

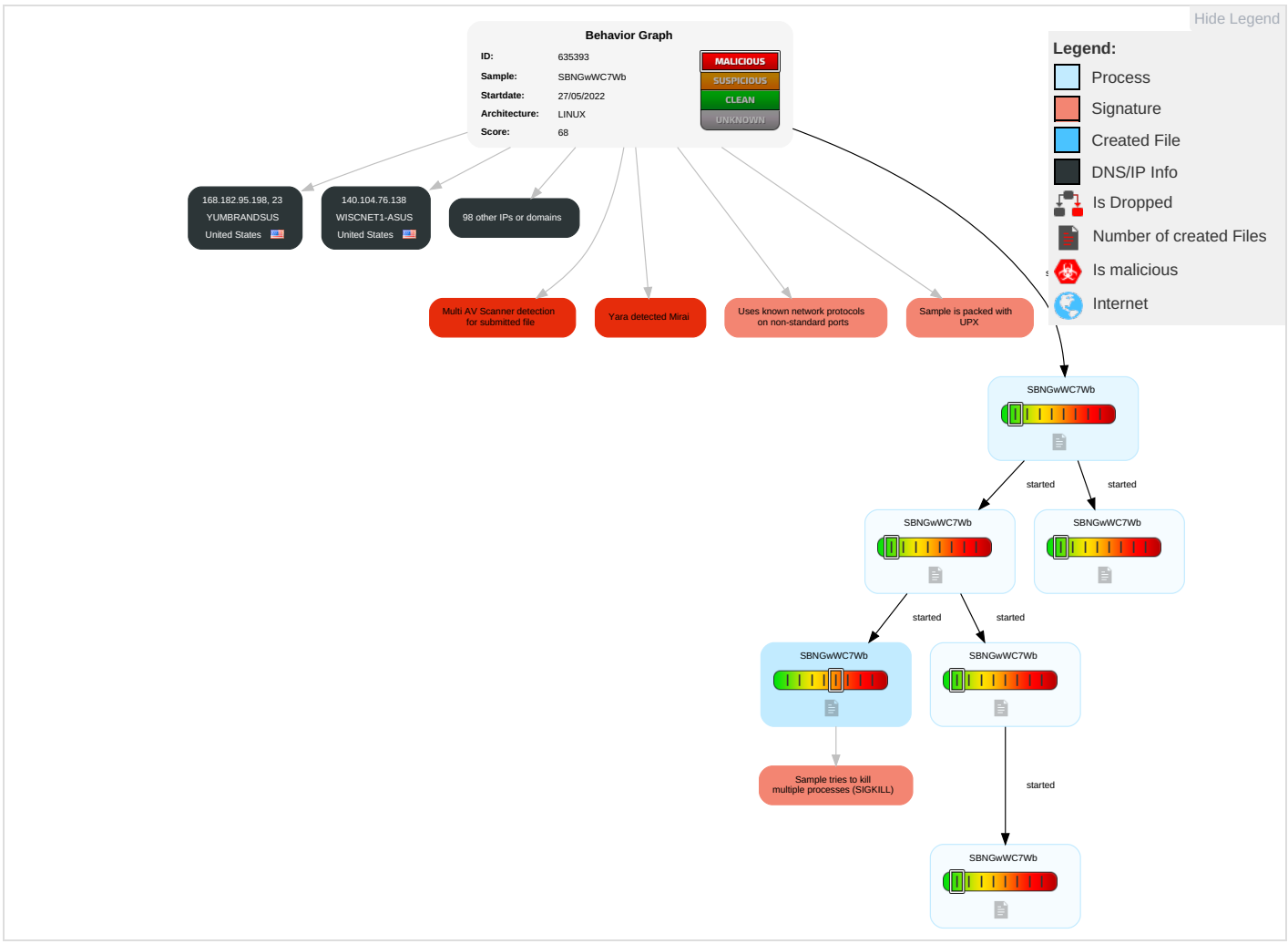
Mitre Att&ck Matrix

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	1 Obfuscated Files or Information	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Service Stop
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	1 1 Non-Standard Port	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	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SBNGwWC7Wb	22%	Virustotal		Browse
SBNGwWC7Wb	25%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

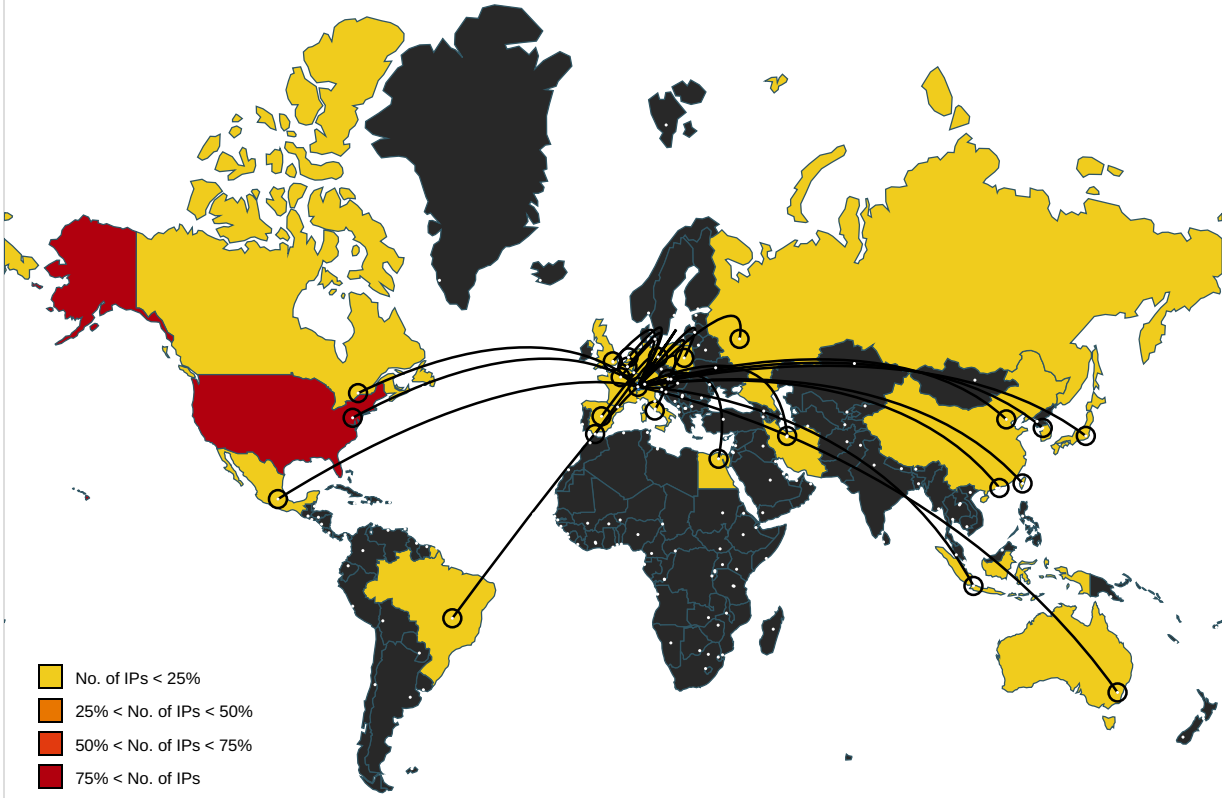
Contacted Domains

No contacted domains info

Copyright Joe Security LLC 2022

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.232.31.217	unknown	United States		7029	WINDSTREAMUS	false
63.184.206.219	unknown	United States		1239	SPRINTLINKUS	false
246.132.172.181	unknown	Reserved		unknown	unknown	false
207.32.216.34	unknown	United States		14315	1GSERVERSUS	false
28.242.55.33	unknown	United States		7922	COMCAST-7922US	false
220.21.234.141	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
168.182.95.198	unknown	United States		18522	YUMBRANDSUS	false
45.25.228.59	unknown	United States		7018	ATT-INTERNET4US	false
98.19.126.234	unknown	United States		7029	WINDSTREAMUS	false
255.84.172.156	unknown	Reserved		unknown	unknown	false
46.172.163.178	unknown	Russian Federation		48044	CHITA-ON-LINE-ASRU	false
214.169.204.9	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
100.227.43.9	unknown	United States		21928	T-MOBILE-AS21928US	false
43.118.46.72	unknown	Japan		4249	LILLY-ASUS	false
50.181.162.86	unknown	United States		7922	COMCAST-7922US	false
22.246.2.216	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
67.96.186.6	unknown	United States		6977	IAC-ASUS	false
160.42.218.209	unknown	United States		1761	TDIR-CAPNETUS	false
247.238.59.67	unknown	Reserved		unknown	unknown	false
69.109.26.14	unknown	United States		7018	ATT-INTERNET4US	false
85.35.1.143	unknown	Italy		3269	ASN-IBSNAZIT	false
120.188.79.134	unknown	Indonesia		4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false
47.195.167.195	unknown	United States		5650	FRONTIER-FRTRUS	false
171.67.143.13	unknown	United States		32	STANFORDUS	false
255.56.220.95	unknown	Reserved		unknown	unknown	false
159.1.39.145	unknown	United States		4193	WA-STATE-GOVUS	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
113.247.214.242	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
252.251.81.4	unknown	Reserved		unknown	unknown	false
172.32.220.45	unknown	United States		21928	T-MOBILE-AS21928US	false
140.211.52.231	unknown	United States		3701	NERONETUS	false
220.14.193.199	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
150.199.109.75	unknown	United States		2572	MORENETUS	false
18.213.221.156	unknown	United States		14618	AMAZON-AESUS	false
246.131.18.105	unknown	Reserved		unknown	unknown	false
253.93.243.136	unknown	Reserved		unknown	unknown	false
28.77.143.29	unknown	United States		7922	COMCAST-7922US	false
217.113.75.78	unknown	Belgium		3491	BTN-ASNUS	false
145.83.208.94	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
201.111.171.232	unknown	Mexico		8151	UninetSAdeCVMX	false
98.89.244.96	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
117.55.179.250	unknown	Korea Republic of		9770	SPEEDONSTV-AS-KRLGHelloVisionCorpKR	false
176.177.113.98	unknown	France		5410	BOUYGTEL-ISPFR	false
112.213.114.218	unknown	Hong Kong		38197	SUNHK-DATA-AS-APSunNetworkHongKongLimited-HongKong	false
140.104.76.138	unknown	United States		2381	WISCNET1-ASUS	false
252.202.169.243	unknown	Reserved		unknown	unknown	false
47.178.236.161	unknown	United States		5650	FRONTIER-FRTRUS	false
137.41.141.14	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
120.87.46.212	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
12.69.83.54	unknown	United States		7018	ATT-INTERNET4US	false
92.38.145.170	unknown	Austria		199524	GCOREAT	false
122.4.122.51	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
172.203.97.144	unknown	United States		18747	IFX18747US	false
185.38.220.182	unknown	Poland		56523	AMELEKTRONIKPL	false
251.179.142.95	unknown	Reserved		unknown	unknown	false
248.231.10.213	unknown	Reserved		unknown	unknown	false
199.245.173.166	unknown	United States		10653	MVANETUS	false
170.174.174.89	unknown	United States		11685	HNBCOL-ASUS	false
189.105.20.33	unknown	Brazil		7738	TelemarNorteLesteSABR	false
43.121.222.110	unknown	Japan		4249	LILLY-ASUS	false
2.163.103.53	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
182.119.170.127	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
145.85.202.109	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
188.78.234.108	unknown	Spain		12479	UNI2-ASES	false
135.4.62.162	unknown	United States		10455	LUCENT-CIOUS	false
215.174.150.203	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
103.237.107.133	unknown	Australia		53580	MARKETOUS	false
66.229.157.194	unknown	United States		7922	COMCAST-7922US	false
180.237.67.211	unknown	Korea Republic of		9658	ETPI-IDS-AS-APEasternTelecomsPhilsIncPH	false
3.102.75.253	unknown	United States		16509	AMAZON-02US	false
98.233.96.179	unknown	United States		7922	COMCAST-7922US	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
168.108.37.33	unknown	United States		3597	FundacionInnovaTAR	false
142.31.146.109	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
33.236.64.10	unknown	United States		2686	ATGS-MMD-ASUS	false
114.241.91.184	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
134.244.73.128	unknown	United States		3479	PEACHNET-AS1US	false
149.176.228.12	unknown	Australia		87	INDIANA-ASUS	false
101.83.244.147	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
16.165.211.152	unknown	United States		unknown	unknown	false
142.80.215.163	unknown	Canada		5769	VIDEOTRONCA	false
57.62.64.136	unknown	Belgium		2686	ATGS-MMD-ASUS	false
123.69.92.169	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
72.152.89.199	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
98.107.192.151	unknown	United States		6167	CELLCO-PARTUS	false
40.69.202.47	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
31.91.224.64	unknown	United Kingdom		12576	EELtdGB	false
196.147.8.25	unknown	Egypt		36935	Vodafone-EG	false
220.138.127.69	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
211.226.202.75	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
17.8.137.173	unknown	United States		714	APPLE-ENGINEERINGUS	false
145.107.128.126	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
37.27.84.41	unknown	Iran (ISLAMIC Republic Of)		39232	UNINETAZ	false
91.215.129.120	unknown	Russian Federation		41082	URALTRANSCOM-ASUA	false
185.126.207.167	unknown	Italy		208920	ROCKETWAY-ASIT	false
215.228.201.148	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
212.22.245.89	unknown	Gibraltar		12798	VCW-ASGibraltarGI	false
65.180.56.237	unknown	United States		1239	SPRINTLINKUS	false
7.138.173.10	unknown	United States		3356	LEVEL3US	false
179.137.207.90	unknown	Brazil		26599	TELEFONICABRASILSABR	false
69.128.229.182	unknown	United States		4181	TDS-ASUS	false
149.160.93.171	unknown	United States		87	INDIANA-ASUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Copyright Joe Security LLC 2022

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.940001959669167
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	SBNGwWC7Wb
File size:	42432
MD5:	275c6e393dcacee32b9ddd8bb4ad8196
SHA1:	64a8605d5f69142a08385b359d3a6fd73120880d
SHA256:	bb0fea23f67c783d1b0d3f8f92e1fd91f1c5d85f7782bc135f0269057e2ab4c3
SHA512:	55a1f799d6f70f71201ff6eadfb06b773f962217bb2138b276aaf823fe601bec605ad8098c485103cd8f6f9912f34b0c4b70768368110f32856cd2c572ca6754
SSDEEP:	768:kBngnCJnfsrVyYfvYdu80skETund52DdwyX2uxPvxfG6sNEx/vjE88VPwqJgGlzg:kBgnwUVy8v0u83TunTL8v4653jE88eOu
TLSH:	B513F277DE1991B6EE5992720ACCC6879C56A9D07B03D88BE825D7E02EC70163203AF1
File Content Preview:	.ELF.....@...4.....4. ...(.....\.F.\.F.\.....UPX!.d.....p...p.....T.....?.E.h4...@b..) ..]....E..$u..s...x..b.bU.ZN.S.#.W).....7.....i... .AT...Y....L.....

Static ELF Info

ELF header

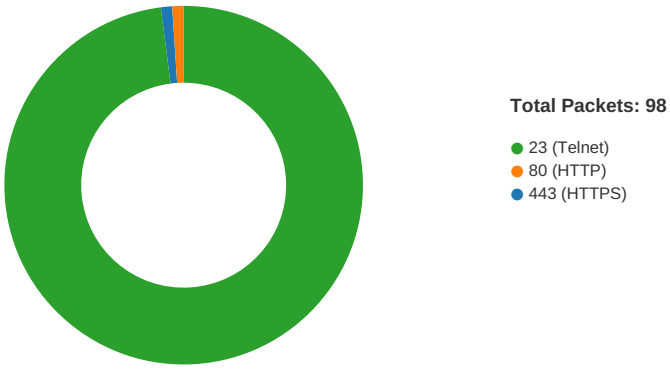
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x109140
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program 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	0xa484	0xa484	4.1326	0x5	R E	0x10000		
LOAD	0xd5c	0x460d5c	0x460d5c	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: SBNGwWC7Wb PID: 6224, Parent PID: 6122

General

Start time:	20:59:30
Start date:	27/05/2022
Path:	/tmp/SBNGwWC7Wb
Arguments:	/tmp/SBNGwWC7Wb
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: SBNGwWC7Wb PID: 6226, Parent PID: 6224

General

Start time:	20:59:30
Start date:	27/05/2022
Path:	/tmp/SBNGwWC7Wb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: SBNGwWC7Wb PID: 6227, Parent PID: 6224

General

Start time:	20:59:30
Start date:	27/05/2022
Path:	/tmp/SBNGwWC7Wb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Copyright Joe Security LLC 2022

Analysis Process: SBNGwWC7Wb PID: **6234**, Parent PID: **6227**

General

Start time:	20:59:30
Start date:	27/05/2022
Path:	/tmp/SBNGwWC7Wb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: SBNGwWC7Wb PID: **6236**, Parent PID: **6227**

General

Start time:	20:59:30
Start date:	27/05/2022
Path:	/tmp/SBNGwWC7Wb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: SBNGwWC7Wb PID: **6238**, Parent PID: **6236**

General

Start time:	20:59:30
Start date:	27/05/2022
Path:	/tmp/SBNGwWC7Wb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Copyright Joe Security LLC 2022