ID: 780228
Sample Name:
JhgW21BqHE.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:34:03
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

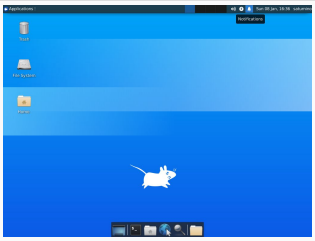
Linux Analysis Report

JhgW21BqHE.elf

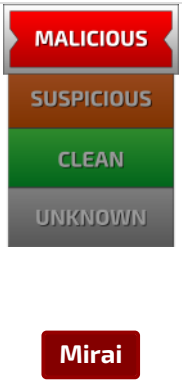
Overview

General Information

Sample Name:	JhgW21BqHE.elf
Analysis ID:	780228
MD5:	d3a4afd2425eb6..
SHA1:	818b61c85a6d3a..
SHA256:	134825331bcbf2..
Tags:	32 elf mirai renesas
Infos:	



Detection



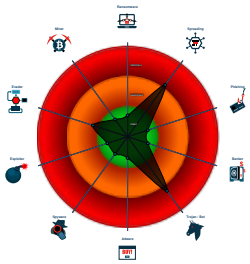
Mirai

Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample tries to kill multiple process…
- 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 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.

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	780228
Start date and time:	2023-01-08 16:34:03 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JhgW21BqHE.elf
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:	mal60.spre.troj.linELF@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/JhgW21BqHE.elf
PID:	6228
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- JhgW21BqHE.elf (PID: 6228, Parent: 6122, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/JhgW21BqHE.elf
  - JhgW21BqHE.elf New Fork (PID: 6230, Parent: 6228)
    - JhgW21BqHE.elf New Fork (PID: 6333, Parent: 6230)
    - JhgW21BqHE.elf New Fork (PID: 6335, Parent: 6230)
      - JhgW21BqHE.elf New Fork (PID: 6337, Parent: 6335)
        - JhgW21BqHE.elf New Fork (PID: 6349, Parent: 6337)
        - JhgW21BqHE.elf New Fork (PID: 6350, Parent: 6337)
      - JhgW21BqHE.elf New Fork (PID: 6339, Parent: 6335)
      - JhgW21BqHE.elf New Fork (PID: 6341, Parent: 6335)
  - JhgW21BqHE.elf New Fork (PID: 6231, Parent: 6228)
  - JhgW21BqHE.elf New Fork (PID: 6232, Parent: 6228)
    - JhgW21BqHE.elf New Fork (PID: 6235, Parent: 6232)
    - JhgW21BqHE.elf New Fork (PID: 6237, Parent: 6232)
    - JhgW21BqHE.elf New Fork (PID: 6239, Parent: 6232)
- **cleanup**

Yara Signatures

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

System Summary

Sample tries to kill multiple processes (SIGKILL)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

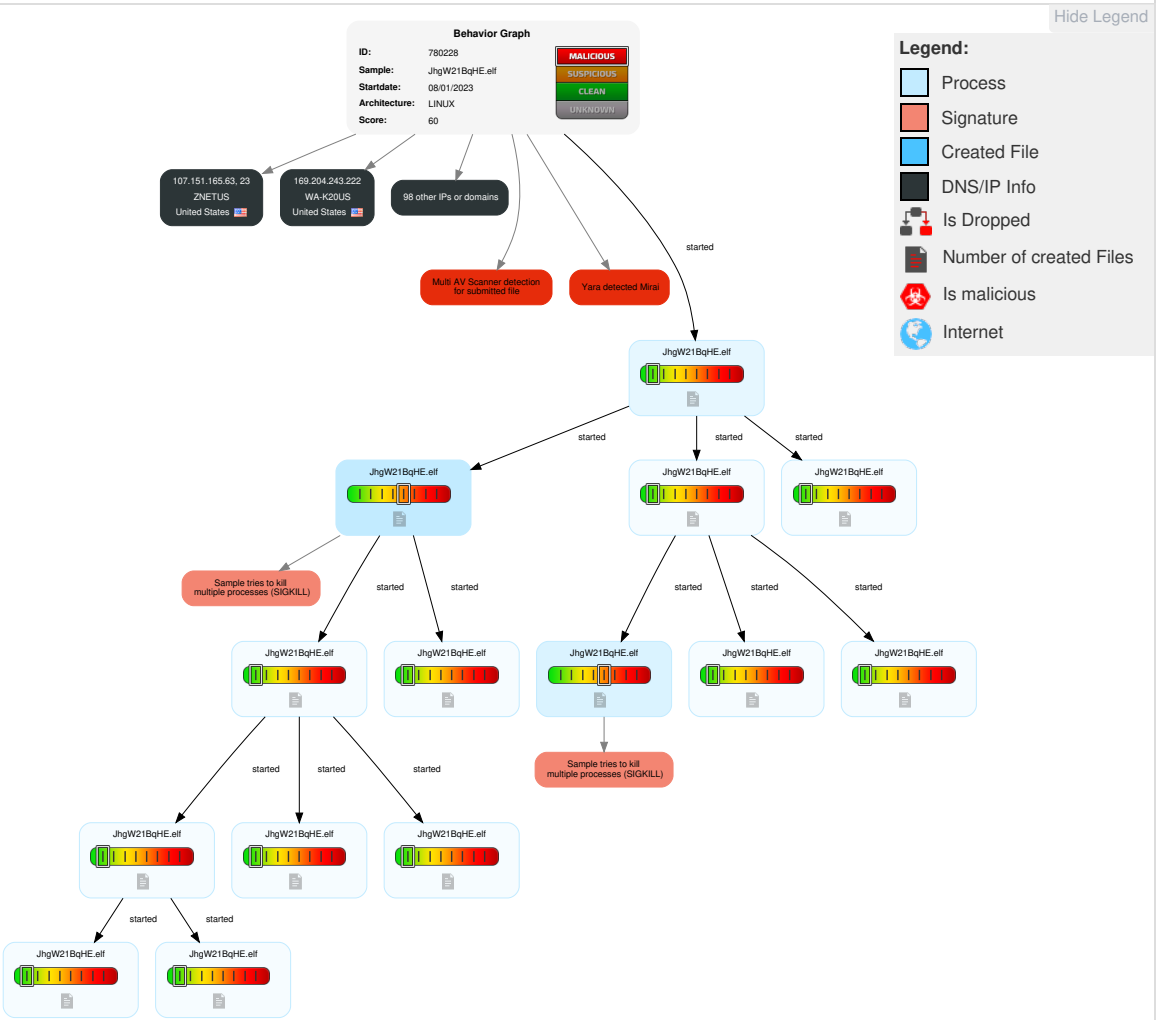
Mitre Att&ck Matrix

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	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 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

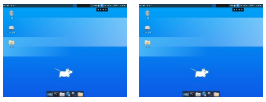
Behavior Graph

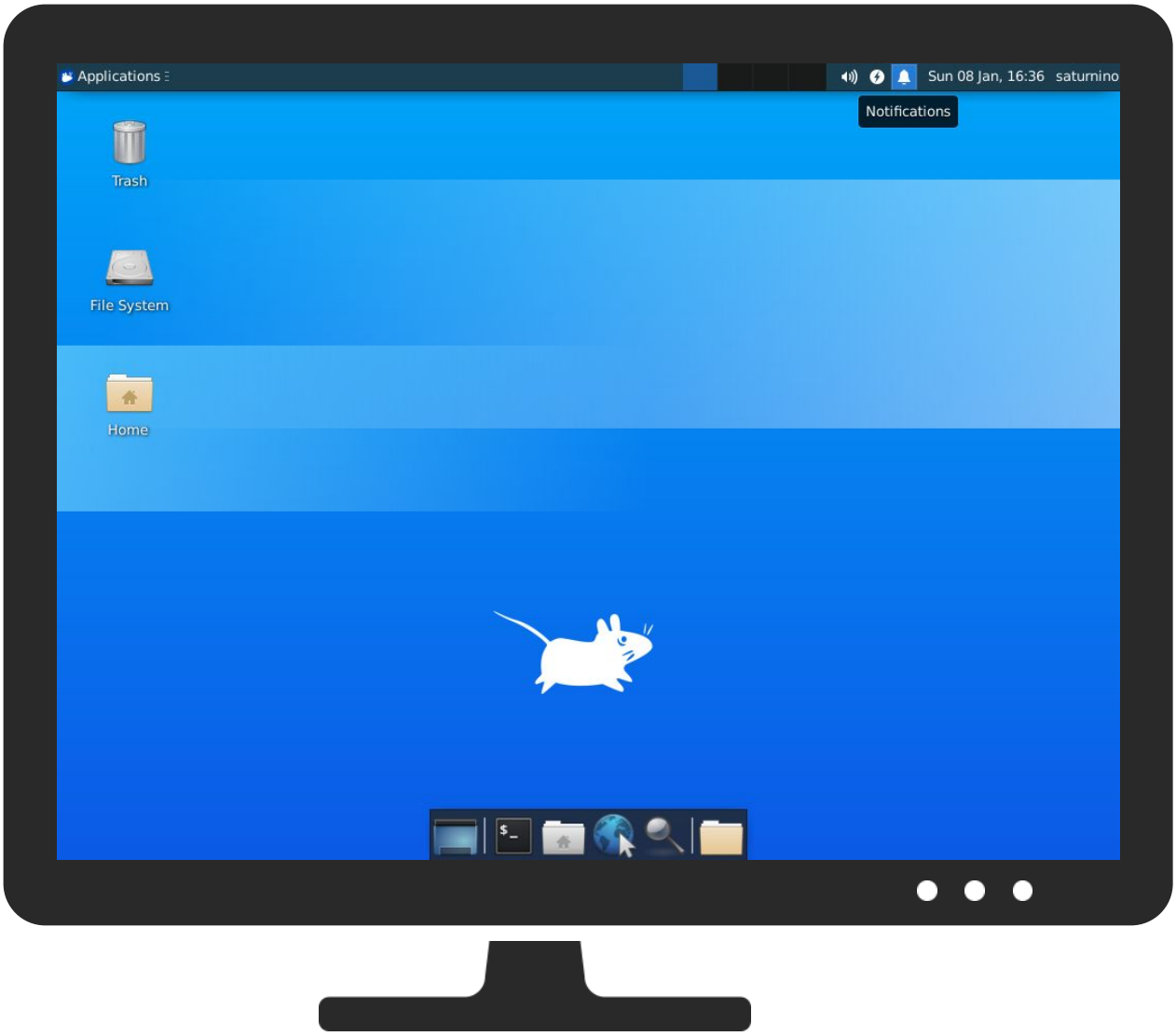


Screenshots

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
JhgW21BqHE.elf	77%	ReversingLabs	Linux.Trojan.Mirai	
JhgW21BqHE.elf	63%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

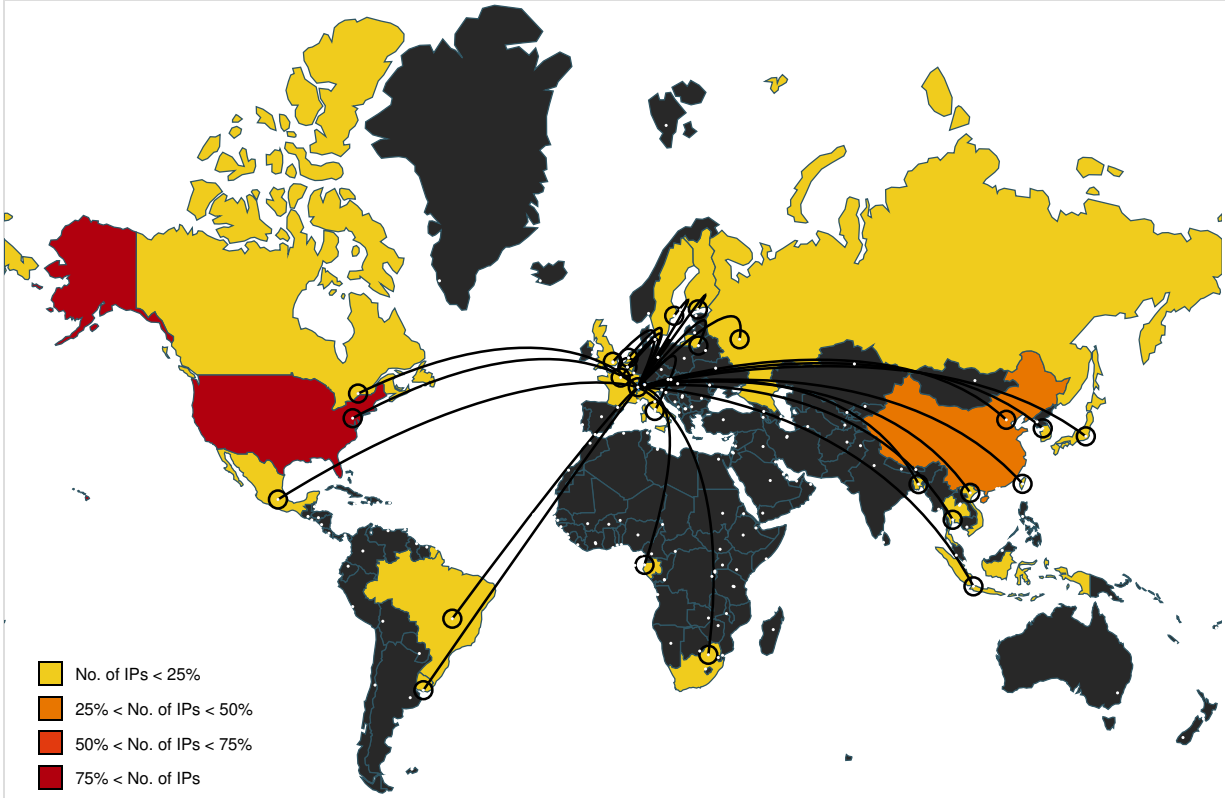
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
117.65.71.158	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
158.131.25.237	unknown	Finland		55	UPENNUS	false
118.230.33.248	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
169.204.243.222	unknown	United States		10430	WA-K20US	false
213.21.10.14	unknown	Russian Federation		39102	AS-ATHMbrandAtHomeRU	false
218.2.239.92	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
120.241.244.130	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
168.108.141.231	unknown	United States		3597	FundacionInnovaTAR	false
251.42.237.111	unknown	Reserved		unknown	unknown	false
14.172.150.21	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
65.43.112.213	unknown	United States		7018	ATT-INTERNET4US	false
88.223.35.64	unknown	Lithuania		39354	INIT-MGNT-LT	false
103.117.108.100	unknown	Bangladesh		137935	ILIS-AS-APILinkInternetServiceBD	false
179.133.81.177	unknown	Brazil		26599	TELEFONICABRASILSAB R	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
246.182.65.48	unknown	Reserved		unknown	unknown	false
42.178.17.251	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
102.142.143.175	unknown	Gabon		36924	GVA-CanalboxBJ	false
113.17.198.4	unknown	China		134419	CHINATELECOM-GUANGXI-BEIHAI-MANBeihaiCN	false
82.175.129.155	unknown	Netherlands		13127	VERSATELASfortheTrans-EuropeanTele2IPTransportbackbo	false
64.229.95.64	unknown	Canada		577	BACOMCA	false
205.176.15.147	unknown	United States		8103	STATE-OF-FLAUS	false
40.38.130.143	unknown	United States		4249	LILLY-ASUS	false
107.33.165.120	unknown	United States		16567	NETRIX-16567US	false
247.184.181.222	unknown	Reserved		unknown	unknown	false
34.91.114.108	unknown	United States		15169	GOOGLEUS	false
72.180.77.119	unknown	United States		11427	TWC-11427-TEXASUS	false
163.193.1.205	unknown	United States		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
84.216.36.105	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
83.247.75.248	unknown	Netherlands		12414	NL-SOLCONSOLCONNL	false
163.213.230.45	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
241.223.124.182	unknown	Reserved		unknown	unknown	false
182.149.90.141	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
242.38.159.152	unknown	Reserved		unknown	unknown	false
168.44.123.13	unknown	United States		1761	TDIR-CAPNETUS	false
153.132.251.0	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
148.13.57.17	unknown	United States		394673	9408US	false
98.61.107.149	unknown	United States		7922	COMCAST-7922US	false
65.170.163.22	unknown	United States		14861	ISC-GROUPUS	false
220.185.96.120	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
57.102.94.118	unknown	Belgium		2647	SITABE	false
183.242.57.111	unknown	China		56048	CMNET-BEIJING-APChinaMobileCommunicaitonsCorporationCN	false
75.73.68.200	unknown	United States		7922	COMCAST-7922US	false
104.221.41.157	unknown	Canada		5769	VIDEOTRONCA	false
139.154.136.23	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
153.186.72.47	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
178.226.185.159	unknown	Netherlands		31615	TMO-NL-ASNL	false
139.236.16.138	unknown	United States		1462	DNIC-ASBLK-01462-01463US	false
133.73.232.160	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
122.146.5.168	unknown	Taiwan; Republic of China (ROC)		9919	NCIC-TWNewCenturyInfoCommTechCoLtdTW	false
175.12.134.233	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
165.36.166.215	unknown	United States		37053	RSAWEB-ASZA	false
123.154.17.246	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
156.130.0.84	unknown	United States		29975	VODACOM-ZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
161.153.72.71	unknown	United States		9328	DATACOM-AUDATACOMSYSTEMSAUPTYLTDAU	false
209.47.188.199	unknown	United States		701	UUNETUS	false
75.134.22.122	unknown	United States		20115	CHARTER-20115US	false
198.113.9.30	unknown	United States		3356	LEVEL3US	false
96.181.213.226	unknown	United States		7922	COMCAST-7922US	false
47.149.220.123	unknown	United States		5650	FRONTIER-FRTRUS	false
189.212.136.208	unknown	Mexico		6503	AxtelSABdeCVMX	false
107.151.165.63	unknown	United States		21859	ZNETUS	false
38.218.17.63	unknown	United States		174	COGENT-174US	false
243.173.63.91	unknown	Reserved		unknown	unknown	false
218.83.9.52	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
180.251.193.134	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
153.40.154.181	unknown	United States		14365	ADOBE-NETUS	false
168.67.37.38	unknown	United States		265240	ULTRANETSERVICOSEMINTERNETLTDABR	false
40.238.166.104	unknown	United States		4249	LILLY-ASUS	false
171.102.140.39	unknown	Thailand		7470	TRUEINTERNET-AS-APTRUEINTERNETCoLtdTH	false
179.31.207.4	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
72.159.171.144	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
110.126.105.237	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
197.221.108.111	unknown	South Africa		37236	Reflex-SolutionsZA	false
122.100.88.214	unknown	Taiwan; Republic of China (ROC)		4662	QTCN-ASN1GCNetReachRangeIncTW	false
152.49.80.179	unknown	United States		81	NCRENUS	false
165.103.166.4	unknown	United States		394053	NAICWEBUS	false
152.145.142.184	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
114.171.18.149	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
208.144.203.116	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
153.250.183.64	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
79.3.165.223	unknown	Italy		3269	ASN-IBSNAZIT	false
148.15.168.173	unknown	United States		394673	9408US	false
196.31.223.112	unknown	South Africa		16637	MTNNS-ASZA	false
175.222.170.116	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
142.84.146.140	unknown	Canada		11489	BACICA	false
86.179.107.49	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
36.56.30.210	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
80.14.1.179	unknown	France		3215	FranceTelecom-OrangeFR	false
177.77.153.108	unknown	Brazil		26599	TELEFONICABRASILSAB R	false
9.31.145.232	unknown	United States		3356	LEVEL3US	false
20.199.232.189	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
58.51.217.122	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
70.2.215.32	unknown	United States		10507	SPCSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
101.39.68.101	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
36.141.1.194	unknown	China		56044	CMNET-AS-LIAONINGChinaMobilecommunicationscorporationC	false
246.197.45.224	unknown	Reserved		unknown	unknown	false
36.194.65.178	unknown	China		24138	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
119.21.239.138	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
198.179.14.115	unknown	United States		26810	HHSNET-NOC-ASNUS	false
18.2.100.92	unknown	United States		10578	GIGAPOP-NEUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.767200503838304
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	JhgW21BqHE.elf
File size:	51584
MD5:	d3a4afd2425eb644fb07e695d4415aa5
SHA1:	818b61c85a6d3ad186aa24532db4e4c5017fc092
SHA256:	134825331bcbf2c60f0d876a042145d12569b2da86bd68273eae6708e010d41e
SHA512:	44fe7796175a2cb8acd821fe8c2040f73df9869f54c52f97e2ca2ad90f271bb4ddd7ecb16d797387de6039171a29d316cf23531241fd093f2fe33e503d6e1ddd
SSDEEP:	768:jaixFwtLSYAagMo0ebH4/ZvQX3hyWfs3INgCJUU/qMCqKomQRCvM:jaQFwtOGBvQXxfs3kgCJt/qMF/RCvM

TLSH:	D8338CB5C579EDE8D1144A78BE248E749723E000C6932EFADA44C6699043EFCF5583F4
File Content Preview:	.ELF.....*.....@.4.....4. ...(.....@...@.<...<.....@...@.A.@.A.p.....Q.td....././"O.n.....#.*@.....#.*@,....o&O.n...l....././.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

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	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xbf40	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40c020	0xc020	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40c044	0xc044	0x5f8	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41c640	0xc640	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41c648	0xc648	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41c654	0xc654	0x15c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x41c7b0	0xc7b0	0x280	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xc7b0	0x3e	0x0	0x0		0	0	1

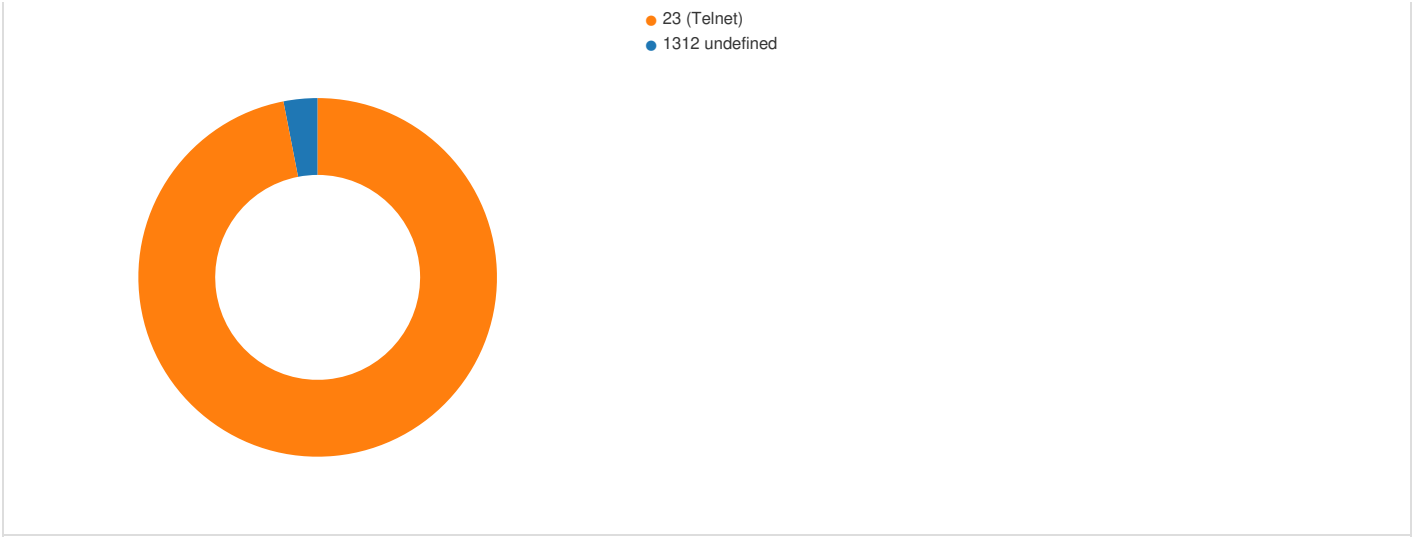
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0xc63c	0xc63c	6.8130	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xc640	0x41c640	0x41c640	0x170	0x3f0	0.8708	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution

Total Packets: 98



TCP Packets

System Behavior

Analysis Process: JhgW21BqHE.elf PID: 6228, Parent PID: 6122

General

Start time:	16:34:48
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	/tmp/JhgW21BqHE.elf
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: JhgW21BqHE.elf PID: 6230, Parent PID: 6228

General

Start time:	16:34:48
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: JhgW21BqHE.elf PID: 6333, Parent PID: 6230

General

Start time:	16:37:56
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6335**, Parent PID: **6230**

General

Start time:	16:37:56
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6337**, Parent PID: **6335**

General

Start time:	16:37:56
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6349**, Parent PID: **6337**

General

Start time:	16:38:01
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6350**, Parent PID: **6337**

General

Start time:	16:38:01
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6339**, Parent PID: **6335**

General

Start time:	16:37:56
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6341**, Parent PID: **6335**

General

Start time:	16:37:56
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6231**, Parent PID: **6228**

General

Start time:	16:34:48
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6232**, Parent PID: **6228**

General

Start time:	16:34:48
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6235**, Parent PID: **6232**

General

Start time:	16:34:48
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: JhgW21BqHE.elf PID: **6237**, Parent PID: **6232**

General

Start time:	16:34:48
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: JhgW21BqHE.elf PID: **6239**, Parent PID: **6232**

General

Start time:	16:34:48
Start date:	08/01/2023
Path:	/tmp/JhgW21BqHE.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9