ID: 1303230
Sample Name: IJB2Ub1KkE.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 05:49:10
Date: 05/09/2023
Version: 38.0.0 Beryl

Table of Contents

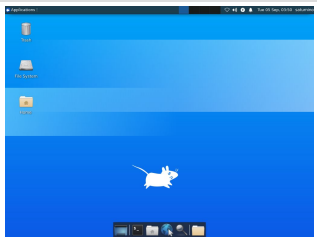
Linux Analysis Report

IJB2Ub1KkE.elf

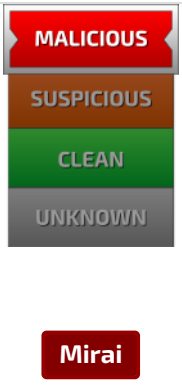
Overview

General Information

Sample Name:	IJB2Ub1KkE.elf
Original Sample Name:	4cb948a32c4e…
Analysis ID:	1303230
MD5:	4cb948a32c4e…
SHA1:	8997b6216a14…
SHA256:	9ef61be75e727..
Tags:	32 elf mirai renesas
Infos:	



Detection

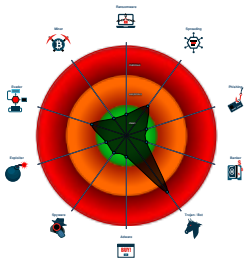


Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on n…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- 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.

General Information

Joe Sandbox Version:	38.0.0 Beryl
Analysis ID:	1303230
Start date and time:	2023-09-05 05:49:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample file name:	IJB2Ub1KkE.elf
Original Sample Name:	4cb948a32c4ef20b6d74006938218277.elf
Detection:	MAL
Classification:	mal68.troj.linELF@0/0@2/0

Warnings

Runtime Messages

Command:	/tmp/IJB2Ub1KkE.elf
PID:	5493
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Follow twitter.com/1337Wicked

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- lJB2Ub1KkE.elf (PID: 5493, Parent: 5402, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/lJB2Ub1KkE.elf
  - lJB2Ub1KkE.elf New Fork (PID: 5495, Parent: 5493)
    - lJB2Ub1KkE.elf New Fork (PID: 5599, Parent: 5495)
    - lJB2Ub1KkE.elf New Fork (PID: 5603, Parent: 5495)
      - lJB2Ub1KkE.elf New Fork (PID: 5606, Parent: 5603)
        - lJB2Ub1KkE.elf New Fork (PID: 5615, Parent: 5606)
        - lJB2Ub1KkE.elf New Fork (PID: 5616, Parent: 5606)
      - lJB2Ub1KkE.elf New Fork (PID: 5608, Parent: 5603)
      - lJB2Ub1KkE.elf New Fork (PID: 5610, Parent: 5603)
  - lJB2Ub1KkE.elf New Fork (PID: 5496, Parent: 5493)
  - lJB2Ub1KkE.elf New Fork (PID: 5498, Parent: 5493)
    - lJB2Ub1KkE.elf New Fork (PID: 5501, Parent: 5498)
      - lJB2Ub1KkE.elf New Fork (PID: 5598, Parent: 5501)
      - lJB2Ub1KkE.elf New Fork (PID: 5601, Parent: 5501)
    - lJB2Ub1KkE.elf New Fork (PID: 5502, Parent: 5498)
    - lJB2Ub1KkE.elf New Fork (PID: 5505, Parent: 5498)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	**http://** osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

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

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

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

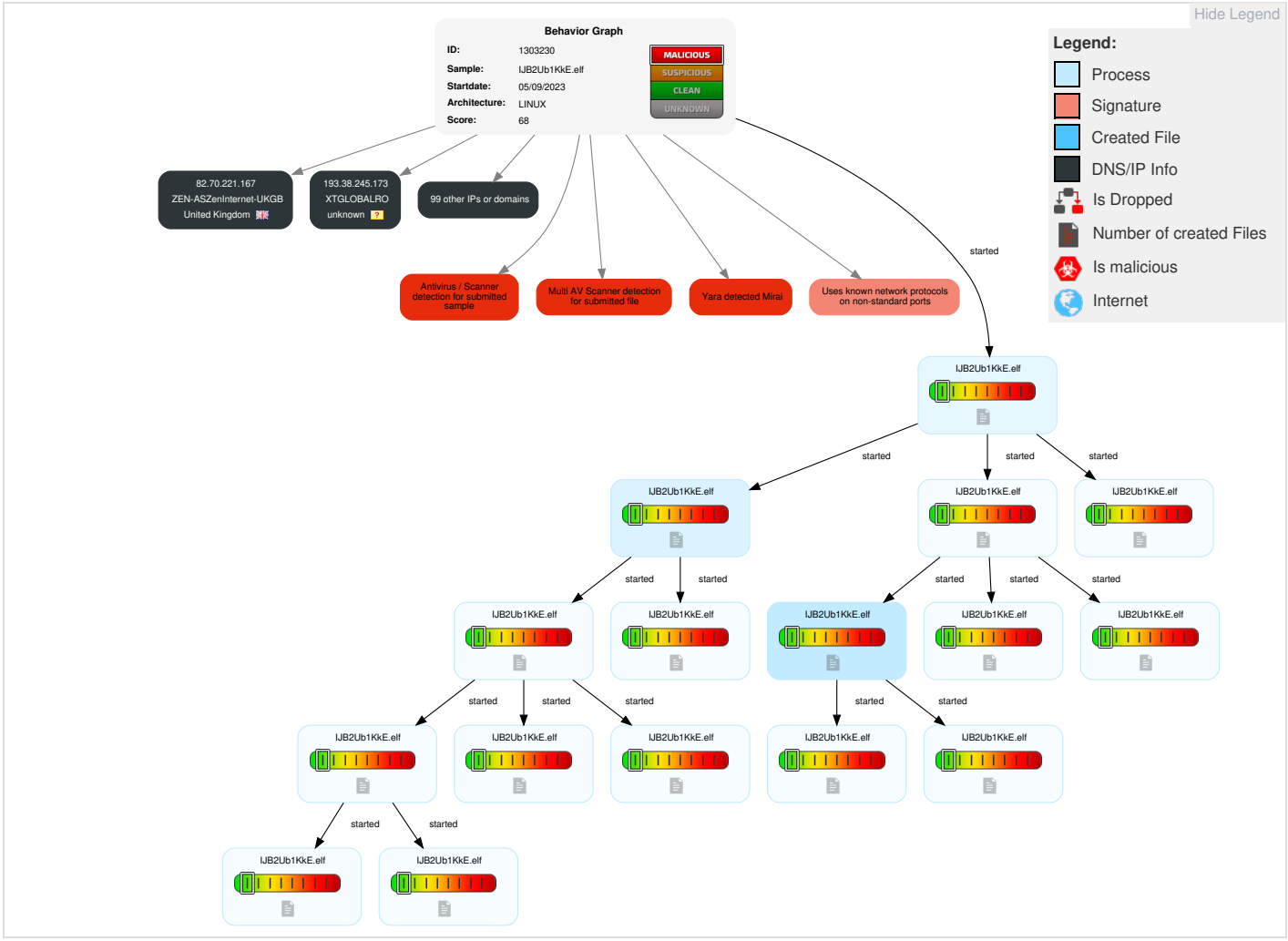
Mitre Att&ck Matrix

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	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 1 Non-Standard Port	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	1 Non-Application Layer Protocol	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

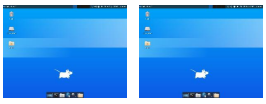
Behavior Graph

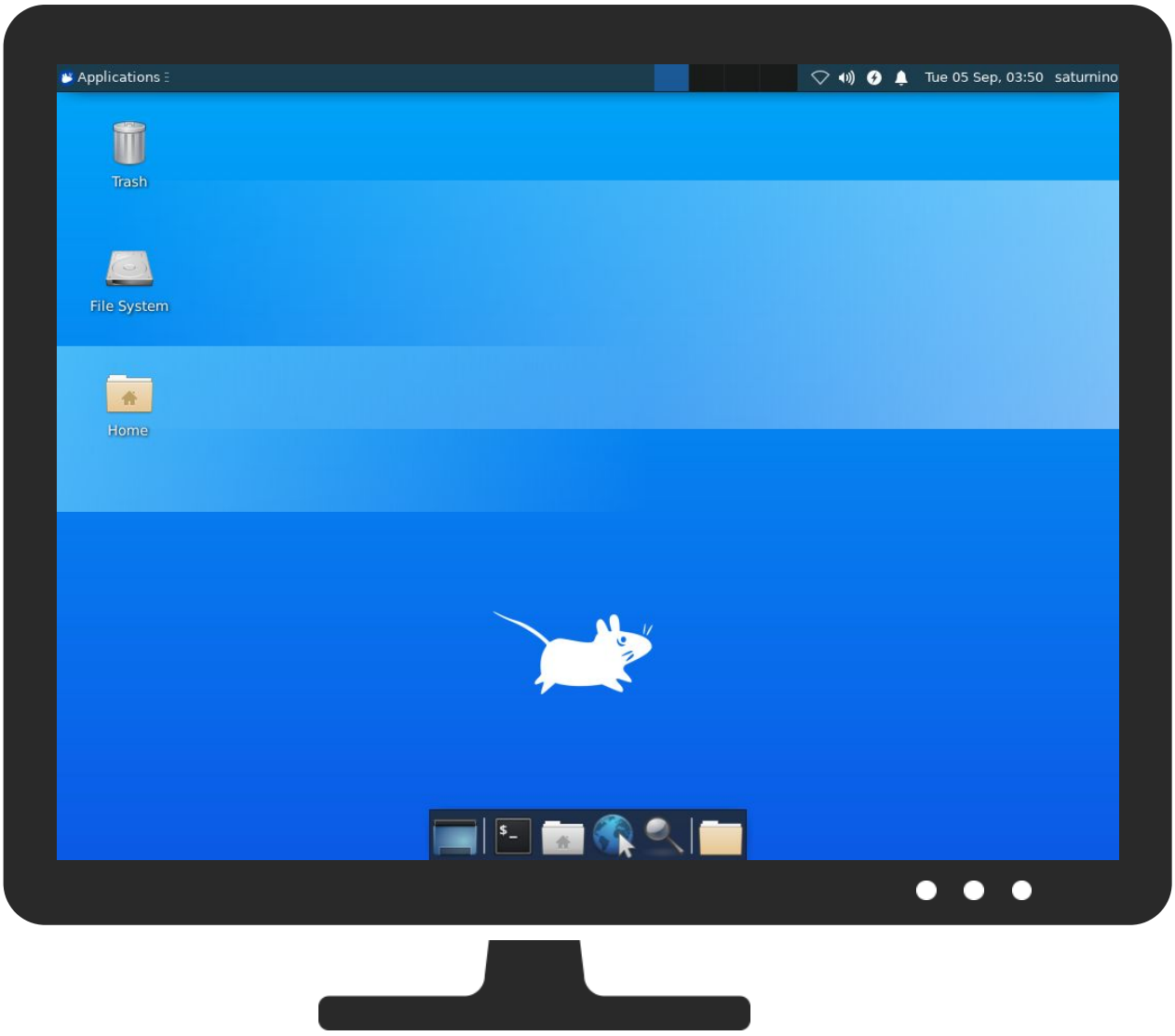


Screenshots

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
IJB2Ub1KkE.elf	63%	ReversingLabs	Linux.Trojan.Mirai	
IJB2Ub1KkE.elf	64%	Virustotal		Browse
IJB2Ub1KkE.elf	100%	Avira	EXP/ELF.Mirai.Botnet.Gen.o	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

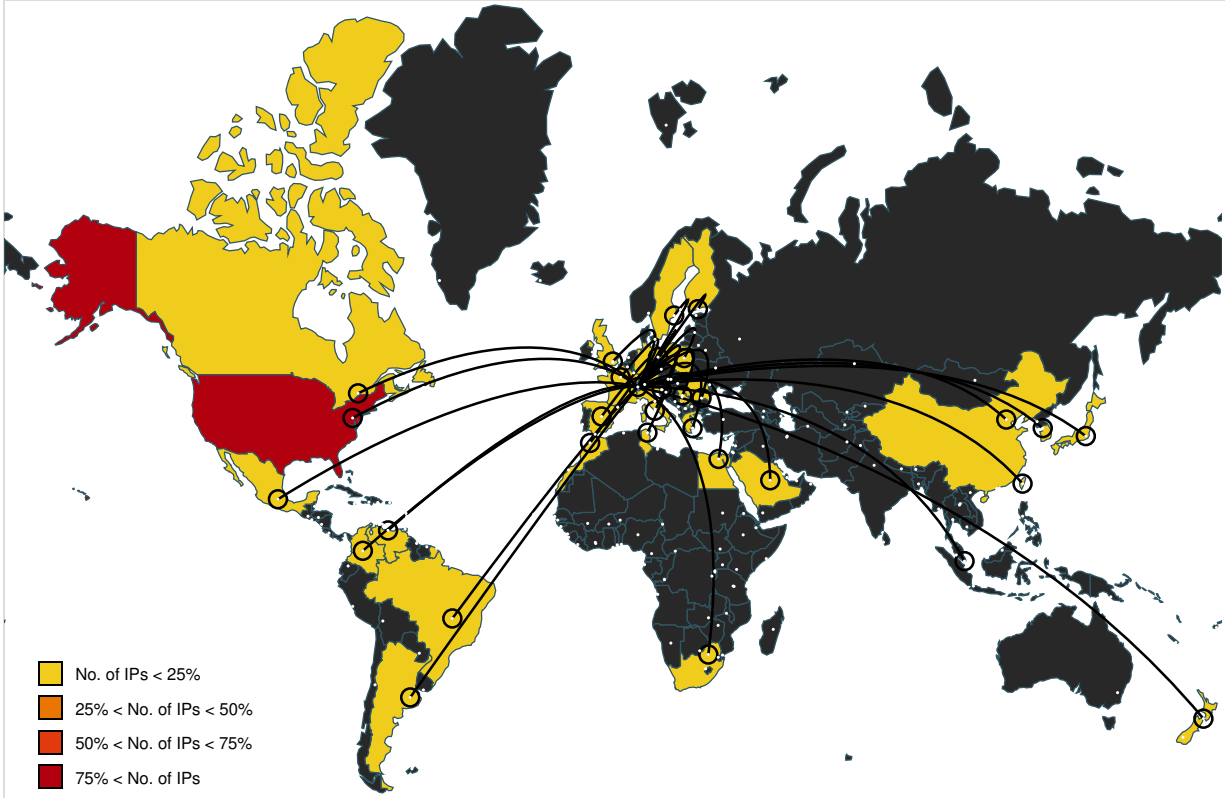
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	185.125.188.137	true	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.64.125.18	unknown	Sweden		1257	TELE2EU	false
8.191.184.106	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
95.85.184.203	unknown	Serbia		41897	SAT-TRAKT-ASSerbiaRS	false
134.233.55.94	unknown	United States		531	DNIC-AS-00531US	false
79.94.10.119	unknown	France		15557	LDCOMNETFR	false
84.235.13.218	unknown	Saudi Arabia		39386	STC-IGW-ASSA	false
91.71.90.179	unknown	France		15557	LDCOMNETFR	false
191.59.30.120	unknown	Brazil		53037	NEXTELTELECOMUNICACOESLTDABR	false
146.212.58.107	unknown	Slovenia		21283	A1SI-ASA1SlovenijaSI	false
146.74.246.103	unknown	United States		30051	SCCGOVUS	false
108.195.224.147	unknown	United States		7018	ATT-INTERNET4US	false
82.70.221.167	unknown	United Kingdom		13037	ZEN-ASZenInternet-UKGB	false
182.83.152.20	unknown	China		23771	SXBCTV-APSXBCTVInternetServiceProviderCN	false
179.44.30.144	unknown	Venezuela		22927	TelefonicadeArgentinaAR	false
178.81.153.30	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
182.159.32.133	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
181.62.19.186	unknown	Colombia		10620	TelmexColombiaSACO	false
175.133.231.226	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
93.127.226.11	unknown	Germany		8893	ARTFILES-ASZirkusweg1DE	false
86.251.252.159	unknown	France		3215	FranceTelecom-OrangeFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
93.236.153.202	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
154.109.4.240	unknown	Tunisia		37693	TUNISIANATN	false
210.45.218.227	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
174.158.74.84	unknown	United States		10507	SPCSUS	false
159.36.214.153	unknown	United States		30449	AZSTATEUS	false
193.38.245.173	unknown	unknown		48095	XTGLOBALRO	false
114.177.133.200	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
32.46.254.208	unknown	United States		7018	ATT-INTERNET4US	false
160.71.58.113	unknown	Finland		12582	TSF-DATANET-NGD-ASTeliaFinlandMPLSVPNServicesFI	false
38.127.94.201	unknown	United States		395657	HOPLITE-ASNUS	false
148.142.187.73	unknown	United States		3246	TDCSONGTele2BusinessTDCSwedenSE	false
182.209.214.210	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
187.134.132.168	unknown	Mexico		8151	UninetSAdeCVMX	false
104.29.0.189	unknown	United States		13335	CLOUDFLARENETUS	false
177.213.50.57	unknown	Brazil		26599	TELEFONICABRASILSABR	false
89.0.8.154	unknown	Germany		8422	NETCOLOGNEDE	false
156.146.251.185	unknown	United States		1448	UNITED-BROADBANDUS	false
221.170.13.52	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
183.44.54.20	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
161.16.211.75	unknown	United States		19512	LYONDELLUS	false
121.98.36.4	unknown	New Zealand		9790	VOCUSGROUPNZVocusGroupNZ	false
133.87.23.174	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
165.251.124.93	unknown	United States		6468	EASYLINK-AS6468US	false
19.82.2.24	unknown	United States		3	MIT-GATEWAYSUS	false
206.9.140.119	unknown	United States		5006	VOYANTUS	false
91.243.156.152	unknown	Spain		12479	UNI2-ASES	false
173.138.55.152	unknown	United States		10507	SPCSUS	false
85.45.125.176	unknown	Italy		3269	ASN-IBSNAZIT	false
94.76.139.152	unknown	Spain		29119	SERVIHOSTING-ASAireNetworksES	false
98.67.105.33	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
158.58.137.188	unknown	Italy		35485	NETWORK-ASIT	false
157.148.253.233	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
159.111.168.101	unknown	United States		33588	BRESNAN-33588US	false
186.180.66.223	unknown	Colombia		27831	ColombiaMovilCO	false
43.196.136.81	unknown	Japan		4249	LILLY-ASUS	false
54.75.118.199	unknown	United States		16509	AMAZON-02US	false
38.198.158.150	unknown	United States		174	COGENT-174US	false
110.7.174.169	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
181.108.163.110	unknown	Argentina		7303	TelecomArgentinaSAAR	false
200.98.219.216	unknown	Brazil		18479	UniversoOnlineSABR	false
154.139.176.182	unknown	Egypt		37069	MOBINILEG	false
72.71.77.95	unknown	United States		701	UUNETUS	false
135.61.120.207	unknown	United States		18676	AVAYAUS	false
152.45.109.45	unknown	United States		81	NCRENUS	false
99.151.3.166	unknown	United States		7018	ATT-INTERNET4US	false
159.21.68.105	unknown	United States		62195	MWH-UK-ASGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
48.64.241.78	unknown	United States		2686	ATGS-MMD-ASUS	false
90.228.230.195	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
192.58.117.187	unknown	United States		1970	TAMUS-NETUS	false
62.169.240.190	unknown	Greece		25472	WIND-ASGR	false
46.134.189.11	unknown	Poland		5617	TPNETPL	false
142.38.158.107	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
213.115.153.120	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
90.80.89.71	unknown	France		3215	FranceTelecom-OrangeFR	false
118.50.89.207	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
114.60.150.91	unknown	China		9812	CNNIC-CN-COLNETOrientalCableNetworkCoLtdCN	false
54.189.236.68	unknown	United States		16509	AMAZON-02US	false
27.94.222.135	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
139.65.39.81	unknown	United States		9905	LINKNET-ID-APLinknetASNID	false
97.121.78.118	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
116.224.242.13	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
49.109.141.211	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
35.45.46.4	unknown	United States		36375	UMICH-AS-5US	false
87.234.8.171	unknown	Germany		20676	PLUSNETDE	false
48.92.145.38	unknown	United States		2686	ATGS-MMD-ASUS	false
173.184.189.170	unknown	United States		7029	WINDSTREAMUS	false
180.203.190.167	unknown	China		9814	FIBRLINKBeijingFibrLINKNetworksCoLtdCN	false
203.133.111.90	unknown	Taiwan; Republic of China (ROC)		9416	MULTIMEDIA-AS-APHoshinMultimediaCenterIncTW	false
168.89.166.83	unknown	South Africa		3741	ISZA	false
109.98.17.156	unknown	Romania		9050	RTDBucharestRomaniaRO	false
192.91.253.231	unknown	United States		3356	LEVEL3US	false
160.168.238.214	unknown	Morocco		6713	IAM-ASMA	false
99.183.148.10	unknown	United States		7018	ATT-INTERNET4US	false
32.202.32.156	unknown	United States		2686	ATGS-MMD-ASUS	false
78.69.183.147	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
149.6.31.174	unknown	United States		174	COGENT-174US	false
108.54.61.23	unknown	United States		701	UUNETUS	false
144.220.240.208	unknown	United States		7896	NU-ASUS	false
164.122.183.106	unknown	United States		668	DNIC-AS-00668US	false
223.4.67.243	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	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):	6.853233537919337
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	IJB2Ub1KkE.elf
File size:	56'000 bytes
MD5:	4cb948a32c4ef20b6d74006938218277
SHA1:	8997b6216a149c550f86df86a8aad5c939594ff0
SHA256:	9ef61be75e7275c7fa42c1e68c533332bb580bcba297097cf230cacd8aa2298b
SHA512:	916e598f5a3a05da53b63796649d749c3a1970315b5c6835a155a6f1750bc86086bc4aa16181826bb1938878a199c286ae399d06b7290c892db2f8362aa400e4
SSDEEP:	768:XZame9eieaqteKc/ziVjwtGzdn048K86UwyFN36UVfvrC4CkoHuLC8v+79yfX:JamM33wa2VwtGGwyFN36UVHfQOLC8vl
TLSH:	00438E26C8299D94E10DC634BD784E741B23F00C9626AEF69E8786924053F7CFB993F1
File Content Preview:	.ELF.....*.....@.4...0.....4. ... (.....@...@.x...x.....|...|.A.|.A.t...d.....Q.td...../../"O.n.....#.*@.....#.*@.....o&O.n...l...../../.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	55600
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

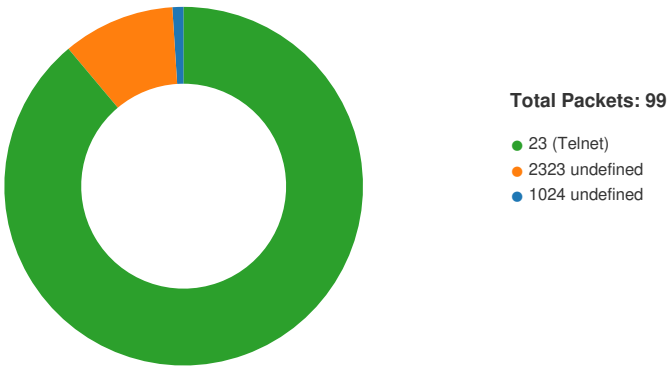
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xc700	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40c7e0	0xc7e0	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40c804	0xc804	0xf74	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41d77c	0xd77c	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41d784	0xd784	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41d790	0xd790	0x160	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x41d8f0	0xd8f0	0x2f0	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xd8f0	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	0xd778	0xd778	6.8957	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xd77c	0x41d77c	0x41d77c	0x174	0x464	0.8809	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 5, 2023 05:52:38.867073059 CEST	192.168.2.14	1.1.1.1	0x4e0e	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)	false
Sep 5, 2023 05:52:38.867162943 CEST	192.168.2.14	1.1.1.1	0xc038	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 5, 2023 05:52:38.886113882 CEST	1.1.1.1	192.168.2.14	0x4e0e	No error (0)	daisy.ubuntu.com		185.125.188.137	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 5, 2023 05:52:38.886113882 CEST	1.1.1.1	192.168.2.14	0x4e0e	No error (0)	daisy.ubuntu.com		185.125.188.136	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: IJB2Ub1KkE.elf PID: **5493**, Parent PID: **5402**

General

Start time:	03:49:56
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	/tmp/IJB2Ub1KkE.elf
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: IJB2Ub1KkE.elf PID: **5495**, Parent PID: **5493**

General

Start time:	03:49:56
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: IJB2Ub1KkE.elf PID: **5599**, Parent PID: **5495**

General

Start time:	03:52:43
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5603**, Parent PID: **5495**

General

Start time:	03:52:43
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5606**, Parent PID: **5603**

General

Start time:	03:52:43
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5615**, Parent PID: **5606**

General

Start time:	03:52:48
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5616**, Parent PID: **5606**

General

Start time:	03:52:48
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5608**, Parent PID: **5603**

General

Start time:	03:52:43
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5610**, Parent PID: **5603**

General

Start time:	03:52:44
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5496**, Parent PID: **5493**

General

Start time:	03:49:56
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5498**, Parent PID: **5493**

General

Start time:	03:49:56
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5501**, Parent PID: **5498**

General

Start time:	03:49:56
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: IJB2Ub1KkE.elf PID: **5598**, Parent PID: **5501**

General

Start time:	03:52:43
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5601**, Parent PID: **5501**

General

Start time:	03:52:43
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5502**, Parent PID: **5498**

General

Start time:	03:49:56
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: IJB2Ub1KkE.elf PID: **5505**, Parent PID: **5498**

General

Start time:	03:49:56
Start date:	05/09/2023
Path:	/tmp/IJB2Ub1KkE.elf
Arguments:	-
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9