ID: 513619
Sample Name: mipsel
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:45:13
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

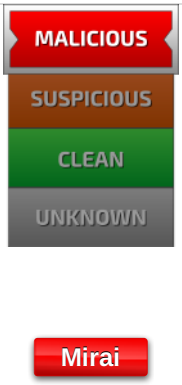
Linux Analysis Report mipsel

Overview

General Information

Sample Name:	mipsel
Analysis ID:	513619
MD5:	04b94c63425607..
SHA1:	a2165f05ecfce4f…
SHA256:	4fddb7884d4855b.
Tags:	Mirai
Infos:	

Detection

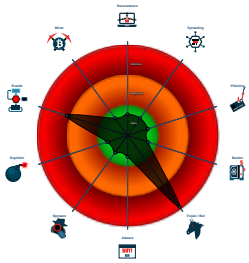


Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample deletes itself
- Uses known network protocols on no…
- Yara signature match
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…

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:	513619
Start date:	02.11.2021
Start time:	11:45:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mipsel
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:	mal100.troj.evad.lin@0/0@1/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- mipsel (PID: 5233, Parent: 5108, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/mipsel
  - mipsel New Fork (PID: 5235, Parent: 5233)
    - mipsel New Fork (PID: 5237, Parent: 5235)
    - mipsel New Fork (PID: 5238, Parent: 5235)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
mipsel	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x1d818:$x1: POST /cdn-cgi/ • 0x1cf60:$x3: /dev/watchdog • 0x1f793:$x5: .mdebug.abi32 • 0x1ff07:$x5: .mdebug.abi32 • 0x1d094:$s1: LCOGQGPTGP
mipsel	MAL_ELF_LNX_Mirai_Oct 10_2	Detects ELF malware Mirai related	Florian Roth	• 0x1d818:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 6 9 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
mipsel	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
mipsel	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
mipsel	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	

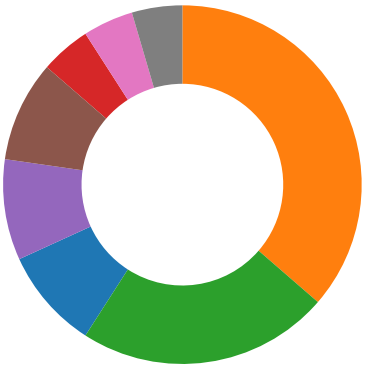
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5233.1.00000000e211a54b.00000000ea571adb.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x1d818:$x1: POST /cdn-cgi/ • 0x1cf60:$x3: /dev/watchdog • 0x1f793:$x5: .mdebug.abi32 • 0x1ff07:$x5: .mdebug.abi32 • 0x1d094:$s1: LCOGQGPTGP
5233.1.00000000e211a54b.00000000ea571adb.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct 10_2	Detects ELF malware Mirai related	Florian Roth	• 0x1d818:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 6 9 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
5233.1.00000000e211a54b.00000000ea571adb.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5233.1.00000000e211a54b.00000000ea571adb.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5233.1.00000000e211a54b.00000000ea571adb.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- 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:

Antivirus / Scanner detection for submitted sample

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:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Sample deletes itself

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

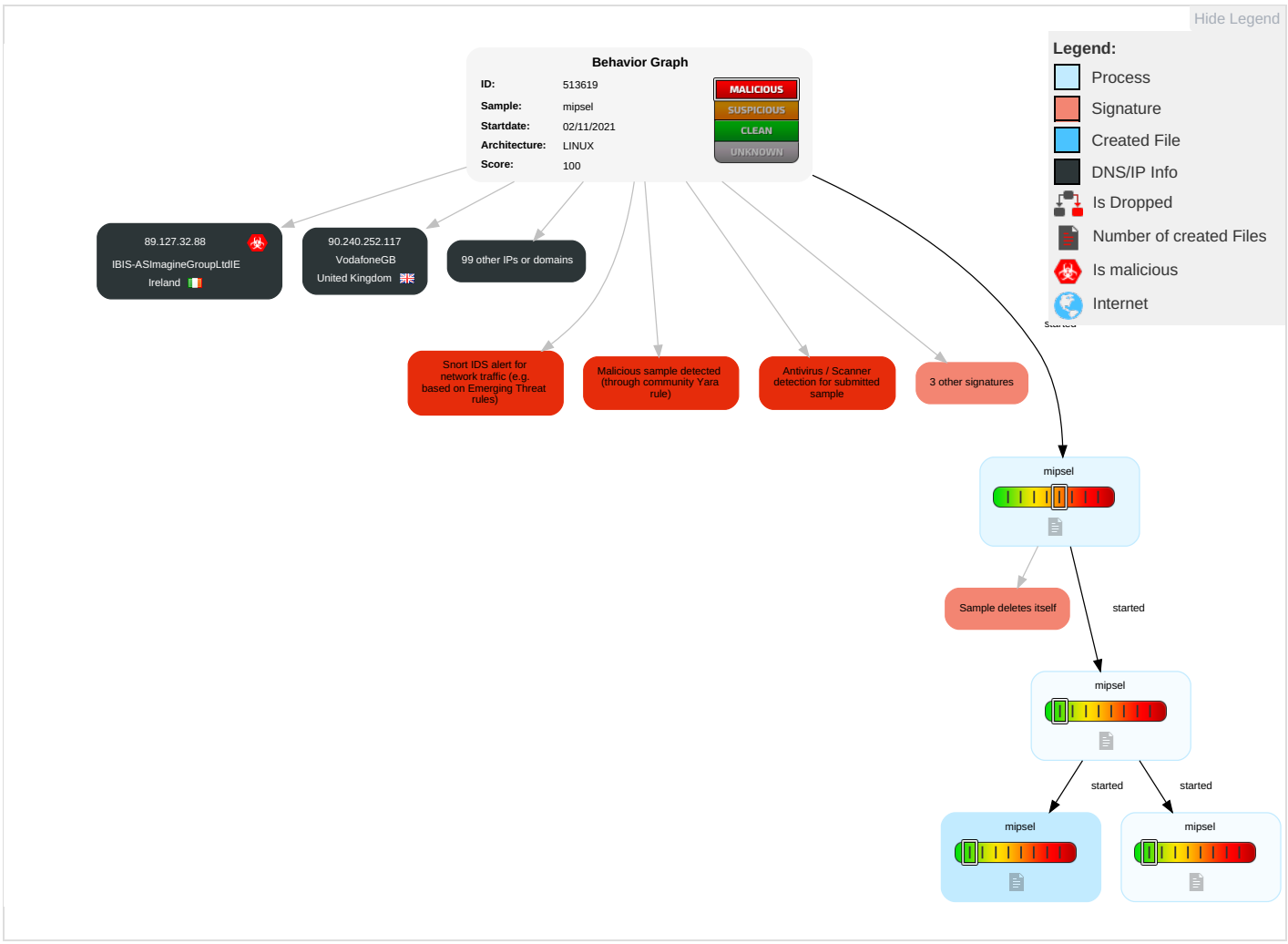
Mitre Att&ck Matrix

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	File Deletion 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	Modify System Partitio
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 Lockou
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	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
mipsel	29%	Metadefender		Browse
mipsel	65%	ReversingLabs	Linux.Trojan.Mirai	
mipsel	100%	Avira	LINUX/Mirai.bonb	

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
arcticboatz.cz	156.96.156.212	true	false		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
126.150.44.151	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
90.81.217.79	unknown	France		3215	FranceTelecom-OrangeFR	false
32.220.190.62	unknown	United States		46690	SNET-FCCUS	false
180.142.37.227	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
206.157.228.118	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
157.102.254.167	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
78.95.246.243	unknown	Saudi Arabia		39891	ALJAWWALSTC-ASSA	false
99.31.241.203	unknown	United States		7018	ATT-INTERNET4US	false
205.34.171.117	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
185.146.23.53	unknown	United States		55293	A2HOSTINGUS	false
25.138.111.88	unknown	United Kingdom		7922	COMCAST-7922US	false
92.55.152.37	unknown	Romania		39737	PRIME-TELECOM-ASRO	false
203.1.229.214	unknown	Australia		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
17.32.131.11	unknown	United States		714	APPLE-ENGINEERINGUS	false
52.13.176.234	unknown	United States		16509	AMAZON-02US	false
186.205.151.110	unknown	Brazil		28573	CLAROSABR	false
5.75.234.246	unknown	Germany		24940	HETZNER-ASDE	false
102.118.234.57	unknown	Mauritius		23889	MauritiusTelecomMU	false
111.134.166.239	unknown	China		24138	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
40.65.53.51	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
90.240.252.117	unknown	United Kingdom		5378	VodafoneGB	false
108.139.242.206	unknown	United States		16509	AMAZON-02US	false
32.190.163.250	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
44.36.244.222	unknown	United States		63479	HAMWANUS	false
142.91.37.47	unknown	United States		7203	LEASEWEB-USA-SFO-12US	false
161.96.213.124	unknown	Japan		7582	UMAC-AS-APUniversityofMacauMO	false
57.240.42.211	unknown	Belgium		2686	ATGS-MMD-ASUS	false
108.54.36.41	unknown	United States		701	UUNETUS	false
44.39.237.252	unknown	United States		7377	UCSDUS	false
72.155.240.173	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
213.51.218.89	unknown	Netherlands		33915	TNF-ASNL	false
126.74.201.174	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
134.90.40.201	unknown	Georgia		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	false
8.20.120.86	unknown	United States		13832	AS13832US	false
131.217.159.45	unknown	Australia		7573	UTASTheUniversityofTasmaniaAU	false
90.176.158.155	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	false
131.39.50.0	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
50.144.231.57	unknown	United States		7922	COMCAST-7922US	false
195.172.155.96	unknown	United Kingdom		4589	EASYNETEasynetGlobalServicesEU	false
186.253.51.2	unknown	Brazil		26615	TIMSABR	false
98.61.107.109	unknown	United States		7922	COMCAST-7922US	false
134.229.178.148	unknown	United States		27066	DNIC-ASBLK-27032-27159US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.239.13.14	unknown	Korea Republic of		9848	SEJONGTELECOM-AS-KRSejongTelecomKR	false
159.38.64.81	unknown	Sweden		19399	SLLNETEU	false
107.130.250.92	unknown	United States		7018	ATT-INTERNET4US	false
17.57.239.119	unknown	United States		714	APPLE-ENGINEERINGUS	false
111.61.56.107	unknown	China		24547	CMNET-V4HEBEI-AS-APHebeiMobileCommunicationCompanyLimit	false
85.64.123.47	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
116.188.238.135	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
129.154.242.2	unknown	United States		7160	NETDYNAMICSUS	false
122.57.38.135	unknown	New Zealand		4771	SPARKNZSparkNewZealandTradingLtdNZ	false
190.187.141.157	unknown	Peru		19180	AMERICATELPERUSAPE	false
110.9.24.108	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
154.134.132.111	unknown	Egypt		37069	MOBINILEG	false
89.127.32.88	unknown	Ireland		25441	IBIS-ASImagineGroupLtdIE	true
185.213.254.236	unknown	Israel		205564	INFINIDATIL	false
48.185.111.80	unknown	United States		2686	ATGS-MMD-ASUS	false
105.244.205.35	unknown	South Africa		36994	Vodacom-VBZA	false
103.236.165.144	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
134.184.14.239	unknown	Belgium		2611	BELNETBE	false
155.48.84.66	unknown	United States		16481	BABSON-GNETUS	false
143.16.48.49	unknown	United States		264008	LANCAMANTOANISERVICOSDEINFORMATICALTDA-MEBR	false
183.88.253.138	unknown	Thailand		45758	TRIPLETNET-AS-APTripleTInternetTripleTBroadbandTH	false
61.214.172.207	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
73.69.38.23	unknown	United States		7922	COMCAST-7922US	false
207.90.126.112	unknown	United States		7321	LNET-ASNUS	false
42.76.124.102	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false
124.144.158.102	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
84.103.32.251	unknown	France		15557	LDCOMNETFR	false
171.43.62.146	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
45.255.61.36	unknown	China		132116	ANINETWORK-INAniNetworkPvtLtdIN	false
147.132.235.1	unknown	Australia		9650	CITEC-AU-APQLDGovernmentBusinessITAU	false
89.19.50.206	unknown	United Kingdom		61317	ASDETUKhttpwwwheficedcomGB	false
12.79.50.235	unknown	United States		7018	ATT-INTERNET4US	false
117.33.176.38	unknown	China		134768	CHINANET-SHAANXI-CLOUD-BASECHINANETSHAANXIprovinceCloud	false
106.178.155.250	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
40.65.77.63	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
198.84.178.65	unknown	Canada		5645	TEKSAVVYCA	false
52.203.21.38	unknown	United States		14618	AMAZON-AESUS	false
129.111.117.191	unknown	United States		26971	UTHSCSA-ASUS	false
89.107.90.194	unknown	Italy		39808	FONTELIT	false
197.16.212.62	unknown	Tunisia		37693	TUNISIANATN	false
95.144.4.23	unknown	United Kingdom		12576	EELtdGB	false
121.177.161.98	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
170.249.52.241	unknown	Canada		46618	DERYTELECOMCA	false
193.77.13.181	unknown	Slovenia		5603	SIOL-NETTelekomSlovenijeddSI	false
206.133.109.184	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
150.40.81.17	unknown	Japan		9991	SHUDO-UHiroshimaShudoUniversityJP	false
96.254.22.112	unknown	United States		5650	FRONTIER-FRTRUS	false
168.153.203.148	unknown	Australia		2764	AAPTAAPTLimitedAU	false
129.164.153.209	unknown	United States		297	AS297US	false
150.185.168.226	unknown	Venezuela		23007	UniversidaddeLosAndesVE	false
32.252.141.152	unknown	United States		2686	ATGS-MMD-ASUS	false
110.243.246.254	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
179.34.244.156	unknown	Brazil		26615	TIMSABR	false
178.9.146.143	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
178.229.218.209	unknown	Netherlands		31615	TMO-NL-ASNL	false
9.120.138.185	unknown	United States		3356	LEVEL3US	false
221.72.28.138	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
199.143.223.121	unknown	United States		4152	USDA-1US	false

Runtime Messages

Command:	/tmp/mipsel
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	qazwsxedc
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
44.36.244.222	mipsel	Get hash	malicious	Browse	
111.134.166.239	PTn4GPy1jh	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
arcticboatz.cz	arm-20211102-0937	Get hash	malicious	Browse	• 156.96.156.212
	mips-20211102-0937	Get hash	malicious	Browse	• 156.96.156.212
	arm5-20211102-0937	Get hash	malicious	Browse	• 156.96.156.212
	arm7	Get hash	malicious	Browse	• 156.96.156.212
	x86_64	Get hash	malicious	Browse	• 156.96.156.212
	arm	Get hash	malicious	Browse	• 156.96.156.212
	x86_64	Get hash	malicious	Browse	• 156.96.156.212
	mips	Get hash	malicious	Browse	• 156.96.156.212
	arm6	Get hash	malicious	Browse	• 156.96.156.212
	arm7	Get hash	malicious	Browse	• 156.96.156.212
	arm5	Get hash	malicious	Browse	• 156.96.156.212

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GIGAINFRASoftbankBBCorpJP	arm-20211102-0937	Get hash	malicious	Browse	• 219.19.55.98
	sora.mpsl	Get hash	malicious	Browse	• 221.24.188.7
	sora.arm7	Get hash	malicious	Browse	• 60.156.178.255
	sora.x86	Get hash	malicious	Browse	• 219.55.17.249
	arm5-20211102-0937	Get hash	malicious	Browse	• 126.13.86.242
	zJk9UEOnQ7	Get hash	malicious	Browse	• 126.11.178.137
	MkyxPXGeTq	Get hash	malicious	Browse	• 126.59.74.157
	TlhOKlVSwf	Get hash	malicious	Browse	• 60.112.223.214
	Hilix.arm	Get hash	malicious	Browse	• 219.56.220.39
	BsXhlyIHzC	Get hash	malicious	Browse	• 220.50.151.236
	L831wSjET5	Get hash	malicious	Browse	• 112.136.40.250
	JVHk2b1Yd5	Get hash	malicious	Browse	• 219.54.86.103
	vRjXKh3l4n	Get hash	malicious	Browse	• 221.49.205.112
	WhFNix8BoE	Get hash	malicious	Browse	• 219.209.16 9.141
	aTQ4RalkUs	Get hash	malicious	Browse	• 219.56.219.26
	RPov9E0iot	Get hash	malicious	Browse	• 60.93.119.210
	8VANaS473t	Get hash	malicious	Browse	• 218.130.99.202
	yVbcX1sEtS	Get hash	malicious	Browse	• 221.55.216.106
	oiHTZaiKnl	Get hash	malicious	Browse	• 126.225.22 3.207
	SZAYTvvY9Y	Get hash	malicious	Browse	• 126.28.125.143
SNET-FCCUS	Ko84iLip1u	Get hash	malicious	Browse	• 32.221.121.104
	st2AAeCXsR	Get hash	malicious	Browse	• 32.219.214.98
	b3astmode.x86	Get hash	malicious	Browse	• 32.217.213.72
	8jfOcvTqQA	Get hash	malicious	Browse	• 32.212.157.51
	pandora.x86	Get hash	malicious	Browse	• 32.215.59.28
	hoho.arm	Get hash	malicious	Browse	• 32.212.164.173
	jew.x86	Get hash	malicious	Browse	• 32.217.201.238
	FbdUX5aU1N	Get hash	malicious	Browse	• 32.209.63.199
	G5vJ46b8cw	Get hash	malicious	Browse	• 32.221.121.129
	8h5TwcAsZi	Get hash	malicious	Browse	• 32.218.103.129
	Mun376v3Zy	Get hash	malicious	Browse	• 32.217.12.22
	rLGunciziY	Get hash	malicious	Browse	• 32.217.237.22
	wXGm2SnAnh	Get hash	malicious	Browse	• 32.219.9.75
	sSQ2BB4tyb	Get hash	malicious	Browse	• 32.223.212.248
	EKDuLCqKpg.dll	Get hash	malicious	Browse	• 32.213.40.128
	22693dBj8t	Get hash	malicious	Browse	• 32.212.116.201
	8kYSWVCyyy	Get hash	malicious	Browse	• 32.220.131.207
	0sf31umxYW	Get hash	malicious	Browse	• 32.213.34.91
	b3astmode.arm	Get hash	malicious	Browse	• 32.216.146.6
	mips	Get hash	malicious	Browse	• 32.211.0.224
FranceTelecom-OrangeFR	sora.arm7	Get hash	malicious	Browse	• 90.33.138.8
	sora.x86	Get hash	malicious	Browse	• 90.15.207.49
	sora.mips	Get hash	malicious	Browse	• 90.35.131.168
	sora.arm5	Get hash	malicious	Browse	• 90.117.147.103
	mips-20211102-0937	Get hash	malicious	Browse	• 109.218.10.134
	MkyxPXGeTq	Get hash	malicious	Browse	• 163.114.42.115
	TlhOKlVSwf	Get hash	malicious	Browse	• 83.114.43.82
	Hilix.arm	Get hash	malicious	Browse	• 90.70.5.162
	L831wSjET5	Get hash	malicious	Browse	• 90.65.125.251
	JVHk2b1Yd5	Get hash	malicious	Browse	• 90.40.164.3
	WhFNix8BoE	Get hash	malicious	Browse	• 86.222.195.131
	Hilix.x86	Get hash	malicious	Browse	• 83.195.96.18
	o6aMoZKsIK	Get hash	malicious	Browse	• 90.126.70.98
	yVbcX1sEtS	Get hash	malicious	Browse	• 92.163.220.65
	Ko84iLip1u	Get hash	malicious	Browse	• 90.67.227.39
	arH2Af5qoc	Get hash	malicious	Browse	• 90.22.85.198
	t7WU0JjLAR	Get hash	malicious	Browse	• 83.114.112.88
	FGVOkw9did	Get hash	malicious	Browse	• 86.229.55.251
	I5A5LzSAql	Get hash	malicious	Browse	• 62.160.230.46
	P8AVd483d7	Get hash	malicious	Browse	• 81.48.247.242

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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.601050973810184
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	mipsel
File size:	146516
MD5:	04b94c63425607f5f58ebd51578dd8e8
SHA1:	a2165f05ecfce4f95f6afc61574361e6db9b2a43
SHA256:	4fddb7884d4855b8b1864825992139fd2b29d46c198b436ec33e2beb0a2f1e2
SHA512:	4924a4b7fb9b8d5cfe823bca0bd0b6b126e999607b45095a7e8658d4e2fe7d16ccb0171ef4c9ba39e1626b9a2fe7c64431021e8c14a0e73249795bbc09d6f31c
SSDEEP:	3072:g8GGdBiE2+IUJ0PbzCwbZnV+6nTmzWfiPklK:u+BipQ0PbmwRVnTmzWTK
File Content Preview:	.ELF.....`.@.4...L:.....4. ...(.....@...@..$...$.....0...0F..0F.....p-.....Q.td.....<...'!.....'.....<...'!... .....9'.. .....<h..'!.....`.9

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:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	145996
Section Header Size:	40
Number of Section Headers:	13
Header String Table Index:	12

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	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x1cdb0	0x0	0x6	AX	0	0	16

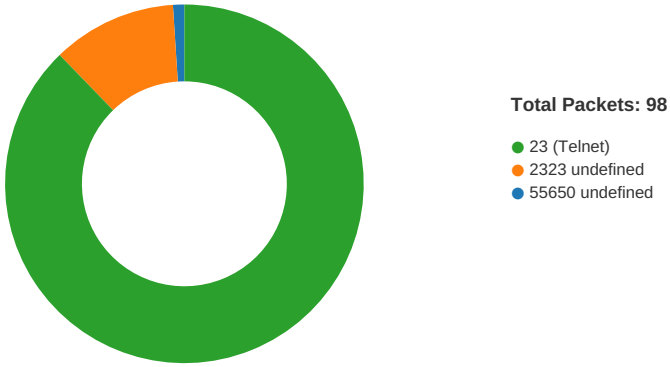
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.fini	PROGBITS	0x41ced0	0x1ced0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x41cf30	0x1cf30	0x5580	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x463000	0x23000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x463008	0x23008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x463014	0x23014	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x463020	0x23020	0x540	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x463560	0x23560	0x494	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x4639f4	0x239f4	0x2c	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x463a20	0x239f4	0x2350	0x0	0x3	WA	0	0	16
.shstrtab	STRTAB	0x0	0x239f4	0x56	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	0x224b0	0x224b0	3.6825	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x23000	0x463000	0x463000	0x9f4	0x2d70	2.6821	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .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
Nov 2, 2021 11:45:58.809940100 CET	192.168.2.23	8.8.8.8	0x78b0	Standard query (0)	arcticboatz.cz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 11:45:58.829411983 CET	8.8.8.8	192.168.2.23	0x78b0	No error (0)	arcticboatz.cz		156.96.156.212	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: mipsel PID: 5233 Parent PID: 5108

General

Start time:	11:45:57
Start date:	02/11/2021
Path:	/tmp/mipsel
Arguments:	/tmp/mipsel
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Deleted

File Read

Analysis Process: mipsel PID: 5235 Parent PID: 5233

General

Start time:	11:45:57
Start date:	02/11/2021
Path:	/tmp/mipsel
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: mipsel PID: 5237 Parent PID: 5235

General

Start time:	11:45:57
Start date:	02/11/2021
Path:	/tmp/mipsel
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: mipsel PID: 5238 Parent PID: 5235

General

Start time:	11:45:57
Start date:	02/11/2021
Path:	/tmp/mipsel
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated