ID: 518272
Sample Name: arm5
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:48:16
Date: 09/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

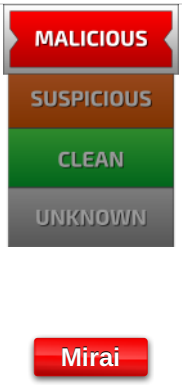
Linux Analysis Report arm5

Overview

General Information

Sample Name:	arm5
Analysis ID:	518272
MD5:	70988ec41b6edd..
SHA1:	60af6f0fee0df7ff9..
SHA256:	1d91574bc880dfb.
Tags:	Mirai
Infos:	

Detection

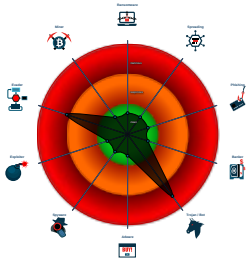


Score:	96
Range:	0 - 100
Whitelisted:	false

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:	518272
Start date:	09.11.2021
Start time:	09:48:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	arm5
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:	mal96.troj.evad.lin@0/0@1/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- arm5 (PID: 5246, Parent: 5120, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm5
  - arm5 New Fork (PID: 5248, Parent: 5246)
    - arm5 New Fork (PID: 5250, Parent: 5248)
    - arm5 New Fork (PID: 5252, Parent: 5248)
- **cleanup**

Yara Overview

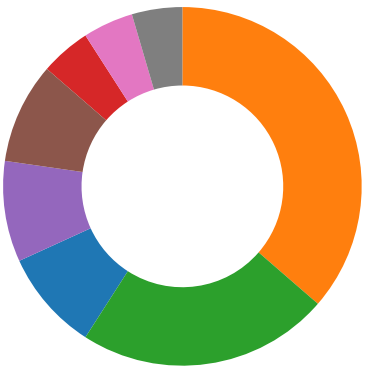
Initial Sample

Source	Rule	Description	Author	Strings
arm5	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x12308:$x1: POST /cdn-cgi/ • 0x11940:$x3: /dev/watchdog • 0x11a74:$s1: LCOGQGPTGP • 0x124a4:$s3: CFOKLKQVPCVMP • 0x12488:$s4: QWRGPTKQMP • 0x125ac:$s5: HWCLVGAJ
arm5	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x12308:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 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
arm5	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
arm5	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5246.1.000000006d4b7060.0000000092f9e265.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x12308:$x1: POST /cdn-cgi/ • 0x11940:$x3: /dev/watchdog • 0x11a74:$s1: LCOGQGPTGP • 0x124a4:$s3: CFOKLKQVPCVMP • 0x12488:$s4: QWRGPTKQMP • 0x125ac:$s5: HWCLVGAJ
5246.1.000000006d4b7060.0000000092f9e265.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x12308:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 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
5246.1.000000006d4b7060.0000000092f9e265.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5246.1.000000006d4b7060.0000000092f9e265.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

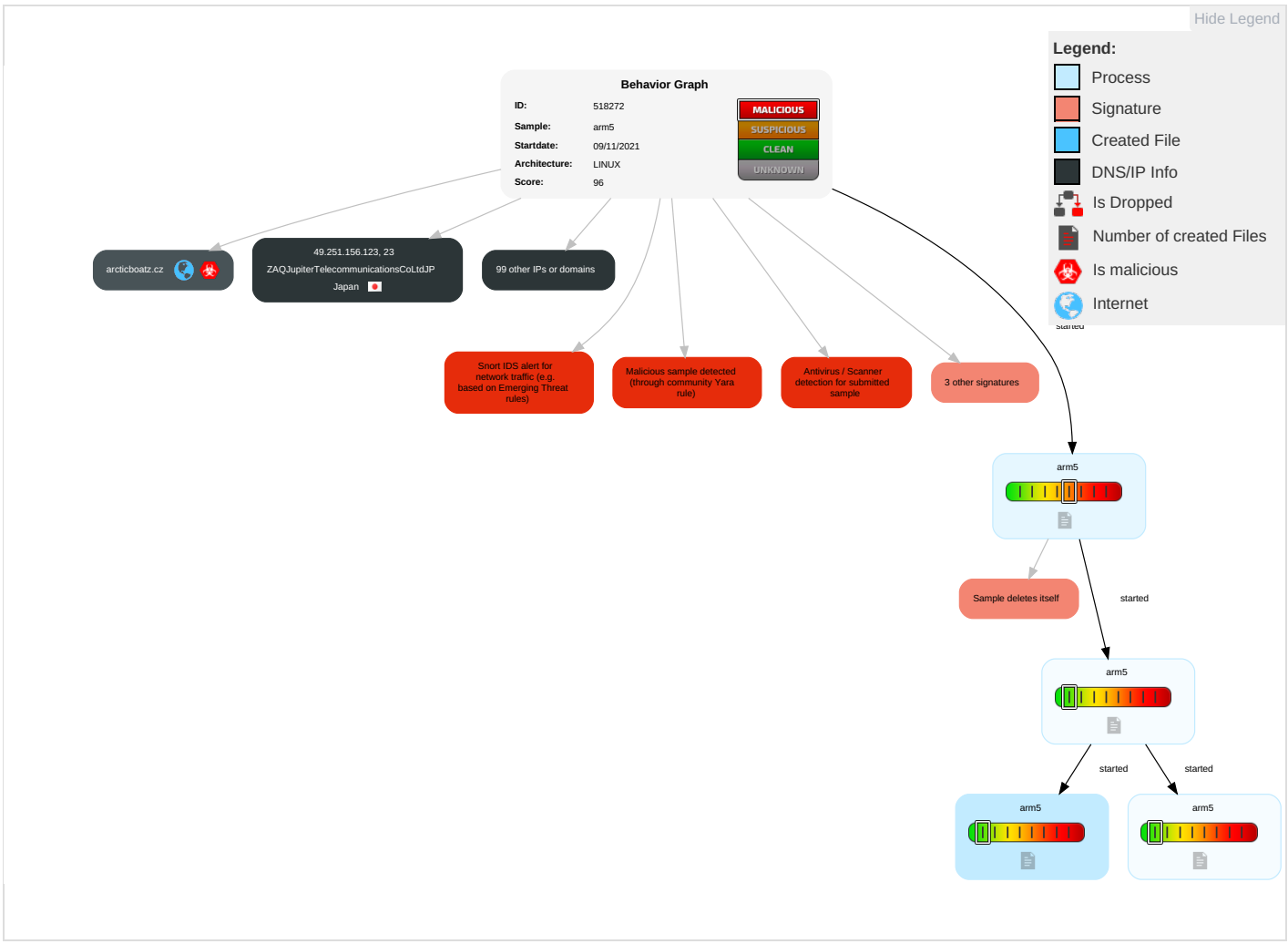
Mitre Att&ck Matrix

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
arm5	40%	ReversingLabs	Linux.Trojan.Mirai	
arm5	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
arcticboatz.cz	1%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
arcticboatz.cz	156.96.62.207	true	true	• 1%, Virustotal, Browse	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.135.187.226	unknown	United States		36384	GOOGLE-ITUS	false
181.206.182.194	unknown	Colombia		27831	ColombiaMovilCO	false
205.105.248.57	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
24.80.107.102	unknown	Canada		6327	SHAWCA	false
145.55.136.81	unknown	United Kingdom		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
176.65.156.36	unknown	Germany		12975	PALTEL-ASPALTELAutonomousSystemPS	false
147.197.175.135	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
125.194.170.24	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
148.134.167.57	unknown	United States		19113	DUKE-ENERGYUS	false
85.89.50.115	unknown	Estonia		3249	ESTPAKEE	false
208.8.240.71	unknown	United States		1239	SPRINTLINKUS	false
185.147.110.118	unknown	United Kingdom		39875	W3ZGB	false
60.213.130.181	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
207.96.101.22	unknown	United States		6079	RCN-ASUS	false
146.55.106.179	unknown	United States		1483	DNIC-AS-01483US	false
153.162.160.177	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
42.211.12.113	unknown	China		4249	LILLY-ASUS	false
195.212.106.195	unknown	European Union		2686	ATGS-MMD-ASUS	false
83.147.173.205	unknown	Ireland		31122	DIGIWEB-ASIE	false
207.54.208.193	unknown	United States		17327	TSTC-ASUS	false
135.212.234.61	unknown	United States		14962	NCR-252US	false
89.76.227.225	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
151.30.121.245	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
190.208.152.163	unknown	Chile		6535	TelmexServiciosEmpresarialesSACL	false
68.157.177.173	unknown	United States		7018	ATT-INTERNET4US	false
141.170.46.168	unknown	United Kingdom		33920	AQLGB	false
114.238.102.79	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
198.111.4.221	unknown	United States		237	MERIT-AS-14US	false
54.133.167.10	unknown	United States		14618	AMAZON-AESUS	false
116.179.161.1	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
140.132.219.138	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
122.148.149.229	unknown	Australia		9443	VOCUS-RETAIL-AUVocusRetailAU	false
63.155.197.137	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
172.57.247.170	unknown	United States		21928	T-MOBILE-AS21928US	false
222.105.112.87	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
176.94.185.164	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
80.7.112.162	unknown	United Kingdom		5089	NTLGB	false
190.11.161.12	unknown	Argentina		13585	PowerVTSAAR	false
162.223.220.198	unknown	United States		55193	LRC-EV-ASNUS	false
73.162.72.27	unknown	United States		7922	COMCAST-7922US	false
104.191.76.16	unknown	United States		7018	ATT-INTERNET4US	false
105.51.135.23	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
91.202.135.49	unknown	Ukraine		44686	SETI-KR-ASUA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.223.11.65	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
144.21.119.168	unknown	Sweden		43894	ORCL-LON-OPC1GB	false
188.51.210.128	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
89.69.52.32	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
20.121.188.50	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
67.112.215.224	unknown	United States		7018	ATT-INTERNET4US	false
74.134.117.69	unknown	United States		10796	TWC-10796-MIDWESTUS	false
101.100.86.131	unknown	New Zealand		17492	VECTOR-COMMUNICATIONS-ASVectorCommunicationsLTDNZ	false
220.242.93.217	unknown	China		7545	TPG-INTERNET-APTPGTelecomLimitedAU	false
80.16.103.39	unknown	Italy		3269	ASN-IBSNAZIT	false
210.134.248.240	unknown	Japan		2512	TCP-NETTCPIncJP	false
206.112.34.148	unknown	United States		701	UUNETUS	false
110.177.120.171	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
210.80.246.120	unknown	Japan		703	UUNETUS	false
189.12.139.117	unknown	Brazil		7738	TelemarNorteLesteSABR	false
52.46.216.113	unknown	United States		16509	AMAZON-02US	false
53.45.213.229	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
49.251.156.123	unknown	Japan		9617	ZAQJupiterTelecommunicationsCoLtdJP	false
218.99.251.246	unknown	China		17966	CIBNChinaInformationBroadcastNetworkLtdCoCN	false
107.164.229.1	unknown	United States		18779	EGIHOSTINGUS	false
156.191.191.174	unknown	Egypt		36992	ETISALAT-MISREG	false
14.190.39.89	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
70.80.242.95	unknown	Canada		5769	VIDEOTRONCA	false
108.220.13.87	unknown	United States		7018	ATT-INTERNET4US	false
82.117.30.135	unknown	Liechtenstein		35223	HOI-ASLI	false
48.161.123.249	unknown	United States		2686	ATGS-MMD-ASUS	false
103.92.222.136	unknown	Australia		59362	KSNETWORK-AS-APKSNetworkLimitedBD	false
162.137.210.24	unknown	United States		35893	ACPCA	false
155.166.228.100	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
192.236.209.63	unknown	United States		54290	HOSTWINDSUS	false
51.188.186.25	unknown	United States		2686	ATGS-MMD-ASUS	false
169.31.110.75	unknown	United States		37611	AfrihostZA	false
187.46.7.181	unknown	Brazil		26615	TIMSABR	false
147.14.174.55	unknown	Sweden		41076	POSTDK-ASDK	false
39.113.92.254	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
126.250.62.250	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
193.184.243.21	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
52.85.81.84	unknown	United States		16509	AMAZON-02US	false
130.188.48.244	unknown	Finland		565	VTT-ASVTTautonomoussystemFI	false
132.110.95.166	unknown	United States		306	DNIC-ASBLK-00306-00371US	false
59.180.132.79	unknown	India		17813	MTNL-APMahanagarTelephoneNigamLimitedIN	false
44.182.104.79	unknown	United States		58247	NETVEILLANCERO	false
164.54.69.130	unknown	United States		683	ARGONNE-ASUS	false
222.203.192.190	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
42.146.84.216	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.128.6.77	unknown	Guam		3605	ERX-KUENTOS-ASGuamCablevisionLLCGU	false
179.66.21.100	unknown	Brazil		7738	TelemarNorteLesteSABR	false
122.78.96.93	unknown	China		63711	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
179.186.80.236	unknown	Brazil		18881	TELEFONICABRASILSABR	false
107.229.88.133	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
221.127.190.120	unknown	Hong Kong		9304	HUTCHISON-AS-APHGCGlobalCommunicationsLimitedHK	false
175.65.29.176	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
81.222.205.171	unknown	Russian Federation		20597	ELTEL-ASRU	false
134.16.105.217	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
167.181.125.128	unknown	United States		59447	SAYFANETTR	false
195.201.97.179	unknown	Germany		24940	HETZNER-ASDE	false
31.168.46.82	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false

Runtime Messages

Command:	/tmp/arm5
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	qazwsxedc
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
arcticboatz.cz	mipsel	Get hash	malicious	Browse	• 156.96.156.212
	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
GOOGLE-ITUS	B94t90Yyoz	Get hash	malicious	Browse	• 104.135.140.227
	H9pX0VKTN5	Get hash	malicious	Browse	• 104.134.26.50
	WZ4DVF29Pb	Get hash	malicious	Browse	• 104.133.236.16

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dark.arm	Get hash	malicious	Browse	• 104.133.236.10
	1u1hBVyy1i	Get hash	malicious	Browse	• 104.132.49.89
	h8RVQktJXr	Get hash	malicious	Browse	• 104.135.213.96
	x86	Get hash	malicious	Browse	• 104.132.50.73
	b3astmode.arm-20211011-1850	Get hash	malicious	Browse	• 104.132.49.83
	4oihqZr8ZO	Get hash	malicious	Browse	• 104.132.98.38
	sora.arm	Get hash	malicious	Browse	• 104.134.12 6.113
	v17c18jKB5	Get hash	malicious	Browse	• 104.132.49.98
	TwlnaihoCK	Get hash	malicious	Browse	• 104.134.3.160
	L5KEcDLI8h	Get hash	malicious	Browse	• 104.133.200.93
	3olJHpiKNe	Get hash	malicious	Browse	• 104.132.49.84
	TDiJdXdD3P	Get hash	malicious	Browse	• 104.135.23 9.184
	fhDiUHnkzb	Get hash	malicious	Browse	• 104.132.49.86
	ImxKJKBtj2	Get hash	malicious	Browse	• 104.135.3.18
	dark.x86	Get hash	malicious	Browse	• 104.133.42.167
	gaxq7wN4q8	Get hash	malicious	Browse	• 104.132.98.31
	ICNMnez5oh	Get hash	malicious	Browse	• 104.132.49.77
ColombiaMovilCO	qgxgn5fQU1	Get hash	malicious	Browse	• 181.207.246.79
	fMGehkjmPv	Get hash	malicious	Browse	• 179.14.232.136
	mktkJhN1Fd	Get hash	malicious	Browse	• 181.205.49.119
	FAuA0G2obM	Get hash	malicious	Browse	• 191.89.251.32
	WcBBoVjwRf	Get hash	malicious	Browse	• 186.97.100.240
	7L38cWaJpW	Get hash	malicious	Browse	• 177.252.114.31
	NEaRhAVeo9	Get hash	malicious	Browse	• 186.181.19 4.128
	mRQwOz6Oit	Get hash	malicious	Browse	• 191.88.9.118
	pTF1ilCUEm	Get hash	malicious	Browse	• 179.12.77.61
	yJOZ3EeESV	Get hash	malicious	Browse	• 186.181.19 4.104
	apep.x86	Get hash	malicious	Browse	• 181.204.13 1.151
	LpX6muTZ4z.exe	Get hash	malicious	Browse	• 191.91.177.6
	en94piXmL6	Get hash	malicious	Browse	• 181.71.150.166
	wRmHCEnowl	Get hash	malicious	Browse	• 181.207.21 2.149
	pwFaKVCXrY	Get hash	malicious	Browse	• 181.204.13 1.145
	elmb49ofup	Get hash	malicious	Browse	• 181.204.13 1.153
	HCyigyiCAH	Get hash	malicious	Browse	• 181.71.150.145
	apep.x86	Get hash	malicious	Browse	• 181.205.208.46
	yOtRXukeq9	Get hash	malicious	Browse	• 181.204.13 1.157
	SecuriteInfo.com.Linux.Mirai.1429.15365.3177	Get hash	malicious	Browse	• 181.204.13 1.169

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, ARM, version 1 (ARM), s tatically linked, stripped
Entropy (8bit):	6.145315108312535
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm5
File size:	80604
MD5:	70988ec41b6eddb41ec1bc3222f8fab8
SHA1:	60af6f0fee0df7ff9e51c0f9f6070ba102f430a8
SHA256:	1d91574bc880dfb70eb8aaa3d3bc75d906bdb7b87f8ee3c 3467a2ed3267e1047
SHA512:	ca6d8462fadcfc0e8f23f9546282b8239f9aef68c9bf26bcd 4de9ba766c855819c7bcca13e491eb0d6bccaf96eb8ead 396b79c1300b0653b9323aac400800e69
SSDEEP:	1536:At/1/M1UUI6MdbCfysm4mhtVTh2nt+WP+IMZqXk hAiSaSderwbZn9:AtxS8dWfs4mVh2nXPbGqXk/RSmwb Zn9
File Content Preview:	.ELF...a.....(.....4...L9.....4. ...(.....5...5.... .....5...5...5..p....&.....Q.td.....-... L."....F.....0@-.\P...0....S.0...P@...0... ....R.....0...0..... .....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x2
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	80204
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

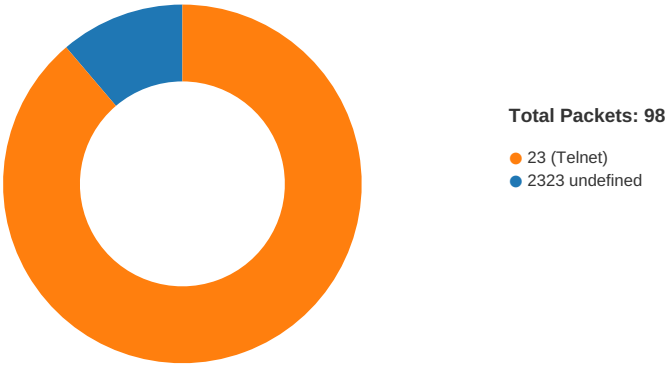
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x11844	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x198f4	0x118f4	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x19908	0x11908	0x1c90	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x2359c	0x1359c	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x235a4	0x135a4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x235b0	0x135b0	0x35c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x2390c	0x1390c	0x2358	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1390c	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	0x8000	0x8000	0x13598	0x13598	3.4378	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x1359c	0x2359c	0x2359c	0x370	0x26c8	1.6461	0x6	RW	0x8000		.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
Nov 9, 2021 09:49:04.040237904 CET	192.168.2.23	8.8.8.8	0x67b	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 9, 2021 09:49:04.069693089 CET	8.8.8.8	192.168.2.23	0x67b	No error (0)	arcticboatz.cz		156.96.62.207	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: arm5 PID: 5246 Parent PID: 5120

General

Start time:	09:49:02
Start date:	09/11/2021
Path:	/tmp/arm5
Arguments:	/tmp/arm5
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Deleted

File Read

Analysis Process: arm5 PID: 5248 Parent PID: 5246

General

Start time:	09:49:03
Start date:	09/11/2021
Path:	/tmp/arm5
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm5 PID: 5250 Parent PID: 5248

General

Start time:	09:49:03
Start date:	09/11/2021
Path:	/tmp/arm5
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm5 PID: 5252 Parent PID: 5248

General

Start time:	09:49:03
Start date:	09/11/2021
Path:	/tmp/arm5
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated