ID: 557499
Sample Name: arm5
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 08:30:06
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

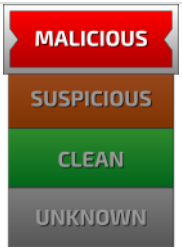
arm5

Overview

General Information

Sample Name:	arm5
Analysis ID:	557499
MD5:	b2499605d6cb98..
SHA1:	25c3039bf8fdb88..
SHA256:	7b876157fd5cc9…
Tags:	Mirai
Infos:	

Detection



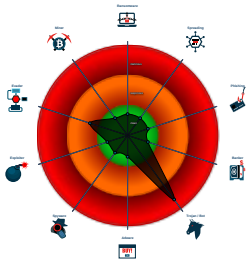
Mirai Moobot

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic (e…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Moobot
- Sets full permissions to files and/or …
- Yara signature match
- Executes the "mkdir" command use…
- Uses the "uname" system call to qu…
- Executes the "chmod" command us…

Classification



Analysis Advice

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 only run correctly on MIPS or ARM architectures

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:	557499
Start date:	21.01.2022
Start time:	08:30:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 57s
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:	mal100.troj.lin@0/0@1/0

Warnings

Runtime Messages

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

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- arm5 (PID: 5223, Parent: 5117, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm5
  - arm5 New Fork (PID: 5225, Parent: 5223)
  - sh (PID: 5225, Parent: 5223, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/arm5 bin/systemd; chmod 777 bin/systemd"
    - sh New Fork (PID: 5227, Parent: 5225)
    - rm (PID: 5227, Parent: 5225, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/systemd
    - sh New Fork (PID: 5228, Parent: 5225)
    - mkdir (PID: 5228, Parent: 5225, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 5229, Parent: 5225)
    - mv (PID: 5229, Parent: 5225, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/arm5 bin/systemd
    - sh New Fork (PID: 5230, Parent: 5225)
    - chmod (PID: 5230, Parent: 5225, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/systemd
  - arm5 New Fork (PID: 5231, Parent: 5223)
    - arm5 New Fork (PID: 5233, Parent: 5231)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
arm5	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x11fb0:$x1: POST /cdn-cgi/ • 0x11530:$x3: /dev/watchdog • 0x1167c:$s1: LCOGQGPTGP
arm5	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x11fb0:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2 F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2 D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
arm5	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
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
5223.1.00000000bdb73fa0.0000000011aa4bfb.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x11fb0:$x1: POST /cdn-cgi/ • 0x11530:$x3: /dev/watchdog • 0x1167c:$s1: LCOGQGPTGP
5223.1.00000000bdb73fa0.0000000011aa4bfb.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x11fb0:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2 F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2 D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
5223.1.00000000bdb73fa0.0000000011aa4bfb.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
5223.1.00000000bdb73fa0.0000000011aa4bfb.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5223.1.00000000bdb73fa0.0000000011aa4bfb.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	

Click to see the 1 entries

Jbx Signature Overview

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)

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

Sets full permissions to files and/or directories

Stealing of Sensitive Information

Yara detected Mirai

Yara detected Moobot

Remote Access Functionality

Yara detected Mirai

Yara detected Moobot

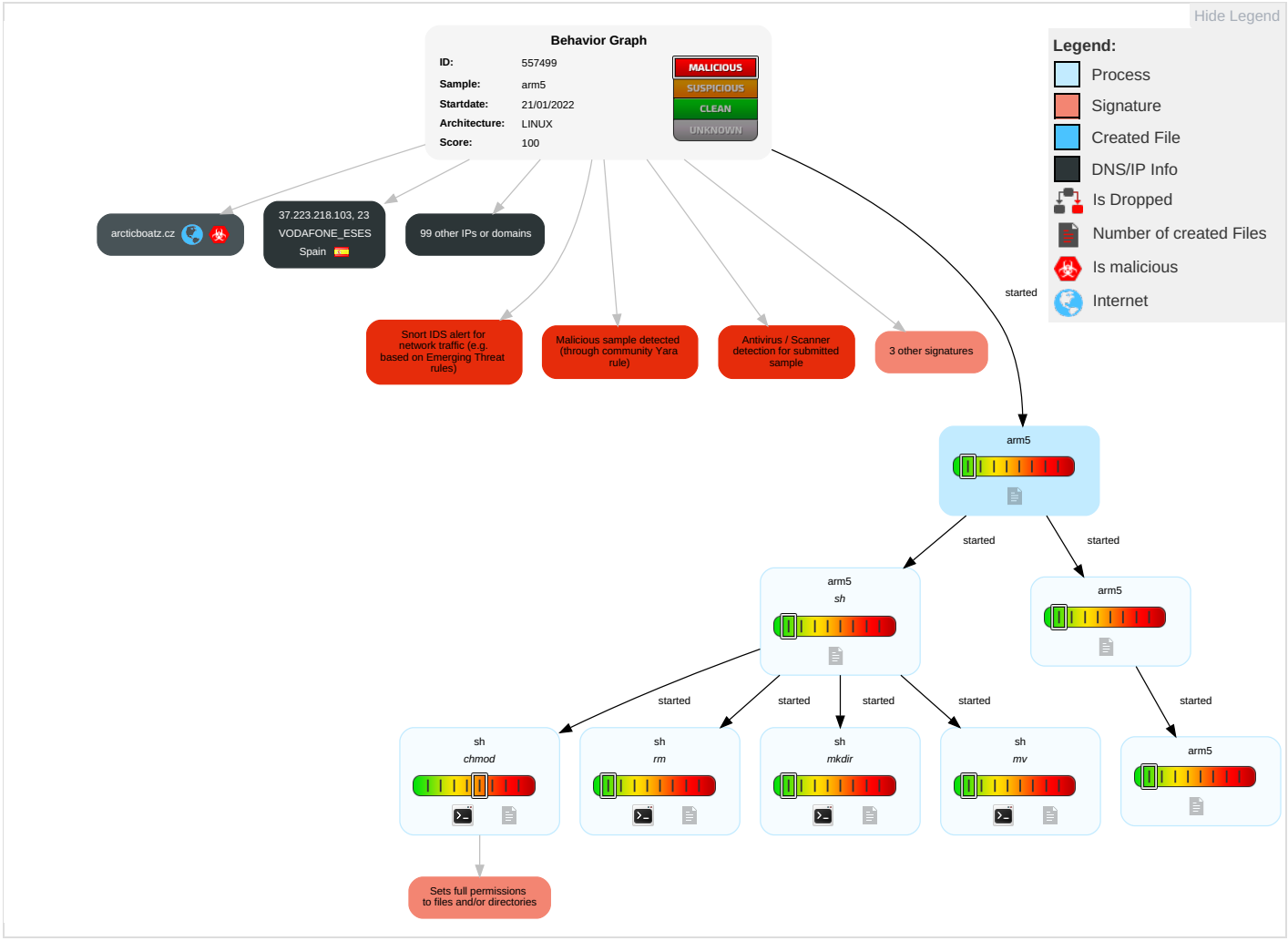
Mitre Att&ck Matrix

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	1 Scripting	Path Interception	Path Interception	2 File and Directory Permissions Modification	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	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Scripting	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)	1 File Deletion	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	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	2 Application Layer Protocol	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	38%	Virustotal		Browse
arm5	51%	ReversingLabs	Linux.Trojan.Mirai	
arm5	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
arcticboatz.cz	4%	Virustotal		Browse

URLs

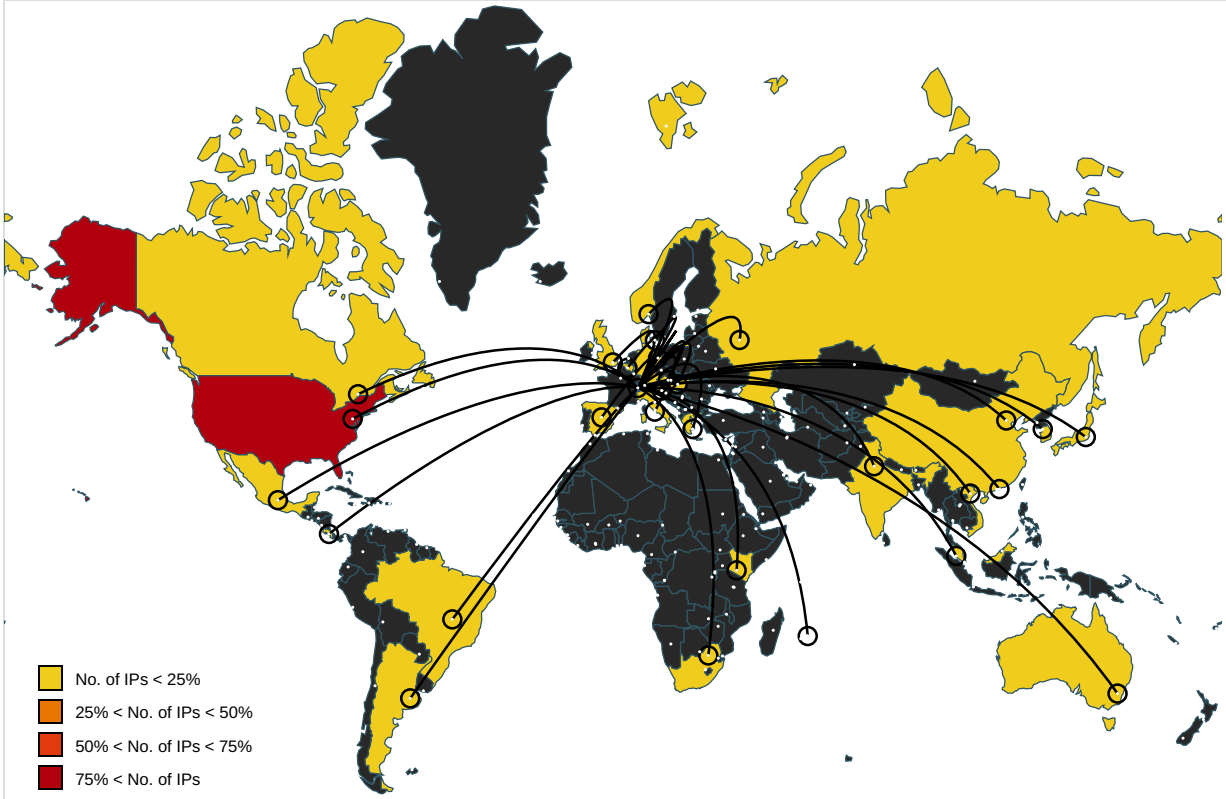
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
arcticboatz.cz	95.181.161.40	true	true	• 4%, Virustotal, Browse	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.101.243.135	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
200.101.154.113	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
159.177.201.81	unknown	Canada		34058	LIFECELL-ASUA	false
197.104.90.78	unknown	South Africa		37168	CELL-CZA	false
210.134.201.242	unknown	Japan		9354	TDNCCommunityNetworkCenterIncJP	false
66.9.20.36	unknown	United States		18885	M2NGAGE2US	false
104.59.161.94	unknown	United States		7018	ATT-INTERNET4US	false
67.59.196.74	unknown	United States		22667	VISTAUS	false
168.55.13.206	unknown	United States		1761	TDIR-CAPNETUS	false
159.73.193.217	unknown	Australia		1257	TELE2EU	false
139.61.36.211	unknown	United States		14618	AMAZON-AESUS	false
115.114.255.34	unknown	India		4755	TATACOMM-ASTATACommunicationsformerlyVSNLisLeadingISP	false
24.104.235.255	unknown	United States		12271	TWC-12271-NYCUS	false
72.200.216.59	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
140.89.4.184	unknown	United States		33651	CMCSUS	false
5.38.244.52	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	false
57.221.183.135	unknown	Belgium		2686	ATGS-MMD-ASUS	false
212.251.163.97	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
213.16.169.31	unknown	Greece		1241	FORTHNET-GRForthnetEU	false
97.14.248.254	unknown	United States		22394	CELLCOUS	false
14.180.194.14	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
189.55.193.122	unknown	Brazil		28573	CLAROSABR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.238.37.165	unknown	United States		14977	STATE-OF-WYOMING-ASNUS	false
12.139.76.104	unknown	United States		7018	ATT-INTERNET4US	false
221.17.67.232	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
137.169.117.219	unknown	United States		14981	KIRKLAND-ELLISUS	false
205.155.0.199	unknown	United States		14212	SANTA-CRUZ-EDNETUS	false
86.145.148.173	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
89.212.1.130	unknown	Slovenia		34779	T-2-ASASsetpropagatedbyT-2dooSI	false
177.239.180.14	unknown	Mexico		28554	CablemasTelecomunicacionesSAdeCVMX	false
73.34.174.52	unknown	United States		7922	COMCAST-7922US	false
98.232.158.193	unknown	United States		7922	COMCAST-7922US	false
111.146.246.17	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
143.26.165.222	unknown	United States		264008	LANCAMANTOANISERVICOSDEINFORMATICALTDA-MEBR	false
201.193.22.123	unknown	Costa Rica		11830	InstitutoCostarricensedeElectricidadyTelecomCR	false
67.156.64.89	unknown	United States		1226	CTA-42-AS1226US	false
65.198.123.22	unknown	United States		701	UUNETUS	false
105.31.246.182	unknown	Mauritius		37100	SEACOM-ASMU	false
32.87.115.107	unknown	United States		2686	ATGS-MMD-ASUS	false
4.115.139.55	unknown	United States		3356	LEVEL3US	false
219.20.46.100	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
73.3.202.148	unknown	United States		7922	COMCAST-7922US	false
137.244.51.233	unknown	United States		385	AFCONC-BLOCK1-ASUS	false
148.184.150.68	unknown	United States		3423	ATTIS-ASN3423US	false
164.55.31.11	unknown	United States		683	ARGONNE-ASUS	false
1.28.186.128	unknown	China		139007	UNICOM-NM-WULANCHABU-IDCUNICOMInnerMongoliaprovincenetwo	false
223.57.9.44	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
137.32.136.109	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
185.11.56.21	unknown	Switzerland		12329	TMRDE	false
43.106.87.16	unknown	Japan		4249	LILLY-ASUS	false
208.8.135.179	unknown	United States		1239	SPRINTLINKUS	false
184.185.219.179	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
2.226.207.141	unknown	Italy		12874	FASTWEBIT	false
78.108.201.88	unknown	Russian Federation		31430	TEL-NET-ASRU	false
106.20.137.151	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
93.161.234.172	unknown	Denmark		3292	TDCTDCASDK	false
70.150.78.4	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
190.188.24.106	unknown	Argentina		10481	TelecomArgentinaSAAR	false
40.107.129.67	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
34.249.149.34	unknown	United States		16509	AMAZON-02US	false
167.44.101.157	unknown	Canada		2665	CDAGOVNCA	false
169.22.99.146	unknown	United States		37611	AfrihostZA	false
177.58.101.176	unknown	Brazil		22085	ClaroSABR	false
170.76.213.125	unknown	United States		23478	CHAS-HEALTHUS	false
104.79.226.223	unknown	United States		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.32.32.175	unknown	Denmark		39642	DK-ESS-ASDK	false
130.178.130.128	unknown	United States		16509	AMAZON-02US	false
155.83.115.83	unknown	United States		4010	DNIC-AS-04010US	false
212.40.173.169	unknown	Germany		61157	PLUSSERVER-ASN1DE	false
180.29.63.127	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
187.245.214.253	unknown	Mexico		13999	MegaCableSAdeCVMX	false
72.249.104.46	unknown	United States		55045	TEKTONICUS	false
157.234.53.177	unknown	United States		7018	ATT-INTERNET4US	false
121.139.48.109	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
100.5.190.229	unknown	United States		701	UUNETUS	false
154.122.4.94	unknown	Kenya		12455	JAMBONETKE	false
78.107.25.80	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
165.83.226.16	unknown	United States		22284	AS22284-DOI-OPSUS	false
37.223.218.103	unknown	Spain		12430	VODAFONE_ESES	false
125.218.31.185	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
217.110.140.204	unknown	Germany		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
218.191.83.197	unknown	Hong Kong		9304	HUTCHISON-AS-APHGCGlobalCommunicationsLimitedHK	false
91.115.41.40	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
136.84.160.156	unknown	United States		60311	ONEFMCH	false
44.246.216.249	unknown	United States		16509	AMAZON-02US	false
171.184.20.206	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
146.35.15.155	unknown	United States		197938	TRAVIANGAMESDE	false
210.154.127.1	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
210.184.41.88	unknown	Hong Kong		4058	CITICTEL-CPC-AS4058CITICTelecomInternationalCPCLimited	false
93.166.171.73	unknown	Denmark		3292	TDCTDCASDK	false
103.56.222.51	unknown	India		36351	SOFTLAYERUS	false
181.92.48.204	unknown	Argentina		7303	TelecomArgentinaSAAR	false
170.38.152.104	unknown	Malaysia		139776	PETRONAS-BHD-AS-APPetroliamNasionalBerhadMY	false
134.116.162.78	unknown	United States		10455	LUCENT-CIOUS	false
57.250.134.147	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
76.40.116.134	unknown	United States		18494	CENTURYLINK-LEGACY-EMBARQ-WRBGUS	false
195.207.36.236	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
87.186.232.66	unknown	Germany		3320	DTAGInternetserviceproviderationsDE	false
101.76.125.54	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
192.111.221.75	unknown	United States		46562	TOTAL-SERVER-SOLUTIONSUS	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, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.130950571252559
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm5
File size:	79440
MD5:	b2499605d6cb98e1d428956ca720f9f3
SHA1:	25c3039bf8fdb8814b1f61fb25c3fe299556e0e1
SHA256:	7b876157fd5cc9e7ca92a6d9702911160a96b4fa400befd40bd1307bbb06e656
SHA512:	ffff2c1124118a8a0598fbbc0b2e052765ba217c3bfea47c3a4c006e42bf6ef5e131adcda2e076b6a123f3c5b652fa36278308ee52d1bb50a9be60a19b646c06
SSDEEP:	1536:EG5ixEJIFOnozX7mgbivK/fl2uHQTnsVqbVb3G33x8vqIT0YwbZnZ:DJgzLmDvbuwTfRb3GOvxwbZnZ
File Content Preview:	.ELF...a.....(.....4....4.....4. ...(.....1...1.....1...1...1..p....&.....Q.td.....-...L."....D.....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:	79040
Section Header Size:	40

ELF header

Number of Section Headers:	10
Header String Table Index:	9

Sections

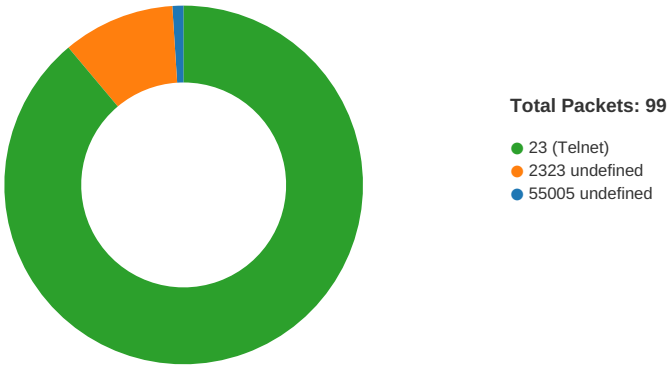
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x11304	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x193b4	0x113b4	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x193c8	0x113c8	0x1d44	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x23110	0x13110	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x23118	0x13118	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x23124	0x13124	0x35c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x23480	0x13480	0x237c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x13480	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	0x1310c	0x1310c	3.4509	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x13110	0x23110	0x23110	0x370	0x26ec	1.6671	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
Jan 21, 2022 08:30:49.197036982 CET	192.168.2.23	8.8.8.8	0xc1d5	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
Jan 21, 2022 08:30:49.215936899 CET	8.8.8.8	192.168.2.23	0xc1d5	No error (0)	arcticboatz.cz		95.181.161.40	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: arm5 PID: **5223**, Parent PID: **5117**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/tmp/arm5
Arguments:	/tmp/arm5
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: arm5 PID: **5225**, Parent PID: **5223**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/tmp/arm5
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5225**, Parent PID: **5223**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/arm5 bin/systemd; chmod 777 bin/systemd"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5227**, Parent PID: **5225**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5227**, Parent PID: **5225**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -rf bin/systemd
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: sh PID: **5228**, Parent PID: **5225**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: **5228**, Parent PID: **5225**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/usr/bin/mkdir
Arguments:	mkdir bin
File size:	88408 bytes
MD5 hash:	088c9d1df5a28ed16c726eca15964cb7

File Activities

File Read

Directory Created

Analysis Process: sh PID: **5229**, Parent PID: **5225**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mv PID: **5229**, Parent PID: **5225**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/usr/bin/mv
Arguments:	mv /tmp/arm5 bin/systemd
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: **5230**, Parent PID: **5225**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a

File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: **5230**, Parent PID: **5225**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/usr/bin/chmod
Arguments:	chmod 777 bin/systemd
File size:	63864 bytes
MD5 hash:	739483b900c045ae1374d6f53a86a279

File Activities

File Read

Permission Modified

Analysis Process: arm5 PID: **5231**, Parent PID: **5223**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/tmp/arm5
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm5 PID: **5233**, Parent PID: **5231**

General

Start time:	08:30:48
Start date:	21/01/2022
Path:	/tmp/arm5
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1