ID: 557445
Sample Name: arm7
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 06:04:21
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

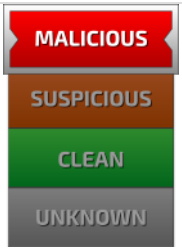
arm7

Overview

General Information

Sample Name:	arm7
Analysis ID:	557445
MD5:	a76e2e6437b384.
SHA1:	0640e30d9ad0a9.
SHA256:	2bd730dc891f39..
Tags:	Mirai
Infos:	

Detection



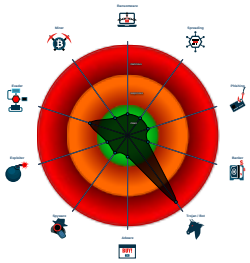
Mirai Moobot

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
- Uses known network protocols on n…
- Sets full permissions to files and/or …
- Yara signature match
- Executes the "mkdir" command use…
- Uses the "uname" system call to qu…

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:	557445
Start date:	21.01.2022
Start time:	06:04:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	arm7
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/arm7
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	qazwsxedc

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- arm7 (PID: 5243, Parent: 5130, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/arm7
  - arm7 New Fork (PID: 5245, Parent: 5243)
  - sh (PID: 5245, Parent: 5243, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv /tmp/arm7 bin/watchdog; chmod 777 bin/watchdog"
    - sh New Fork (PID: 5247, Parent: 5245)
    - rm (PID: 5247, Parent: 5245, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/watchdog
    - sh New Fork (PID: 5248, Parent: 5245)
    - mkdir (PID: 5248, Parent: 5245, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 5249, Parent: 5245)
    - mv (PID: 5249, Parent: 5245, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/arm7 bin/watchdog
    - sh New Fork (PID: 5250, Parent: 5245)
    - chmod (PID: 5250, Parent: 5245, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/watchdog
  - arm7 New Fork (PID: 5252, Parent: 5243)
    - arm7 New Fork (PID: 5254, Parent: 5252)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
arm7	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x18b58:$x1: POST /cdn-cgi/ • 0x180d8:$x3: /dev/watchdog • 0x18224:$s1: LCOGQGPTGP
arm7	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x18b58:$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
arm7	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
arm7	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
arm7	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5243.1.00000000eb7d369e.000000003b9895dc.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x18b58:$x1: POST /cdn-cgi/ • 0x180d8:$x3: /dev/watchdog • 0x18224:$s1: LCOGQGPTGP
5243.1.00000000eb7d369e.000000003b9895dc.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x18b58:$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
5243.1.00000000eb7d369e.000000003b9895dc.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
5243.1.00000000eb7d369e.000000003b9895dc.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5243.1.00000000eb7d369e.000000003b9895dc.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)
- Uses known network protocols on non-standard ports

System Summary

- Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

- Sets full permissions to files and/or directories

Hooking and other Techniques for Hiding and Protection

- Uses known network protocols on non-standard ports

Stealing of Sensitive Information

- Yara detected Mirai
- Yara detected Moobot

Remote Access Functionality

- Yara detected Mirai
- Yara detected Moobot

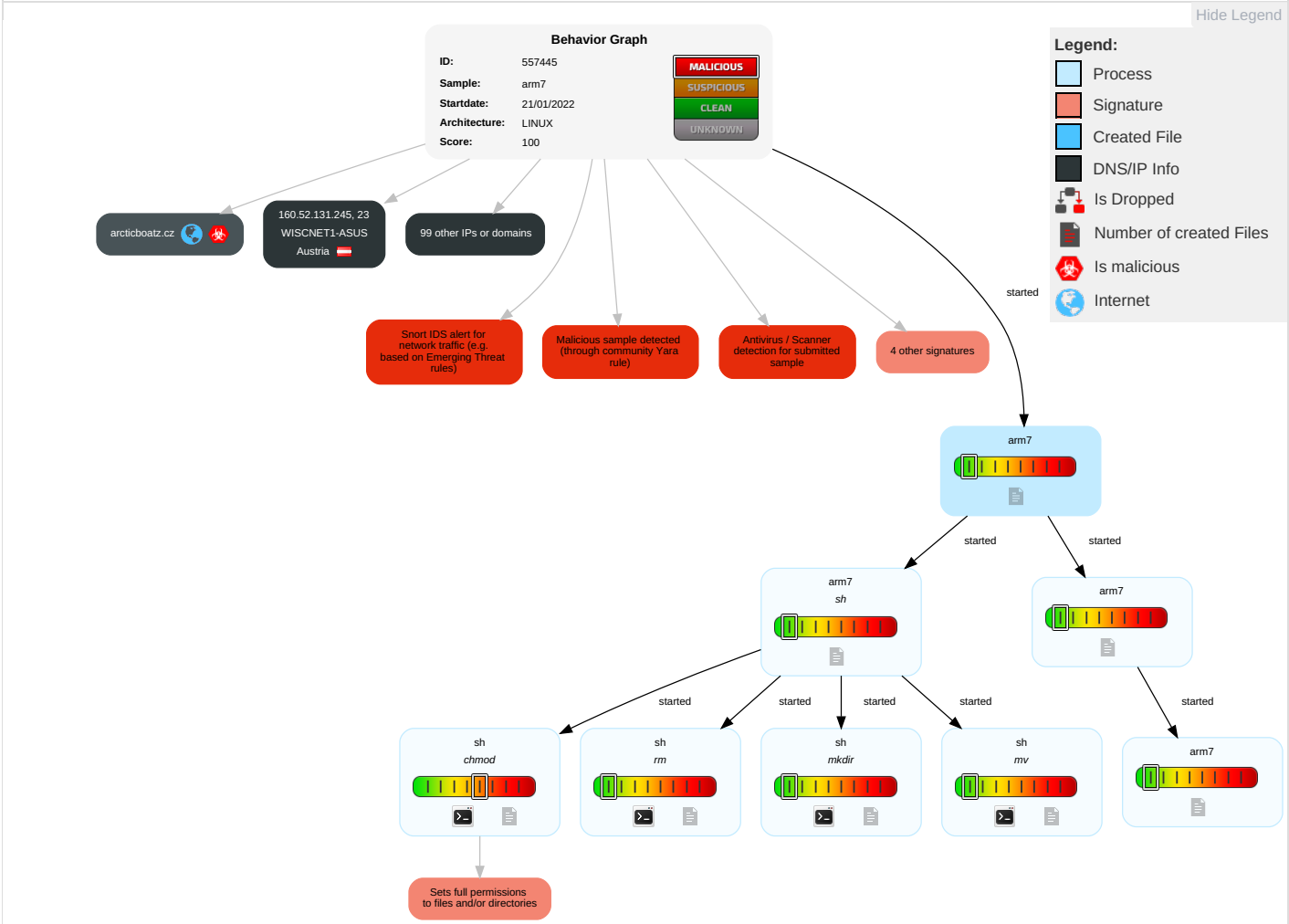
Mitre Att&ck Matrix

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 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
arm7	48%	Virustotal		Browse
arm7	56%	ReversingLabs	Linux.Trojan.Mirai	
arm7	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

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

URLs

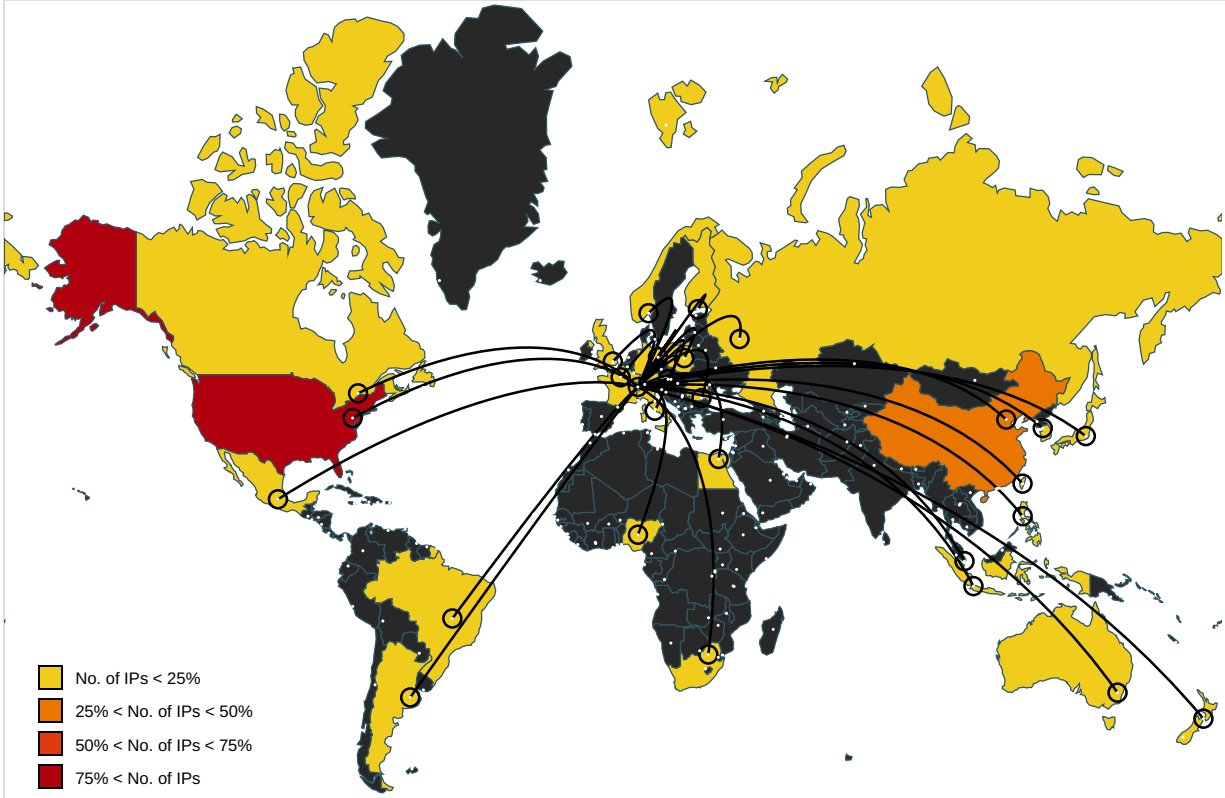
No Antivirus matches

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
89.244.88.20	unknown	Germany		8881	VERSATELDE	false
38.243.205.45	unknown	United States		36336	NATIXISUS	false
150.254.72.227	unknown	Poland		9112	POZMANPOZMAN-EDUPL	false
167.115.231.112	unknown	United States		17386	GRAINGERUS	false
88.213.227.97	unknown	France		8399	SEWAN-FR	false
128.122.29.231	unknown	United States		12	NYU-DOMAINUS	false
41.29.112.209	unknown	South Africa		29975	VODACOM-ZA	false
131.106.228.81	unknown	United States		6079	RCN-ASUS	false
54.176.161.42	unknown	United States		16509	AMAZON-02US	false
180.118.199.42	unknown	China		137702	CHINATELECOM-JIANGSU-NANJING-IDCNanjingJiangsuProvince	false
121.49.221.72	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
158.133.31.192	unknown	Switzerland		4616	HKPOLYU-HKInformationTechnologyServicesHK	false
69.245.183.227	unknown	United States		7922	COMCAST-7922US	false
136.116.11.165	unknown	United States		15169	GOOGLEUS	false
81.104.80.69	unknown	United Kingdom		5089	NTLGB	false
148.94.25.77	unknown	United States		786	JANETJiscServicesLimitedGB	false
98.51.41.129	unknown	United States		7922	COMCAST-7922US	false
189.220.156.46	unknown	Mexico		28509	CablemasTelecomunicacionesSAdeCVMX	false
218.98.10.57	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
20.156.174.178	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
121.64.81.231	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
80.116.244.216	unknown	Italy		3269	ASN-IBSNAZIT	false
46.36.5.67	unknown	Russian Federation		48642	KTEL-ASEkaterinburgRussiaRU	false
111.119.144.79	unknown	China		38342	CNNIC-SVCNET-APSHANGHAIVSATNETWORKSYSTEMSCOLTDCN	false
199.48.243.166	unknown	United States		22363	PHMGMT-AS1US	false
24.191.167.207	unknown	United States		6128	CABLE-NET-1US	false
191.175.211.88	unknown	Brazil		26615	TIMSABR	false
211.101.17.254	unknown	China		17964	DXTNETBeijingDian-Xin-TongNetworkTechnologiesCoLtd	false
203.44.155.66	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
134.241.171.162	unknown	United States		1256	MASSNET-ASUS	false
131.228.43.31	unknown	Finland		200656	NOKIA-EMEAFI	false
196.146.167.242	unknown	Egypt		36935	Vodafone-EG	false
137.234.55.185	unknown	United States		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
98.99.70.146	unknown	United States		62566	STARBUCKSUS	false
128.241.235.110	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
152.163.238.165	unknown	United States		12129	123NETUS	false
39.212.214.250	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
143.224.224.137	unknown	Austria		2036	JOANNEUMJOANNEUMRESEARCHAT	false
151.80.145.18	unknown	Italy		16276	OVHFR	false
105.181.50.118	unknown	Egypt		37069	MOBINILEG	false
173.190.153.159	unknown	United States		7029	WINDSTREAMUS	false
186.152.31.235	unknown	Argentina		7303	TelecomArgentinaSAAR	false
171.44.88.170	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
102.66.4.1	unknown	South Africa		328471	Hero-TelecomsZA	false
220.78.28.186	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
1.192.152.159	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
2.63.69.178	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
86.222.2.26	unknown	France		3215	FranceTelecom-OrangeFR	false
186.140.126.112	unknown	Argentina		11315	TelefonicaMovilesArgentinaSAMovistarArgentinaAR	false
192.169.38.188	unknown	Singapore		4628	PACIFICINTERNET-AS-APPacificInternetPteLtdSG	false
131.77.142.148	unknown	United States		5974	DNIC-ASBLK-05800-06055US	false
125.165.67.14	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
153.23.135.175	unknown	United States		6035	DNIC-ASBLK-05800-06055US	false
209.84.106.224	unknown	United States		3356	LEVEL3US	false
129.116.67.107	unknown	United States		18	UTEXASUS	false
90.223.27.70	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
218.236.189.226	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
188.195.163.241	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
24.197.106.250	unknown	United States		20115	CHARTER-20115US	false
133.229.179.199	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
150.34.171.252	unknown	Japan		9991	SHUDO-UHiroshimaShudoUniversityJP	false
216.221.87.6	unknown	Canada		7992	COGECOWAVECA	false
158.224.185.45	unknown	United States		9159	CreditAgricoleFR	false
105.121.229.83	unknown	Nigeria		36873	VNL1-ASNG	false
12.66.163.165	unknown	United States		7018	ATT-INTERNET4US	false
201.2.252.218	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
42.202.153.211	unknown	China		134762	CHINANET-LIAONING-DALIAN-MANCHINANETLiaoningprovinceDali	false
210.48.124.143	unknown	New Zealand		4770	ICONZ-ASICONZLtdNZ	false
76.212.146.151	unknown	United States		7018	ATT-INTERNET4US	false
193.122.104.171	unknown	United States		31898	ORACLE-BMC-31898US	false
144.112.151.160	unknown	United States		3634	SFASU-ASUS	false
194.202.200.68	unknown	United Kingdom		702	UUNETUS	false
212.93.155.41	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
142.75.189.154	unknown	Canada		3900	TEXASNET-ASNUS	false
160.52.131.245	unknown	Austria		2381	WISCNET1-ASUS	false
36.34.215.226	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
114.58.80.77	unknown	Indonesia		4795	INDOSATM2-IDINDOSATM2ASNID	false
119.45.82.84	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
125.223.24.12	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
157.245.211.172	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
40.78.216.75	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
123.194.54.251	unknown	Taiwan; Republic of China (ROC)		38841	KBRO-AS-TWkbroCOLtdTW	false
63.71.13.10	unknown	United States		13380	ASN-CUSTUS	false
165.164.162.250	unknown	United States		2381	WISCNET1-ASUS	false
75.152.207.199	unknown	Canada		852	ASN852CA	false
223.138.80.187	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false
86.79.155.52	unknown	France		15557	LDCOMNETFR	false
108.143.6.204	unknown	United States		16509	AMAZON-02US	false
32.146.125.147	unknown	United States		2686	ATGS-MMD-ASUS	false
48.63.246.40	unknown	United States		2686	ATGS-MMD-ASUS	false
206.27.103.109	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
36.192.214.241	unknown	China		24138	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
157.237.150.70	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
14.60.196.52	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
157.73.206.112	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
161.226.162.238	unknown	United States		3709	NET-CITY-SAUS	false
116.93.43.5	unknown	Philippines		23930	IPVG-AS-APIP-ConvergeDataCenterIncPH	false
9.79.229.204	unknown	United States		3356	LEVEL3US	false
110.129.128.165	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.34.33.137	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	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, EABI4 version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.120571086954281
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	arm7
File size:	107924
MD5:	a76e2e6437b384772b6ee03037a6d632
SHA1:	0640e30d9ad0a973536e9805b762748ddc267277
SHA256:	2bd730dc891f395d5bd663c9113ca86d23d046ecfb92f4b7ab28ad72cb40296a
SHA512:	6a2e153205f78ed6be5b989f23ca5c9cd44ed3c37281e99e59997d3b138924edc0b8dfde07ebb2217e06b67f3cbd63aeba2b25c3b0ca727762a47091e344ec8f
SSDEEP:	3072:JrIuUGKQm4F4VzfdKuaam+edAE5bft3KVFvwwbZnz:JrIuUGKV4iVLNaam+edAEJft8lwRz
File Content Preview:	.ELF.....(.....4...<.....4. ...(.....pp...p...p... ... .\4.....Q.td.....-...L.....@-.,@...0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM

ELF header	
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8194
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	5
Section Header Offset:	107324
Section Header Size:	40
Number of Section Headers:	15
Header String Table Index:	14

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80d4	0xd4	0x10	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80f0	0xf0	0x17e6c	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x1ff5c	0x17f5c	0x10	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1ff70	0x17f70	0x1de8	0x0	0x2	A	0	0	8
.ARM.extab	PROGBITS	0x21d58	0x19d58	0x18	0x0	0x2	A	0	0	4
.ARM.exidx	ARM_EXIDX	0x21d70	0x19d70	0x120	0x0	0x82	AL	2	0	4
.eh_frame	PROGBITS	0x2a000	0x1a000	0x4	0x0	0x3	WA	0	0	4
.tbss	NOBITS	0x2a004	0x1a004	0x8	0x0	0x403	WAT	0	0	4
.init_array	INIT_ARRAY	0x2a004	0x1a004	0x4	0x0	0x3	WA	0	0	4
.fini_array	FINI_ARRAY	0x2a008	0x1a008	0x4	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x2a010	0x1a010	0xa8	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x2a0b8	0x1a0b8	0x210	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x2a2c8	0x1a2c8	0x3194	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1a2c8	0x73	0x0	0x0		0	0	1

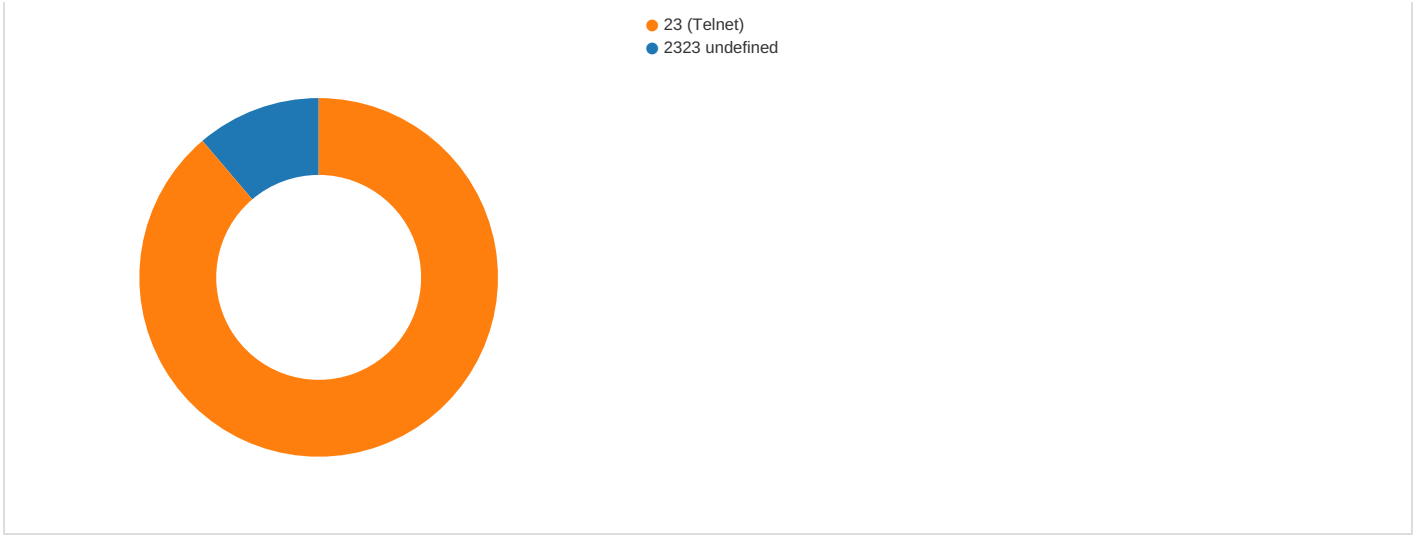
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
EXIDX	0x19d70	0x21d70	0x21d70	0x120	0x120	1.8471	0x4	R	0x4		.ARM.exidx
LOAD	0x0	0x8000	0x8000	0x19e90	0x19e90	3.4054	0x5	R E	0x8000		.init .text .fini .rodata .ARM.extab .ARM.exidx
LOAD	0x1a000	0x2a000	0x2a000	0x2c8	0x345c	2.1490	0x6	RW	0x8000		.eh_frame .init_array .fini_array .got .data .bss
TLS	0x1a004	0x2a004	0x2a004	0x0	0x8	0.0000	0x4	R	0x4		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution

Total Packets: 98



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2022 06:05:07.692047119 CET	192.168.2.23	8.8.8.8	0xb3da	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 06:05:07.710294008 CET	8.8.8.8	192.168.2.23	0xb3da	No error (0)	arcticboatz.cz		95.181.161.40	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: arm7 PID: **5243**, Parent PID: **5130**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/tmp/arm7
Arguments:	/tmp/arm7
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: arm7 PID: **5245**, Parent PID: **5243**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: **5245**, Parent PID: **5243**

General

Start time:	06:05:06

Start date:	21/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "rm -rf bin/watchdog && mkdir bin; >bin/watchdog && mv /tmp/arm7 bin/watchdog; chmod 777 bin/watchdog"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **5247**, Parent PID: **5245**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **5247**, Parent PID: **5245**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/usr/bin/rm
Arguments:	rm -rf bin/watchdog
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: sh PID: **5248**, Parent PID: **5245**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: **5248**, Parent PID: **5245**

General

Start time:	06:05:06
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: **5249**, Parent PID: **5245**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mv PID: **5249**, Parent PID: **5245**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/usr/bin/mv
Arguments:	mv /tmp/arm7 bin/watchdog
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: **5250**, Parent PID: **5245**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: **5250**, Parent PID: **5245**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/usr/bin/chmod
Arguments:	chmod 777 bin/watchdog
File size:	63864 bytes
MD5 hash:	739483b900c045ae1374d6f53a86a279

File Activities

File Read

Permission Modified

Analysis Process: arm7 PID: **5252**, Parent PID: **5243**

General

Start time:	06:05:06
Start date:	21/01/2022
Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: arm7 PID: **5254**, Parent PID: **5252**

General

Start time:	06:05:06
Start date:	21/01/2022

Path:	/tmp/arm7
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1