ID: 651255
Sample Name: loligang.arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 17:51:06
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

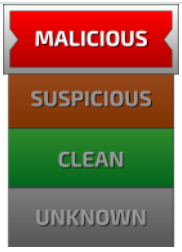
loligang.arm

Overview

General Information

Sample Name:	loligang.arm
Analysis ID:	651255
MD5:	400fb602a83456..
SHA1:	58ae954f8e0f72c..
SHA256:	e7ebfd53202270..
Infos:	

Detection



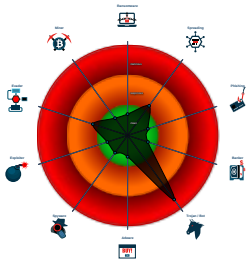
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- 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…
- 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.

All HTTP servers contacted by the sample do not answer. The sample is likely 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.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651255
Start date and time: 23/06/202217:51:06	2022-06-23 17:51:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	loligang.arm
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:	mal80.troj.linARM@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/loligang.arm
PID:	6233
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	lzrd cock fest"/proc/"/exe

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- loligang.arm (PID: 6233, Parent: 6123, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/loligang.arm
  - loligang.arm New Fork (PID: 6235, Parent: 6233)
  - loligang.arm New Fork (PID: 6236, Parent: 6233)
  - loligang.arm New Fork (PID: 6237, Parent: 6233)
    - loligang.arm New Fork (PID: 6241, Parent: 6237)
    - loligang.arm New Fork (PID: 6242, Parent: 6237)
    - loligang.arm New Fork (PID: 6245, Parent: 6237)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
loligang.arm	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x10c48:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x10cb8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x10d28:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x10d98:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x10e08:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x11078:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x110cc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x11120:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x11174:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x111c8:$xo1: oMXKNNC\x0D\x17\x0C\x12
loligang.arm	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	0x10624:$x1: POST /cdn-cgi/ 0x10ac8:$s1: LCOGQGPTGP
loligang.arm	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	0x10624:$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
loligang.arm	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
loligang.arm	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
6233.1.00000000cc577198.00000000dadd8b75.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x78:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xcc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x120:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x174:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c8:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
6236.1.00000000dadd8b75.0000000004e52adb.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x414:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x488:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x4fc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x570:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5e4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x864:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x8bc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x914:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x96c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9c4:$xo1: oMXKNNC\x0D\x17\x0C\x12
6242.1.00000000cc577198.00000000dadd8b75.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x78:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xcc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x120:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x174:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c8:$xo1: oMXKNNC\x0D\x17\x0C\x12
6236.1.000000008e4bd100.000000001113544c.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x10c48:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x10cb8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x10d28:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x10d98:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x10e08:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11078:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x110cc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11120:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11174:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x111c8:$xo1: oMXKNNC\x0D\x17\x0C\x12
6236.1.000000008e4bd100.000000001113544c.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x10624:$x1: POST /cdn-cgi/ • 0x10ac8:$s1: LCOGQGPTGP
Click to see the 23 entries				

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

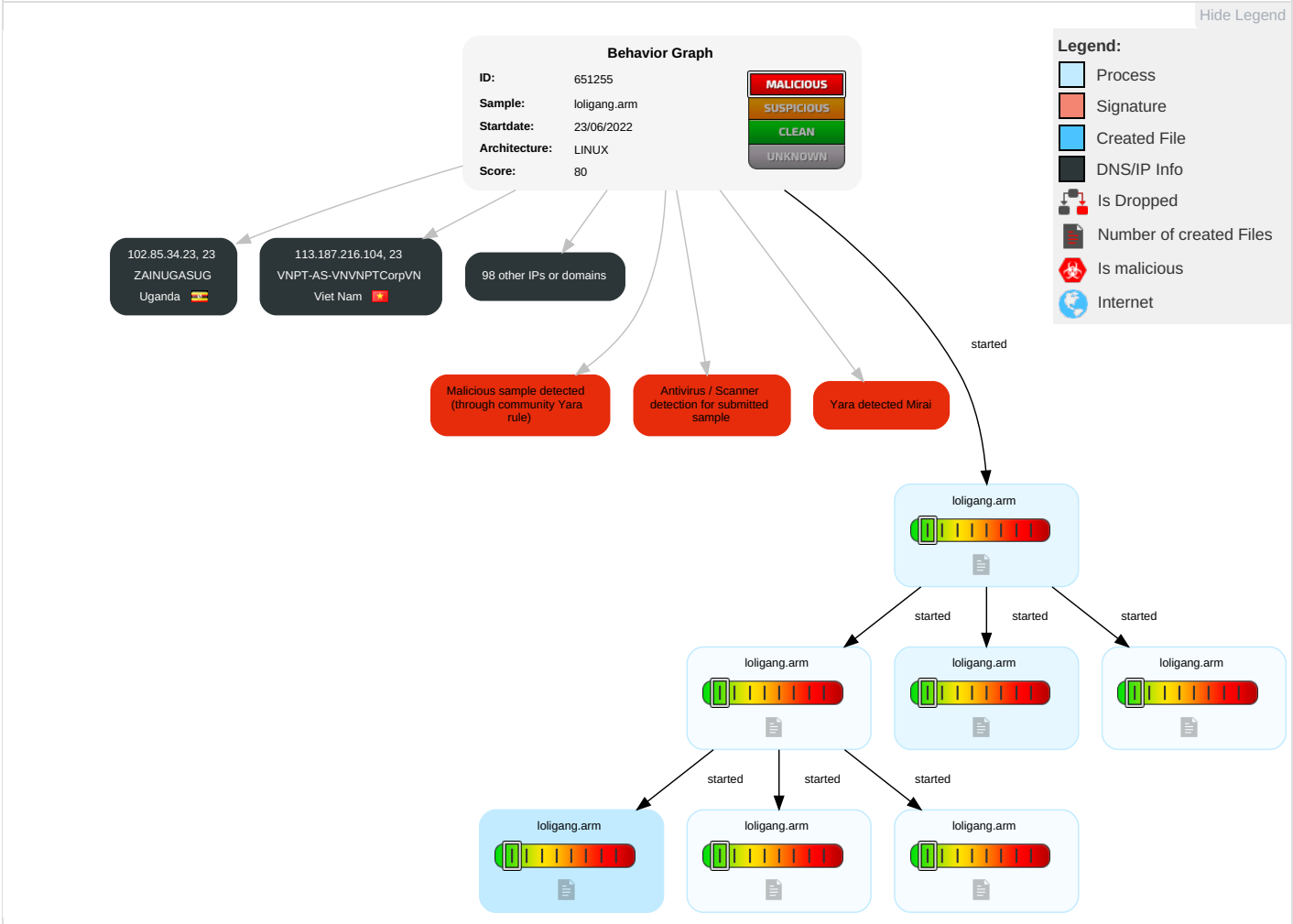
Mitre Att&ck Matrix

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 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	Rootkit	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)	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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
loligang.arm	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

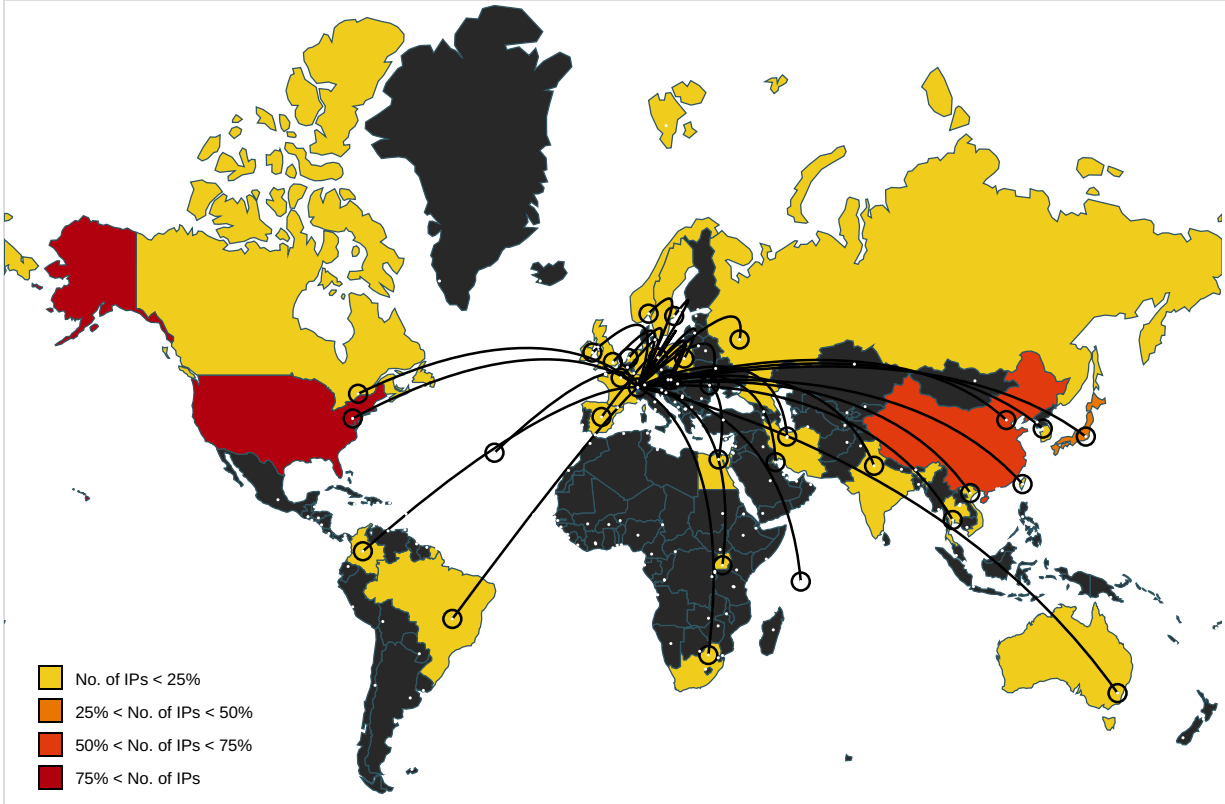
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.237.38.231	unknown	Moldova Republic of		8926	MOLDTELECOM-ASMoldtelecomAutonomousSystemMD	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
98.158.42.126	unknown	United States		17306	RISE-BROADBANDUS	false
81.166.61.176	unknown	Norway		29695	ALTIBOX_ASNorwayNO	false
2.122.220.103	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
62.245.20.215	unknown	United Kingdom		203872	VEMGB	false
223.230.16.135	unknown	India		24560	AIRTELBROADBAND-AS-APBhartiAirtelLtdTelemediaServices	false
188.232.6.38	unknown	Russian Federation		50543	SARATOV-ASRU	false
145.219.184.241	unknown	Netherlands		49362	DSVDK	false
166.134.236.213	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
79.90.254.241	unknown	France		15557	LDCOMNETFR	false
146.34.23.98	unknown	United States		197938	TRAVIANGAMESDE	false
181.146.17.126	unknown	Colombia		26611	COMCELSACO	false
222.45.77.40	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
118.88.27.239	unknown	Australia		55359	FLUCCS-AS-APFluccsAustraliaAustralianCloudProviderAU	false
177.190.166.209	unknown	Brazil		263458	ITRIXINTELIGENCIAEINTERNETBR	false
42.249.183.52	unknown	China		17799	CHINATELECOM-LN-AS-APasnforLiaoningProvincialNetofCT	false
156.251.78.61	unknown	Seychelles		26484	IKGUL-26484US	false
159.77.128.229	unknown	United States		492	AFCONC-BLOCK1-ASUS	false
147.213.160.130	unknown	Slovakia (SLOVAK Republic)		2607	SANETSlovakAcademicNetworkSK	false
222.113.239.144	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
40.211.135.51	unknown	United States		4249	LILLY-ASUS	false
113.187.216.104	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
240.224.198.104	unknown	Reserved		unknown	unknown	false
163.20.187.74	unknown	Taiwan; Republic of China (ROC)		1659	ERX-TANET-ASN1TaiwanAcademicNetworkTANetInformationC	false
222.11.173.244	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
149.206.194.4	unknown	Germany		15854	HP_WEBSERVICESDE	false
105.44.92.64	unknown	Egypt		37069	MOBINILEG	false
20.227.23.243	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
42.248.127.60	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
101.252.178.244	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
47.99.164.40	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
36.58.35.247	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
18.16.46.59	unknown	United States		3	MIT-GATEWAYSUS	false
83.61.33.150	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
94.241.185.156	unknown	Iran (ISLAMIC Republic Of)		42337	RESPINA-ASIR	false
176.228.32.11	unknown	Israel		12400	PARTNER-ASIL	false
245.213.137.128	unknown	Reserved		unknown	unknown	false
141.201.43.120	unknown	Austria		1109	UNI-SALZBURGUniversityofSalzburgAT	false
101.205.147.135	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
192.169.159.31	unknown	United States		398101	GO-DADDY-COM-LLCUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
122.80.72.247	unknown	China		45069	CNNIC-CTTSDNET-APchinatietongShandongnetCN	false
149.73.188.25	unknown	United States		188	SAIC-ASUS	false
221.240.51.10	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
41.179.145.19	unknown	Egypt		24863	LINKdotNET-ASEG	false
93.117.249.225	unknown	Netherlands		33915	TNF-ASNL	false
141.127.33.139	unknown	United States		719	ELISA-ASHelsinkiFinlandEU	false
191.129.172.223	unknown	Brazil		26615	TIMSABR	false
58.16.167.185	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
244.64.108.209	unknown	Reserved		unknown	unknown	false
99.72.102.149	unknown	United States		7018	ATT-INTERNET4US	false
133.87.238.64	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
182.72.85.51	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	false
77.151.220.86	unknown	France		15557	LDCOMNETFR	false
209.0.150.141	unknown	United States		3356	LEVEL3US	false
113.222.162.8	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
183.208.234.96	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
36.196.163.206	unknown	China		24138	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
81.45.3.111	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
154.178.63.147	unknown	Egypt		8452	TE-ASTE-ASEG	false
219.108.67.191	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
31.14.77.32	unknown	Poland		21409	IKOULAFR	false
111.19.246.226	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
142.191.158.100	unknown	Canada		13760	UNITI-FIBERUS	false
107.4.196.123	unknown	United States		7922	COMCAST-7922US	false
172.123.53.186	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
27.87.97.161	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
82.118.104.161	unknown	United Kingdom		8607	TIMICOUnitedKingdomGB	false
80.233.61.189	unknown	Ireland		13280	H3GIE	false
53.40.175.68	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
108.254.96.55	unknown	United States		7018	ATT-INTERNET4US	false
107.106.2.142	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
66.84.101.21	unknown	United States		27216	AIR-ADVANTAGE-ASNUS	false
118.61.81.85	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
155.35.171.61	unknown	United States		24324	KORDIA-TRANSIT-AS-APKordiaLimitedNZ	false
158.108.104.176	unknown	Thailand		9411	NONTRINET-AS-APKasetsartUniversityThailandTH	false
34.164.102.196	unknown	United States		2686	ATGS-MMD-ASUS	false
85.143.199.212	unknown	Russian Federation		57010	CLODO-ASRU	false
38.163.207.143	unknown	United States		174	COGENT-174US	false
79.138.230.65	unknown	Sweden		44034	HI3GSE	false
208.192.136.191	unknown	United States		701	UUNETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
106.221.153.169	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
42.166.144.20	unknown	China		4249	LILLY-ASUS	false
102.85.34.23	unknown	Uganda		37075	ZAINUGASUG	false
102.196.103.173	unknown	unknown		36926	CKL1-ASNKE	false
124.154.228.165	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
217.150.110.26	unknown	United Kingdom		24867	ADAPT-ASGB	false
13.7.122.55	unknown	United States		33631	PARC-ASNUS	false
168.187.73.254	unknown	Kuwait		6412	KWKEMSBlock-AFloor7SouqAl-KabeerKuwaitCityState	false
174.186.214.205	unknown	United States		7922	COMCAST-7922US	false
63.95.201.190	unknown	United States		701	UUNETUS	false
184.173.179.2	unknown	United States		36351	SOFTLAYERUS	false
77.247.166.42	unknown	Russian Federation		20807	CREDOLINK-ASNSt-PetersburgRU	false
211.253.115.146	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
182.117.125.21	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
171.68.221.173	unknown	United States		109	CISCOSYSTEMSUS	false
40.39.30.111	unknown	United States		4249	LILLY-ASUS	false
2.252.62.57	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
196.248.26.17	unknown	South Africa		2018	TENET-1ZA	false
133.62.8.142	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
159.250.78.159	unknown	United States		11776	ATLANTICBB-JOHNSTOWNUS	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):	6.08524219348038
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	loligang.arm
File size:	71864
MD5:	400fb602a83456d046d02ca8a746bb27
SHA1:	58ae954f8e0f72c13920faf69379652e6e61519c
SHA256:	e7ebfd53202270d83db456a781899c4ac41b8a11333ccb7d6e3454f3d6409e08
SHA512:	d463e640f75c6dddb88370783e8537b56ca88df61802bc2f4b4b302074e3e73fe57b20ade115c3377d4780b88fec165843991635b20467dbac6013455db36e48
SSDEEP:	1536:GbtexU5L9XouIRhb96pUQzXtwavaJ3V8OHxouJeZWDFI8iM:GbtexU0r8QCKw2FbL
TLSH:	FB6319817C80AA26C7D0177BFA9F108E3314ABD8E1DB73478C141F95769A81F0D6BB5A
File Content Preview:	.ELF...a.....(.....4...(.....4. ...(.....p...p.....t...t...t...t...L.....Q.td.....-...L."...JA.....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:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	71464
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	0x10560	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x18610	0x10610	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x18624	0x10624	0xf4c	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x21574	0x11574	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x2157c	0x1157c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x21588	0x11588	0x160	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x216e8	0x116e8	0x4d8	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x116e8	0x3e	0x0	0x0		0	0	1

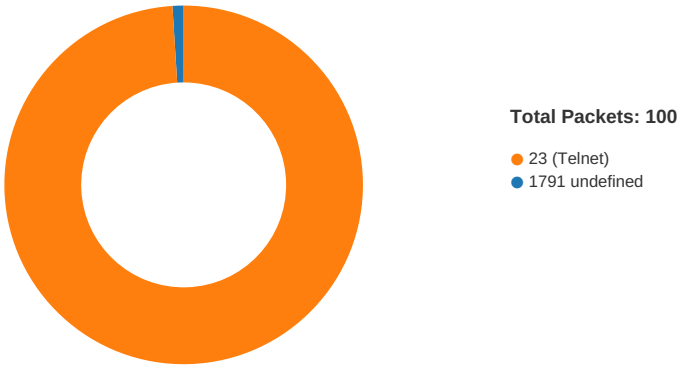
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x11570	0x11570	6.1108	0x5	R E	0x8000		.init .text .fini .rodata

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x11574	0x21574	0x21574	0x174	0x64c	0.8500	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

System Behavior

Analysis Process: loligang.arm PID: 6233, Parent PID: 6123

General

Start time:	17:51:57
Start date:	23/06/2022
Path:	/tmp/loligang.arm
Arguments:	/tmp/loligang.arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: loligang.arm PID: 6235, Parent PID: 6233

General

Start time:	17:51:57
Start date:	23/06/2022
Path:	/tmp/loligang.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: loligang.arm PID: **6236**, Parent PID: **6233**

General

Start time:	17:51:57
Start date:	23/06/2022
Path:	/tmp/loligang.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: loligang.arm PID: **6237**, Parent PID: **6233**

General

Start time:	17:51:57
Start date:	23/06/2022
Path:	/tmp/loligang.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: loligang.arm PID: **6241**, Parent PID: **6237**

General

Start time:	17:51:57
Start date:	23/06/2022
Path:	/tmp/loligang.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: loligang.arm PID: **6242**, Parent PID: **6237**

General

Start time:	17:51:57
Start date:	23/06/2022
Path:	/tmp/loligang.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: loligang.arm PID: **6245**, Parent PID: **6237**

General

Start time:	17:51:57
Start date:	23/06/2022
Path:	/tmp/loligang.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1