ID: 755689
Sample Name: f03XBkpBK6.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:11:38
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Linux Analysis Report

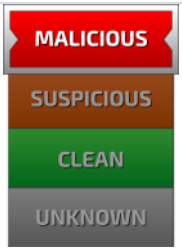
f03XBkpBK6.elf

Overview

General Information

Sample Name:	f03XBkpBK6.elf
Analysis ID:	755689
MD5:	55d542dcd32aee..
SHA1:	2d8927726e1c34..
SHA256:	815804338b816b.
Tags:	32 elf mips mirai
Infos:	

Detection



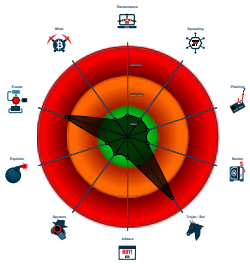
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample contains only a LOAD segm…
- Yara signature match
- 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…

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:	36.0.0 Rainbow Opal
Analysis ID:	755689
Start date and time:	2022-11-29 02:11:38 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	f03XBkpBK6.elf
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.evad.linELF@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/f03XBkpBK6.elf
PID:	6226
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- f03XBkpBK6.elf (PID: 6226, Parent: 6125, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/f03XBkpBK6.elf
  - f03XBkpBK6.elf New Fork (PID: 6228, Parent: 6226)
  - f03XBkpBK6.elf New Fork (PID: 6229, Parent: 6226)
  - f03XBkpBK6.elf New Fork (PID: 6231, Parent: 6226)
    - f03XBkpBK6.elf New Fork (PID: 6234, Parent: 6231)
    - f03XBkpBK6.elf New Fork (PID: 6235, Parent: 6231)
    - f03XBkpBK6.elf New Fork (PID: 6237, Parent: 6231)
- **cleanup**

Yara Signatures

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
6226.1.00007fc8b8455000.00007fc8b8457000.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	• 0x1584:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x15f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x166c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x16e0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1754:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x19d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a2c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a84:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1adc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1b34:$xo1: oMXKNNC\x0D\x17\x0C\x12
6229.1.00007fc8b8455000.00007fc8b8457000.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	• 0x1584:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x15f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x166c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x16e0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1754:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x19d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a2c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1a84:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1adc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1b34:$xo1: oMXKNNC\x0D\x17\x0C\x12
6226.1.00007fc8b8400000.00007fc8b8415000.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	• 0x145b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14628:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14698:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14708:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14778:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x149e8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14a3c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14a90:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14ae4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x14b38:$xo1: oMXKNNC\x0D\x17\x0C\x12
6226.1.00007fc8b8400000.00007fc8b8415000.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x13e50:$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
6226.1.00007fc8b8400000.00007fc8b8415000.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	

Click to see the 7 entries

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

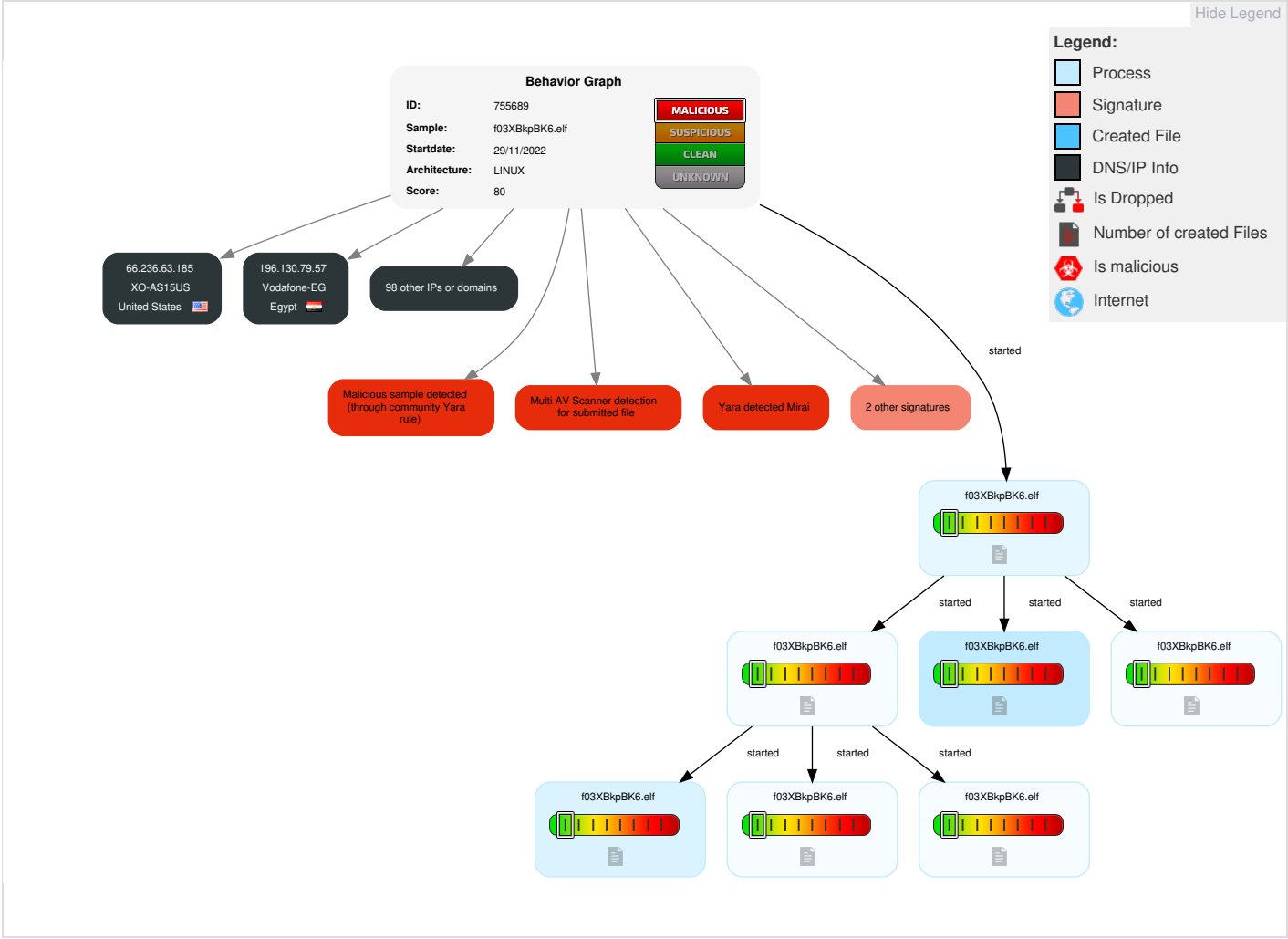
Mitre Att&ck Matrix

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	1 1 Obfuscated Files or Information	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 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
f03XBkpBK6.elf	52%	ReversingLabs	Linux.Trojan.Mirai	
f03XBkpBK6.elf	41%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

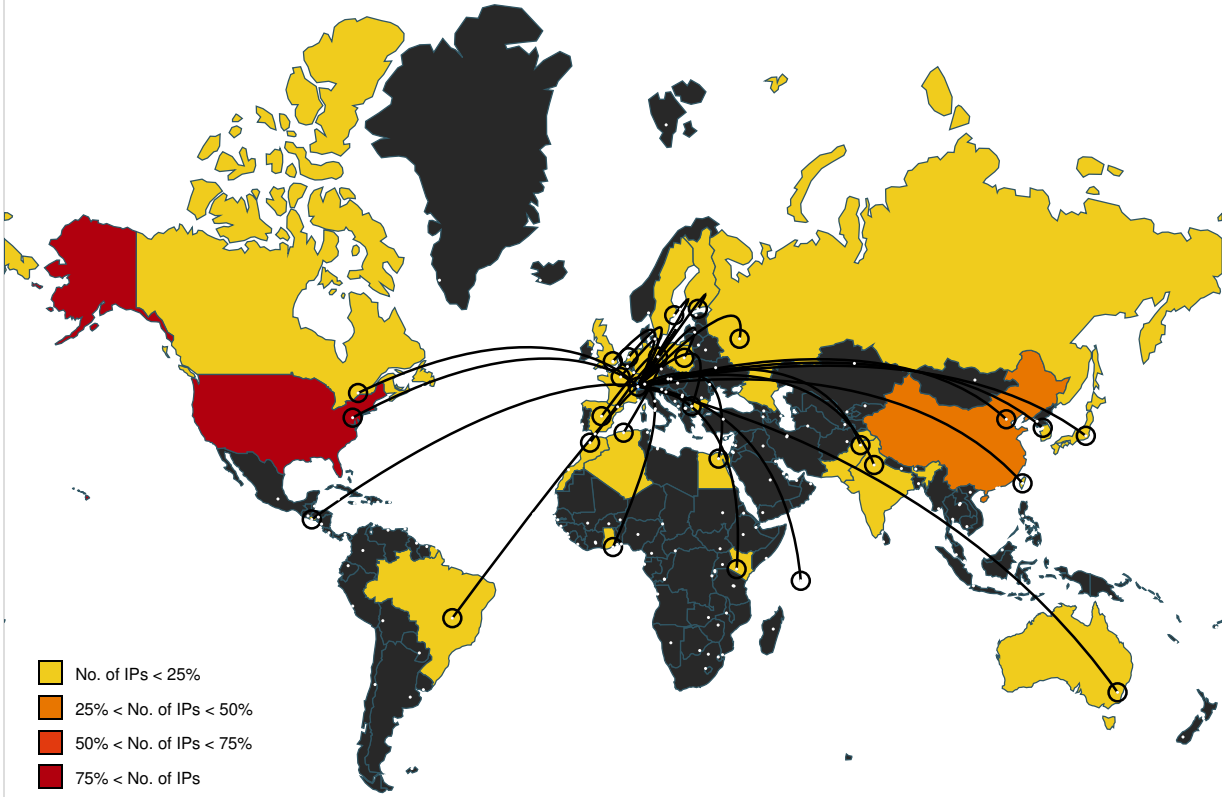
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
155.35.98.213	unknown	United States		24324	KORDIA-TRANSIT-AS-APKordiaLimitedNZ	false
101.228.227.91	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
204.30.147.16	unknown	United States		3356	LEVEL3US	false
40.83.2.247	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
35.231.235.136	unknown	United States		15169	GOOGLEUS	false
158.151.234.190	unknown	United States		26442	DNB-US	false
20.132.231.191	unknown	United States		206	CSC-IGN-AMERUS	false
32.250.225.133	unknown	United States		2686	ATGS-MMD-ASUS	false
212.246.61.101	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
197.204.101.52	unknown	Algeria		36947	ALGTEL-ASDZ	false
101.8.222.161	unknown	Taiwan; Republic of China (ROC)		701	UUNETUS	false
70.202.90.164	unknown	United States		22394	CELLCOUS	false
172.123.164.243	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
104.235.30.136	unknown	United States		22379	MANIFOLDUS	false
242.150.57.1	unknown	Reserved		unknown	unknown	false
144.80.148.191	unknown	United States		62989	IUPUS	false
97.45.39.141	unknown	United States		22394	CELLCOUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.36.110.218	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
31.48.217.190	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
90.217.222.125	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
187.121.39.106	unknown	Brazil		19182	TELEFONICABRASILSABR	false
66.236.63.185	unknown	United States		2828	XO-AS15US	false
145.116.23.144	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
122.117.147.238	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
248.77.126.194	unknown	Reserved		unknown	unknown	false
253.254.230.97	unknown	Reserved		unknown	unknown	false
218.193.82.71	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
142.31.170.14	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
107.127.53.141	unknown	United States		7018	ATT-INTERNET4US	false
223.245.245.95	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
123.63.98.82	unknown	India		55410	VIL-AS-APVodafoneIdeaLtdIN	false
80.50.183.227	unknown	Poland		5617	TPNETPL	false
65.248.145.171	unknown	United States		701	UUNETUS	false
133.195.181.231	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
73.83.162.186	unknown	United States		7922	COMCAST-7922US	false
76.41.20.91	unknown	United States		18494	CENTURYLINK-LEGACY-EMBARQ-WRBGUS	false
185.216.12.42	unknown	Russian Federation		41161	REALWEB-ASRU	false
59.180.5.108	unknown	India		17813	MTNL-APMahanagarTelephoneNigamLimitedIN	false
60.121.113.4	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
75.9.72.18	unknown	United States		7018	ATT-INTERNET4US	false
133.98.75.26	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
172.131.55.193	unknown	United States		7018	ATT-INTERNET4US	false
12.203.71.89	unknown	United States		22983	FISERV-INCUS	false
249.33.223.198	unknown	Reserved		unknown	unknown	false
85.77.171.140	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
156.63.125.11	unknown	United States		19902	NET-STATE-OHIOUS	false
153.119.253.101	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
154.95.51.164	unknown	Seychelles		54600	PEGTECHINCUS	false
253.238.149.215	unknown	Reserved		unknown	unknown	false
87.143.249.130	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
250.246.178.84	unknown	Reserved		unknown	unknown	false
82.204.20.201	unknown	Netherlands		15670	BBNED-AS1NL	false
200.175.108.106	unknown	Brazil		18881	TELEFONICABRASILSABR	false
105.88.235.219	unknown	Egypt		36992	ETISALAT-MISREG	false
190.87.62.2	unknown	El Salvador		14754	TelguaGT	false
240.156.18.94	unknown	Reserved		unknown	unknown	false
90.80.141.126	unknown	France		3215	FranceTelecom-OrangeFR	false
253.173.143.152	unknown	Reserved		unknown	unknown	false
246.33.49.77	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
102.63.100.89	unknown	Egypt		36992	ETISALAT-MISREG	false
241.141.146.48	unknown	Reserved		unknown	unknown	false
133.25.175.80	unknown	Japan		55379	HOSEI-NETHoseiUniversityJP	false
158.49.59.106	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
158.128.204.184	unknown	Canada		721	DNIC-ASBLK-00721-00726US	false
196.130.79.57	unknown	Egypt		36935	Vodafone-EG	false
171.60.231.176	unknown	India		24560	AIRTELBROADBAND-AS-APBhartiAirtelLtdTelemediaServices	false
100.149.110.121	unknown	United States		21928	T-MOBILE-AS21928US	false
23.196.34.233	unknown	United States		20940	AKAMAI-ASN1EU	false
125.120.126.142	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
58.65.191.26	unknown	Pakistan		23674	NAYATEL-PKNayatelPvtLtdPK	false
12.150.234.90	unknown	United States		2386	INS-ASUS	false
240.9.25.12	unknown	Reserved		unknown	unknown	false
88.211.88.51	unknown	United Kingdom		35575	VAIONIGB	false
140.230.5.22	unknown	Canada		8111	DALUNIVCA	false
160.18.19.56	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	false
126.1.101.35	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
160.168.12.233	unknown	Morocco		6713	IAM-ASMA	false
147.144.77.90	unknown	United States		2152	CSUNET-NWUS	false
85.231.153.146	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
87.120.3.93	unknown	Bulgaria		34577	SKATTV-ASBG	false
42.176.235.4	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
2.209.235.24	unknown	Germany		6805	TDDE-ASN1DE	false
156.134.58.77	unknown	United States		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
168.181.68.212	unknown	Brazil		265357	KDINTERNETBR	false
179.68.220.84	unknown	Brazil		7738	TelemarNorteLesteSABR	false
73.244.217.200	unknown	United States		7922	COMCAST-7922US	false
145.170.88.101	unknown	Netherlands		59524	KPN-IAASNL	false
114.140.203.30	unknown	Taiwan; Republic of China (ROC)		9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
45.222.232.161	unknown	Ghana		37282	MAINONENG	false
153.51.249.240	unknown	United States		14962	NCR-252US	false
206.70.233.170	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
217.230.103.141	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
120.13.218.124	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
192.110.155.171	unknown	United States		393835	CCS-COLOUS	false
169.255.104.242	unknown	Kenya		327906	EMBARQKE	false
124.5.1.168	unknown	Korea Republic of		10036	CNM-AS-KRDLIVEKR	false
117.180.195.198	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
147.177.133.237	unknown	United States		243	HARRIS-ATD-ASUS	false
161.50.51.158	unknown	Australia		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
58.192.78.190	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	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, MIPS, MIPS-I version 1 (SYSV), statically linked, no section header
Entropy (8bit):	7.900277247917175
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	f03XBkpBK6.elf
File size:	30316
MD5:	55d542dcd32aee3788c86ab2ae634ca6
SHA1:	2d8927726e1c34cd6355c8095aef1dd27c5e86ae
SHA256:	815804338b816bf198769f53a3962dd33a04b16dffef46a87ac89e9775adae6b
SHA512:	282401d5563bcf39a65962730dd347a41ae3ec75f95cbf13adaeece28608d31c27d024b01485c166222cb040935ff060475f95ee19c592e5e62392305097bdb4
SSDEEP:	768:C1uUtLrVDsAp6tLkF4FuetwEub4sU/M9g36KNSJb8WUP:CbDs06t4BEub4sU/MbUSAP
TLSH:	EED2E12CD94D7D05DAAD3EBE50CE9AF5298C74C0A35DEACE07168448B617ACBEC071E4
File Content Preview:	.ELF.....b..4.....4. ...(.....Eu..Eu.....[...[E.. [E.....u...UPX!`.....Z...Z.....S.....?.E.h;...#.....b.L#8....&C.....}+..ze.aw....2"ds...:.Z...;.g...l.D.....t6/..N...^.....+

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	

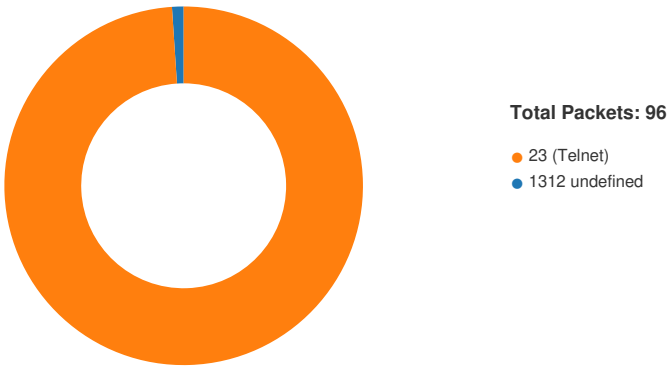
ELF header	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x7545	0x7545	7.9039	0x5	R E	0x10000		
LOAD	0x5b00	0x455b00	0x455b00	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: f03XBkpBK6.elf PID: 6226, Parent PID: 6125

General

Start time:	02:12:24
Start date:	29/11/2022
Path:	/tmp/f03XBkpBK6.elf
Arguments:	/tmp/f03XBkpBK6.elf
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: f03XBkpBK6.elf PID: **6228**, Parent PID: **6226**

General

Start time:	02:12:24
Start date:	29/11/2022
Path:	/tmp/f03XBkpBK6.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: f03XBkpBK6.elf PID: **6229**, Parent PID: **6226**

General

Start time:	02:12:24
Start date:	29/11/2022
Path:	/tmp/f03XBkpBK6.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: f03XBkpBK6.elf PID: **6231**, Parent PID: **6226**

General

Start time:	02:12:24
Start date:	29/11/2022
Path:	/tmp/f03XBkpBK6.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: f03XBkpBK6.elf PID: **6234**, Parent PID: **6231**

General

Start time:	02:12:24
Start date:	29/11/2022
Path:	/tmp/f03XBkpBK6.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: f03XBkpBK6.elf PID: **6235**, Parent PID: **6231**

General

Start time:	02:12:24
Start date:	29/11/2022
Path:	/tmp/f03XBkpBK6.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: f03XBkpBK6.elf PID: **6237**, Parent PID: **6231**

General

Start time:	02:12:24
Start date:	29/11/2022
Path:	/tmp/f03XBkpBK6.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9