ID: 635404
Sample Name: gmjJxVFJKQ
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:12:13
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

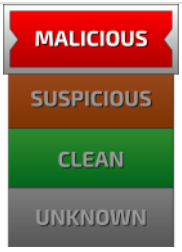
gmjJxVFJKQ

Overview

General Information

Sample Name:	gmjJxVFJKQ
Analysis ID:	635404
MD5:	a8fbc7563fe019c..
SHA1:	d9842c2d31a735..
SHA256:	e92cdc162e5091..
Tags:	32 elf mips mirai
Infos:	

Detection



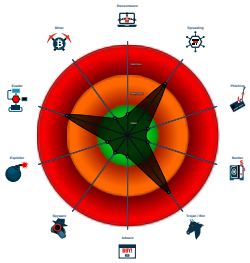
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- 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:	34.0.0 Boulder Opal
Analysis ID:	635404
Start date and time: 27/05/202221:12:13	2022-05-27 21:12:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gmjJxVFJKQ
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:	mal68.spre.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/gmjJxVFJKQ
PID:	6223
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- gmjJxVFJKQ (PID: 6223, Parent: 6125, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/gmjJxVFJKQ
  - gmjJxVFJKQ New Fork (PID: 6225, Parent: 6223)
  - gmjJxVFJKQ New Fork (PID: 6226, Parent: 6223)
    - gmjJxVFJKQ New Fork (PID: 6231, Parent: 6226)
    - gmjJxVFJKQ New Fork (PID: 6233, Parent: 6226)
      - gmjJxVFJKQ New Fork (PID: 6235, Parent: 6233)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
gmjJxVFJKQ	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x9ee0:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x9f4f:$s2: $Id: UPX • 0x9f00:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

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

Sample tries to kill multiple processes (SIGKILL)

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

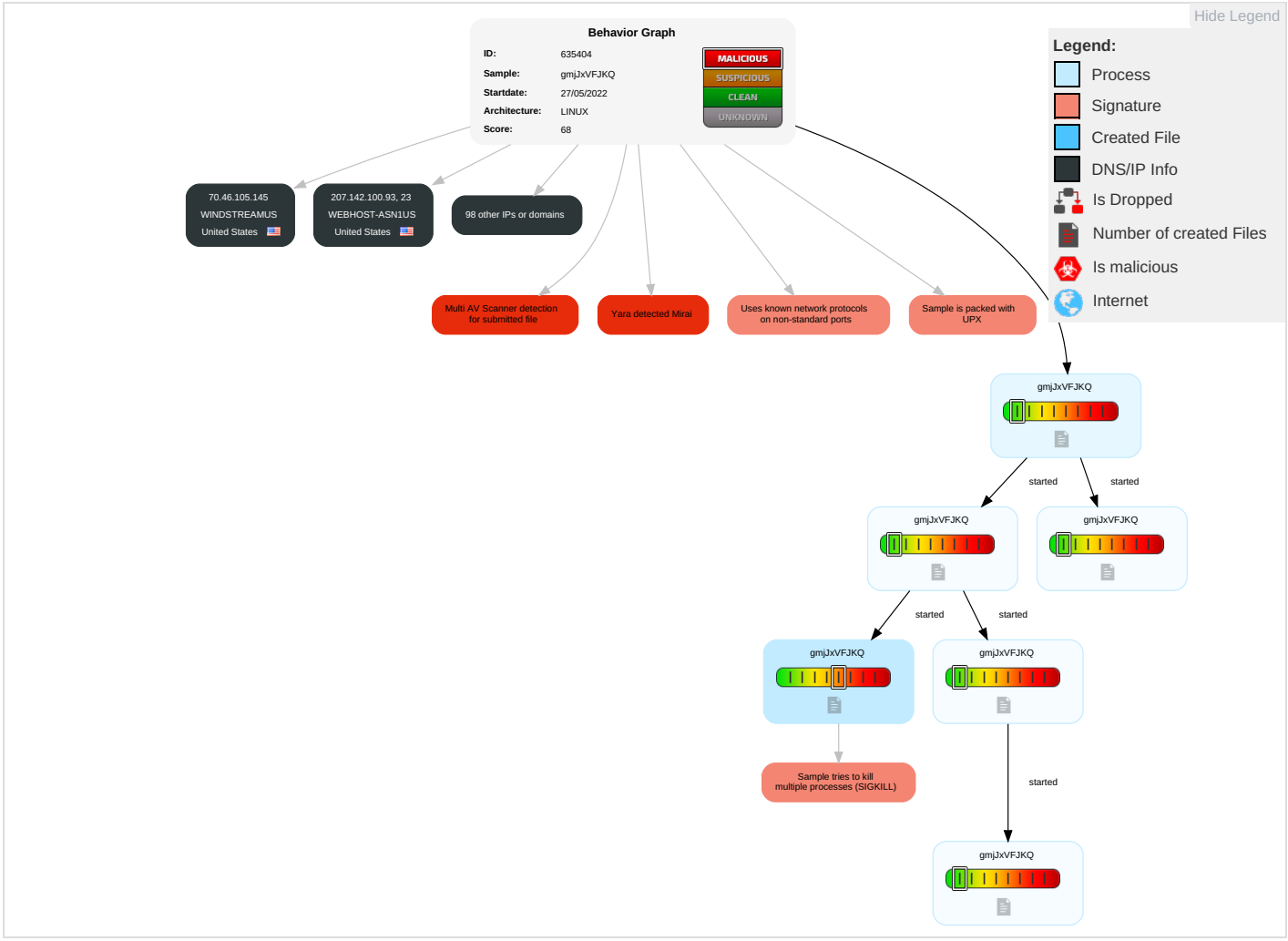
Mitre Att&ck Matrix

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 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	1 Service Stop
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
gmjJxVFJKQ	23%	Virustotal		Browse
gmjJxVFJKQ	25%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

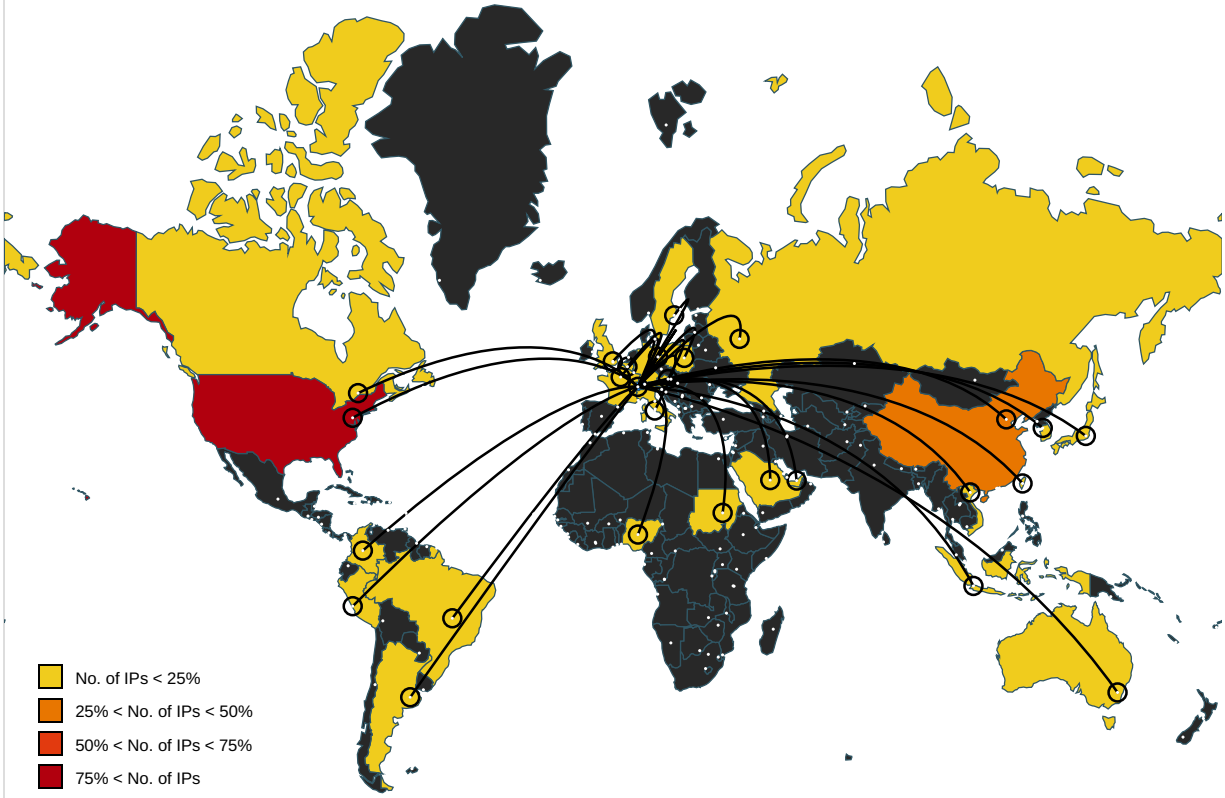
Domains and IPs

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
179.181.176.98	unknown	Brazil		10429	TELEFONICABRASILSAB R	false
83.6.123.68	unknown	Poland		5617	TPNETPL	false
212.117.245.240	unknown	European Union		3561	CENTURYLINK-LEGACY-SAVVISUS	false
39.208.21.158	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelular ID	false
129.152.120.162	unknown	United States		7160	NETDYNAMICSUS	false
78.134.1.110	unknown	Italy		35612	NGI-ASIT	false
200.11.55.186	unknown	Peru		6147	TelefonicadelPeruSAAPE	false
158.250.44.138	unknown	Russian Federation		2683	RADIO-MSURADIO-MSUEU	false
76.197.217.4	unknown	United States		7018	ATT-INTERNET4US	false
173.45.39.91	unknown	United States		33597	ATLANTIC-METRO-COMMUNICATIONS-II-INCUS	false
129.154.158.48	unknown	United States		7160	NETDYNAMICSUS	false
70.46.105.145	unknown	United States		7029	WINDSTREAMUS	false
156.43.93.37	unknown	United Kingdom		3549	LVLT-3549US	false
11.15.144.105	unknown	United States		3356	LEVEL3US	false
63.34.86.17	unknown	United States		16509	AMAZON-02US	false
52.118.189.55	unknown	United States		36351	SOFTLAYERUS	false
115.76.201.180	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
207.142.100.93	unknown	United States		27229	WEBHOST-ASN1US	false
152.133.192.199	unknown	United States		29992	VA-TMP-COREUS	false
204.176.239.90	unknown	United States		701	UUNETUS	false
114.8.69.141	unknown	Indonesia		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
181.13.216.197	unknown	Argentina		7303	TelecomArgentinaSAAR	false
30.36.127.176	unknown	United States		7922	COMCAST-7922US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
112.114.205.160	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
149.148.16.109	unknown	Austria		2494	MUWNETMUWNETAutonomousSystemAT	false
31.60.104.188	unknown	Poland		5617	TPNETPL	false
22.200.27.214	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
43.64.131.238	unknown	Japan		4249	LILLY-ASUS	false
96.209.51.126	unknown	United States		7922	COMCAST-7922US	false
125.144.13.186	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
3.143.238.175	unknown	United States		16509	AMAZON-02US	false
193.43.44.10	unknown	Italy		3269	ASN-IBSNAZIT	false
211.133.52.222	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
108.197.70.158	unknown	United States		7018	ATT-INTERNET4US	false
144.185.40.170	unknown	United States		19773	MOTOROLAUS	false
104.150.9.208	unknown	United States		1832	SMUUS	false
81.137.94.161	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
22.12.154.202	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
151.99.155.238	unknown	Italy		3269	ASN-IBSNAZIT	false
31.219.177.128	unknown	United Arab Emirates		8966	ETISALAT-ASPOBox1150DubaiUAE	false
137.145.59.136	unknown	United States		2152	CSUNET-NWUS	false
23.200.128.157	unknown	United States		14638	LCPRLUS	false
39.176.217.227	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
218.2.240.61	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
181.152.79.162	unknown	Colombia		26611	COMCELSACO	false
78.119.70.105	unknown	France		8228	CEGETEL-ASFR	false
130.125.217.205	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
18.230.73.245	unknown	United States		16509	AMAZON-02US	false
73.160.78.147	unknown	United States		7922	COMCAST-7922US	false
151.171.24.143	unknown	United States		3257	GTT-BACKBONEGTTDE	false
31.89.219.233	unknown	United Kingdom		12576	EELtdGB	false
128.30.226.157	unknown	United States		3	MIT-GATEWAYSUS	false
183.57.192.37	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
151.255.85.241	unknown	Saudi Arabia		39451	MELBOURNE-ASGB	false
39.163.166.11	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
197.252.128.197	unknown	Sudan		15706	SudatelSD	false
105.114.236.209	unknown	Nigeria		36873	VNL1-ASNG	false
29.146.52.83	unknown	United States		7922	COMCAST-7922US	false
252.118.26.52	unknown	Reserved		unknown	unknown	false
145.55.14.173	unknown	United Kingdom		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
29.52.115.242	unknown	United States		7922	COMCAST-7922US	false
210.85.166.50	unknown	Taiwan; Republic of China (ROC)		7482	APOL-ASAsiaPacificOnlineServiceIncTW	false
19.76.79.167	unknown	United States		3	MIT-GATEWAYSUS	false
184.95.51.79	unknown	United States		20454	SSASN2US	false
58.105.224.126	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
70.34.47.217	unknown	United States		15830	EQUINIX-CONNECT-EMEAGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
81.225.146.229	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
58.32.178.207	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
188.121.44.111	unknown	Germany		21501	GODADDY-AMSDE	false
106.96.40.205	unknown	Korea Republic of		17853	LGTELECOM-AS-KRLGTELECOMKR	false
242.161.53.186	unknown	Reserved		unknown	unknown	false
181.250.206.235	unknown	Colombia		26611	COMCELSACO	false
18.176.199.11	unknown	United States		16509	AMAZON-02US	false
142.5.110.66	unknown	Canada		46606	UNIFIEDLAYER-AS-1US	false
114.235.99.95	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
162.139.66.206	unknown	Canada		40341	Q9-AS-CAL2CA	false
48.16.103.185	unknown	United States		2686	ATGS-MMD-ASUS	false
205.6.160.185	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
63.153.51.35	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
90.29.33.106	unknown	France		3215	FranceTelecom-OrangeFR	false
212.58.250.50	unknown	United Kingdom		2818	BBCBBCInternetServicesUKGB	false
42.215.246.135	unknown	China		4249	LILLY-ASUS	false
161.253.110.135	unknown	United States		11039	GWUUS	false
171.204.130.148	unknown	United States		10794	BANKAMERICAUS	false
104.144.232.233	unknown	Canada		55286	SERVER-MANIACA	false
183.105.106.47	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
158.218.168.105	unknown	United Kingdom		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
36.119.225.165	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
220.165.128.130	unknown	China		134765	CHINANET-YUNNAN-IDC1CHINANETYunnanprovinceIDC1network	false
56.227.65.101	unknown	United States		2686	ATGS-MMD-ASUS	false
109.126.35.19	unknown	Russian Federation		42038	VLADLINK-ASRU	false
159.38.64.36	unknown	Sweden		19399	SLLNETEU	false
223.96.74.95	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	false
252.33.149.249	unknown	Reserved		unknown	unknown	false
57.217.232.34	unknown	Belgium		2686	ATGS-MMD-ASUS	false
31.226.76.24	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
139.35.103.114	unknown	United States		9905	LINKNET-ID-APLinknetASNID	false
83.76.95.50	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
110.113.89.16	unknown	China		24138	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
19.133.219.65	unknown	United States		3	MIT-GATEWAYSUS	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, stripped
Entropy (8bit):	7.940559496820084
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	gmjJxVFJKQ
File size:	42928
MD5:	a8fbc7563fe019ca689573d43d7797f3
SHA1:	d9842c2d31a7357d8c92414edbff9e60fce317b2
SHA256:	e92cdc162e5091c4916d12d2f4a5f7e7e9ffdb4dae8a18427d81f97ed08edcef
SHA512:	f0ebf55bd633efbaeba15d1c37cbb77f4c0be09c20f70638d05baa484c81204f90440a37f518c745d735d8fdeae8a5b67bd52cf44acf7d987fd2b5703501b9a4
SSDEEP:	768:vL2P9rDZe1V1zzXCgDugq7qovNFPmvKk4ywL7Eug+xwWD:vL2PdV6jzzXCgkPF9mSRywvzF
TLSH:	7F13F15640FDB4CFCCCEAD7A132819E5EE08588966EB135D6B04C589E8A8B5FF05E4B0
File Content Preview:	.ELF.....0...4.....4. ... (.....m...m.....\...\.F.\.F....._|UPX!d.....p...p.....U.....?.E.h;....#.....b.L#3..b.6RMN.....u..F..)..R.n.....bg.F.q+h...z..U%..\...C,...o.\.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x109330
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0

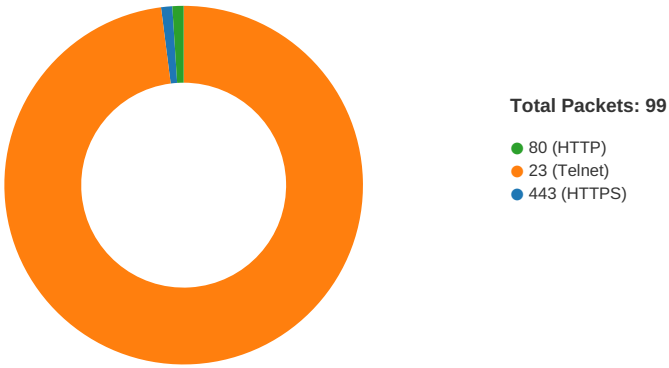
ELF header	
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

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	0xa66d	0xa66d	4.1473	0x5	R E	0x10000		
LOAD	0xd5c	0x460d5c	0x460d5c	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: gmjJxVFJKQ PID: 6223, Parent PID: 6125

General

Start time:	21:12:59
Start date:	27/05/2022
Path:	/tmp/gmjJxVFJKQ
Arguments:	/tmp/gmjJxVFJKQ
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: gmjJxVFJKQ PID: 6225, Parent PID: 6223

General

Start time:	21:13:00
Start date:	27/05/2022
Path:	/tmp/gmjJxVFJKQ

Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: gmjJxVFJKQ PID: **6226**, Parent PID: **6223**

General

Start time:	21:13:00
Start date:	27/05/2022
Path:	/tmp/gmjJxVFJKQ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: gmjJxVFJKQ PID: **6231**, Parent PID: **6226**

General

Start time:	21:13:00
Start date:	27/05/2022
Path:	/tmp/gmjJxVFJKQ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: gmjJxVFJKQ PID: **6233**, Parent PID: **6226**

General

Start time:	21:13:00
Start date:	27/05/2022
Path:	/tmp/gmjJxVFJKQ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: gmjJxVFJKQ PID: **6235**, Parent PID: **6233**

General

Start time:	21:13:00
Start date:	27/05/2022
Path:	/tmp/gmjJxVFJKQ
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9