ID: 510721
Sample Name: Mozi.a
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 06:46:30
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

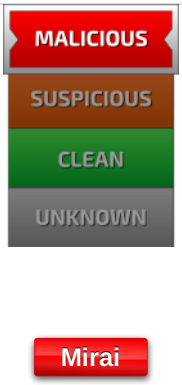
Linux Analysis Report Mozi.a

Overview

General Information

Sample Name:	Mozi.a
Analysis ID:	510721
MD5:	e30a81d66f18f07..
SHA1:	a7fd1a1d71f7f7b...
SHA256:	b7ba5aa2f8f7781..
Infos:	

Detection

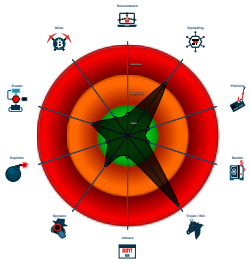


Score:	92
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Found strings indicative of a multi-pl…
- Sample contains only a LOAD segm…
- Yara signature match
- Sample contains strings that are pot…
- Sample contains strings indicative o…
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Sample contains strings indicative o…

Classification



Analysis Advice

- **Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures**
- **All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work**
- **Non-zero exit code suggests an error during the execution. Lookup the error code for hints.**
- **Static ELF header machine description suggests that the sample might not execute correctly on this machine**

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510721
Start date:	28.10.2021
Start time:	06:46:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Mozi.a
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:	mal92.spre.troj.linA@0/0@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
  - Mozi.a (PID: 5244, Parent: 5118, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/Mozi.a
- **cleanup**

Yara Overview

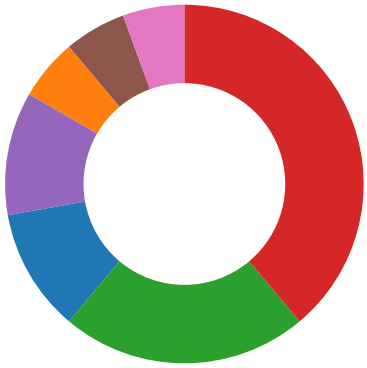
Initial Sample

Source	Rule	Description	Author	Strings
Mozi.a	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x1fce8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x1fd57:$s2: $Id: UPX • 0x1fd08:$s3: $Info: This file is packed with the UPX executable packer
Mozi.a	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x37450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x374c0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37530:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x375a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37610:$xo1: oMXKNNC\x0D\x17\x0C\x12
Mozi.a	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Mozi.a	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
Mozi.a	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
5244.1.00000000462a18a2.00000000e4311033.r-x.sdmp	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x1fce8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x1fd57:$s2: $Id: UPX • 0x1fd08:$s3: $Info: This file is packed with the UPX executable packer

Jbx Signature Overview



- AV Detection
- Spreading
- Networking
- System Summary
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Spreading:

Found strings indicative of a multi-platform dropper

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

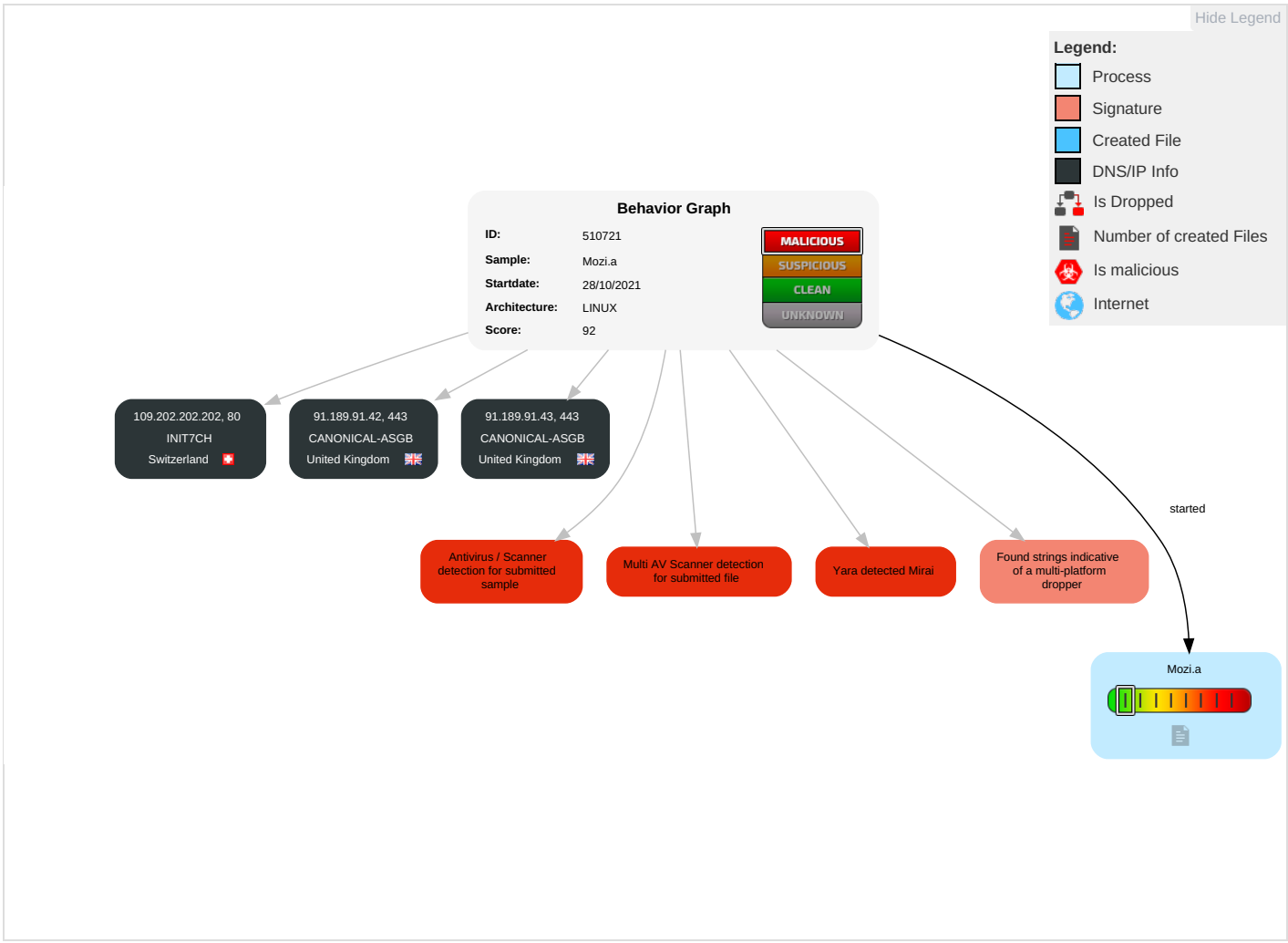
Mitre Att&ck Matrix

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	Command and Scripting Interpreter 1	Path Interception	Path Interception	Scripting 1	Brute Force 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scripting 1	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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Mozi.a	64%	Virustotal		Browse
Mozi.a	50%	Metadefender		Browse
Mozi.a	79%	ReversingLabs	Linux.Trojan.Mirai	
Mozi.a	100%	Avira	LINUX/Mirai.oreox	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://%s:%d/bin.sh;chmod	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;chmod	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;/tmp/Mozi.m	0%	Avira URL Cloud	safe	
http://%s:%d/bin.sh	0%	Avira URL Cloud	safe	
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://%s:%d/Mozi.m;	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;$	0%	Avira URL Cloud	safe	
http://HTTP/1.1	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;sh$	0%	Avira URL Cloud	safe	
http://127.0.0.1	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m	0%	Avira URL Cloud	safe	
http://127.0.0.1sendcmd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Runtime Messages

Command:	/tmp/Mozi.a
Exit Code:	133
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 5 (Trace/breakpoint trap) - core dumped

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
109.202.202.202	ggbMKQDdG2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	
	AbriuSDkeL	Get hash	malicious	Browse	
	xjmPNreY8l	Get hash	malicious	Browse	
	u7kjf23xQc	Get hash	malicious	Browse	
	nrT4coM180	Get hash	malicious	Browse	
	Fy8SpcfH79	Get hash	malicious	Browse	
	6vqWv6BFhR	Get hash	malicious	Browse	
	WaH4Q4OTzD	Get hash	malicious	Browse	
	6s4RqypN8p	Get hash	malicious	Browse	
	0vknf5ybYd	Get hash	malicious	Browse	
	sddX6Yllru	Get hash	malicious	Browse	
	8NC2CO6W0B	Get hash	malicious	Browse	
	nEzZe0JYXL	Get hash	malicious	Browse	
	D3xbHFJTIC	Get hash	malicious	Browse	
	ivgMZPUOLx	Get hash	malicious	Browse	
	5VWtwrKOJb	Get hash	malicious	Browse	
	Bs5fIqZapq	Get hash	malicious	Browse	
	hZt4RvNpGT	Get hash	malicious	Browse	
	nCEHDEKsvv	Get hash	malicious	Browse	
91.189.91.43	ggbMKQDdG2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	
	AbriuSDkeL	Get hash	malicious	Browse	
	xjmPNreY8l	Get hash	malicious	Browse	
	u7kjf23xQc	Get hash	malicious	Browse	
	nrT4coM180	Get hash	malicious	Browse	
	Fy8SpcfH79	Get hash	malicious	Browse	
	6vqWv6BFhR	Get hash	malicious	Browse	
	WaH4Q4OTzD	Get hash	malicious	Browse	
	6s4RqypN8p	Get hash	malicious	Browse	
	0vknf5ybYd	Get hash	malicious	Browse	
	sddX6Yllru	Get hash	malicious	Browse	
	8NC2CO6W0B	Get hash	malicious	Browse	
	nEzZe0JYXL	Get hash	malicious	Browse	
	D3xbHFJTIC	Get hash	malicious	Browse	
	ivgMZPUOLx	Get hash	malicious	Browse	
	5VWtwrKOJb	Get hash	malicious	Browse	
	Bs5fIqZapq	Get hash	malicious	Browse	
	hZt4RvNpGT	Get hash	malicious	Browse	
	nCEHDEKsvv	Get hash	malicious	Browse	
91.189.91.42	ggbMKQDdG2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	
	AbriuSDkeL	Get hash	malicious	Browse	
	xjmPNreY8l	Get hash	malicious	Browse	
	u7kjf23xQc	Get hash	malicious	Browse	
	nrT4coM180	Get hash	malicious	Browse	
	Fy8SpcfH79	Get hash	malicious	Browse	
	6vqWv6BFhR	Get hash	malicious	Browse	
	WaH4Q4OTzD	Get hash	malicious	Browse	
	6s4RqypN8p	Get hash	malicious	Browse	
	0vknf5ybYd	Get hash	malicious	Browse	
	sddX6Yllru	Get hash	malicious	Browse	
	8NC2CO6W0B	Get hash	malicious	Browse	
	nEzZe0JYXL	Get hash	malicious	Browse	
	D3xbHFJTIC	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ivgMZPUOLx	Get hash	malicious	Browse	
	5VWtwrKOJb	Get hash	malicious	Browse	
	Bs5fIqZapq	Get hash	malicious	Browse	
	hZt4RvNpGT	Get hash	malicious	Browse	
	nCEHDEKsvv	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CANONICAL-ASGB	ggbMKQDdG2	Get hash	malicious	Browse	• 91.189.91.42
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	• 91.189.91.42
	AbriuSDkeL	Get hash	malicious	Browse	• 91.189.91.42
	xjmPNreY8l	Get hash	malicious	Browse	• 91.189.91.42
	u7kjf23xQc	Get hash	malicious	Browse	• 91.189.91.42
	nrT4coM180	Get hash	malicious	Browse	• 91.189.91.42
	Fy8SpcfH79	Get hash	malicious	Browse	• 91.189.91.42
	6vqWv6BFhR	Get hash	malicious	Browse	• 91.189.91.42
	WaH4Q4OTzD	Get hash	malicious	Browse	• 91.189.91.42
	6s4RqypN8p	Get hash	malicious	Browse	• 91.189.91.42
	0vknf5ybYd	Get hash	malicious	Browse	• 91.189.91.42
	sddX6Yllru	Get hash	malicious	Browse	• 91.189.91.42
	8NC2CO6W0B	Get hash	malicious	Browse	• 91.189.91.42
	nEzZe0JYXL	Get hash	malicious	Browse	• 91.189.91.42
	D3xbHFJTIC	Get hash	malicious	Browse	• 91.189.91.42
	ivgMZPUOLx	Get hash	malicious	Browse	• 91.189.91.42
	5VWtwrKOJb	Get hash	malicious	Browse	• 91.189.91.42
	Bs5fIqZapq	Get hash	malicious	Browse	• 91.189.91.42
	hZt4RvNpGT	Get hash	malicious	Browse	• 91.189.91.42
	nCEHDEKsvv	Get hash	malicious	Browse	• 91.189.91.42
CANONICAL-ASGB	ggbMKQDdG2	Get hash	malicious	Browse	• 91.189.91.42
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	• 91.189.91.42
	AbriuSDkeL	Get hash	malicious	Browse	• 91.189.91.42
	xjmPNreY8l	Get hash	malicious	Browse	• 91.189.91.42
	u7kjf23xQc	Get hash	malicious	Browse	• 91.189.91.42
	nrT4coM180	Get hash	malicious	Browse	• 91.189.91.42
	Fy8SpcfH79	Get hash	malicious	Browse	• 91.189.91.42
	6vqWv6BFhR	Get hash	malicious	Browse	• 91.189.91.42
	WaH4Q4OTzD	Get hash	malicious	Browse	• 91.189.91.42
	6s4RqypN8p	Get hash	malicious	Browse	• 91.189.91.42
	0vknf5ybYd	Get hash	malicious	Browse	• 91.189.91.42
	sddX6Yllru	Get hash	malicious	Browse	• 91.189.91.42
	8NC2CO6W0B	Get hash	malicious	Browse	• 91.189.91.42
	nEzZe0JYXL	Get hash	malicious	Browse	• 91.189.91.42
	D3xbHFJTIC	Get hash	malicious	Browse	• 91.189.91.42
	ivgMZPUOLx	Get hash	malicious	Browse	• 91.189.91.42
	5VWtwrKOJb	Get hash	malicious	Browse	• 91.189.91.42
	Bs5fIqZapq	Get hash	malicious	Browse	• 91.189.91.42
	hZt4RvNpGT	Get hash	malicious	Browse	• 91.189.91.42
	nCEHDEKsvv	Get hash	malicious	Browse	• 91.189.91.42
INIT7CH	ggbMKQDdG2	Get hash	malicious	Browse	• 109.202.202.202
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	• 109.202.202.202
	AbriuSDkeL	Get hash	malicious	Browse	• 109.202.202.202
	xjmPNreY8l	Get hash	malicious	Browse	• 109.202.202.202
	u7kjf23xQc	Get hash	malicious	Browse	• 109.202.202.202
	nrT4coM180	Get hash	malicious	Browse	• 109.202.202.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Fy8SpcfH79	Get hash	malicious	Browse	• 109.202.202.202
	6vqWv6BFhR	Get hash	malicious	Browse	• 109.202.202.202
	WaH4Q4OTzD	Get hash	malicious	Browse	• 109.202.202.202
	6s4RqypN8p	Get hash	malicious	Browse	• 109.202.202.202
	0vknf5ybYd	Get hash	malicious	Browse	• 109.202.202.202
	sddX6Yllru	Get hash	malicious	Browse	• 109.202.202.202
	8NC2CO6W0B	Get hash	malicious	Browse	• 109.202.202.202
	nEzZe0JYXL	Get hash	malicious	Browse	• 109.202.202.202
	D3xbHFJTIC	Get hash	malicious	Browse	• 109.202.202.202
	ivgMZPUOLx	Get hash	malicious	Browse	• 109.202.202.202
	5VWtwrKOJb	Get hash	malicious	Browse	• 109.202.202.202
	Bs5fIqZapq	Get hash	malicious	Browse	• 109.202.202.202
	hZt4RvNpGT	Get hash	malicious	Browse	• 109.202.202.202
	nCEHDEKsvv	Get hash	malicious	Browse	• 109.202.202.202

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 MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.016914162546184
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	Mozi.a
File size:	307960
MD5:	e30a81d66f18f07647397d1defbad11b
SHA1:	a7fd1a1d71f7f7b00886741db52c42af0c8873f1
SHA256:	b7ba5aa2f8f7781d408e87b2131fa2cc9b95cdf3460f9778229398c9e851772a
SHA512:	df7b274ac394ca1192019d35212b076d645e095050930a42342d32d7937b37a7981c19029ecb54d9390bd8a9ba91fb137d52e89b176891ac05809daa1a28b766
SSDEEP:	6144:7O/QJHZweEL/NOjCHm7FZZncaoNsKqqfPqOJ:78QpZsKCaiaHKqoPqOJ
File Content Preview:	.ELF.....A.h...4.....4. ...(.....@...@.....C...C.....*.*UPX!.X.....\....|.$..ELF.....@.`....4..^h... ...(.....<...@.....ll.....H.W.`.t.d.....dt.Q.....].M.....6...

Static ELF Info

ELF header

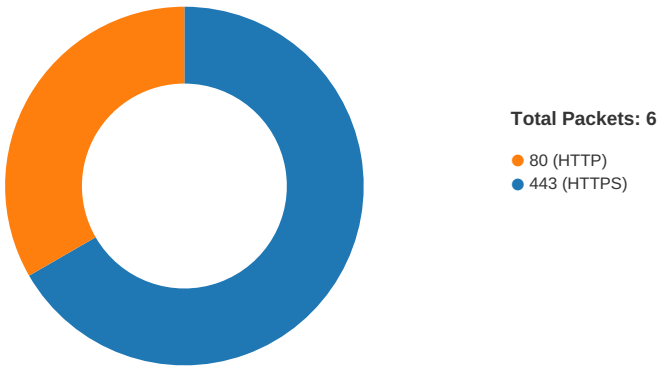
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x41fb68
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
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	0x400000	0x400000	0x205b2	0x205b2	4.4298	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x8ac18	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: Mozi.a PID: 5244 Parent PID: 5118

General

Start time:	06:47:10
Start date:	28/10/2021
Path:	/tmp/Mozi.a
Arguments:	/tmp/Mozi.a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read