

JOeSandbox Cloud BASIC



ID: 645916

Sample Name: Mozi.m

Cookbook:

defaultlinuxfilecookbook.jbs

Time: 07:33:36

Date: 15/06/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Linux Analysis Report Mozi.m	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Analysis Advice	3
General Information	3
Runtime Messages	3
Process Tree	4
Yara Signatures	4
Initial Sample	4
Memory Dumps	4
Snort Signatures	4
Joe Sandbox Signatures	4
AV Detection	4
Data Obfuscation	4
Mitre Att&ck Matrix	4
Malware Configuration	5
Behavior Graph	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	6
World Map of Contacted IPs	6
Public IPs	6
Joe Sandbox View / Context	6
IPs	6
Domains	7
ASNs	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	7
General	7
Static ELF Info	7
ELF header	7
Program Segments	8
Network Behavior	8
Network Port Distribution	8
TCP Packets	8
System Behavior	8
Analysis Process: Mozi.m PID: 6230, Parent PID: 6125	8
General	8
File Activities	8
File Read	8

Linux Analysis Report

Mozi.m

Overview

General Information

Sample Name:	Mozi.m
Analysis ID:	645916
MD5:	59ce0baba11893..
SHA1:	5857a7dd621c4c..
SHA256:	4293c1d8574dc8..
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

Antivirus / Scanner detection for sub...

Multi AV Scanner detection for subm...

Sample is packed with UPX

Sample contains only a LOAD segm...

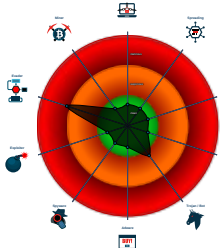
Yara signature match

Uses the "uname" system call to qu...

Tries to connect to HTTP servers, b...

ELF contains segments with high en...

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.
- 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 only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	645916
Start date and time: 15/06/202207:33:36	2022-06-15 07:33:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Mozi.m
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:	mal60.evad.linM@0/0@0/0

Runtime Messages

Command:	/tmp/Mozi.m
PID:	6230
Exit Code:	133
Exit Code Info:	
Killed:	False
Standard Output:	

Standard Error: gemu: uncaught target signal 5 (Trace/breakpoint trap) - core dumped

Process Tree

- system is Inxubuntu20
 - [Mozi.m](#) (PID: 6230, Parent: 6125, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/Mozi.m
- cleanup

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Mozi.m	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	0x20828:\$s1: PROT_EXEC PROT_WRITE failed. 0x20897:\$s2: \$Id: UPX 0x20848:\$s3: \$Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
6230.1.00000000fc11ff02.00000000bed15890.r-x.sdmp	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	0x20828:\$s1: PROT_EXEC PROT_WRITE failed. 0x20897:\$s2: \$Id: UPX 0x20848:\$s3: \$Info: This file is packed with the UPX executable packer

Snort Signatures

⛔ No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Data Obfuscation



Sample is packed with UPX

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	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

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

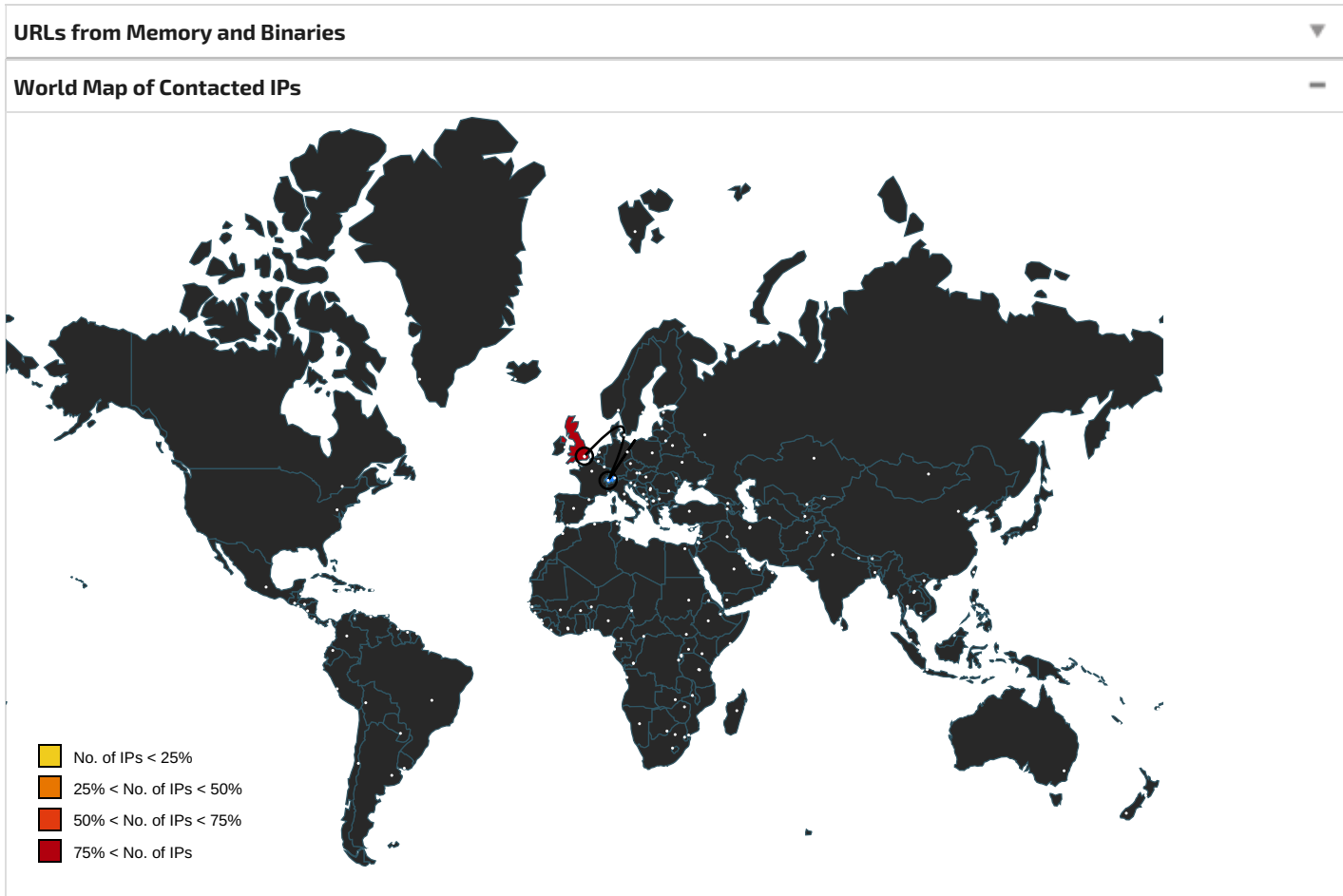
URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info



Public IPs

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

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 MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.814832789965999
TrID:	- ELF Executable and Linkable format (Linux) (4029/14) 50.16% - ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	Mozi.m
File size:	135784
MD5:	59ce0baba11893f90527fc951ac69912
SHA1:	5857a7dd621c4c3ebb0b5a3bec915d409f70d39f
SHA256:	4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7
SHA512:	c5b12797b477e5e5964a78766bb40b1c0d9fdfb8eef1f9aee3df451e3441a40c61d325bf400ba51048811b68e1c70a95f15e4166b7a65a4eca0c624864328647
SSDEEP:	3072:phNIHuBafLeBtfCzpta8xlBIOdVo3/4sxlJ10xioP:p3IOYoaJa8xzx/0wsxzSi2
TLSH:	E5D3128BEF36DC1ECF001EB226DA5B9E9C6D756B41CBF0A4B9C1818F13A01C97D52215
File Content Preview:	.ELF.....B.....4.....4. ..(.....@...@.....C..C...../*UPX!X.....^.... \$.ELF.....@.`....4...0... ..(.....<...@.....[v.....H...`.t.;_...dt.Q....].M.....

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:	0x4206a8
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52

ELF header

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	0x210f2	0x210f2	7.8156	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x92fd8	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



Total Packets: 6

- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

System Behavior

Analysis Process: Mozi.m PID: 6230, Parent PID: 6125	
General	
Start time:	07:34:22
Start date:	15/06/2022
Path:	/tmp/Mozi.m
Arguments:	/tmp/Mozi.m
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c
File Activities	
File Read	