ID: 650139
Sample Name: Mozi.m
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:42:56
Date: 22/06/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

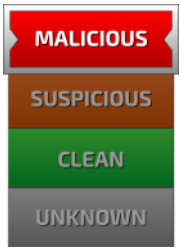
Mozi.m

Overview

General Information

Sample Name:	Mozi.m
Analysis ID:	650139
MD5:	59ce0baba11893..
SHA1:	5857a7dd621c4c..
SHA256:	4293c1d8574dc8..
Infos:	

Detection

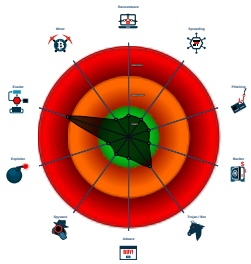


Score:	60
Range:	0 - 100
Whitelisted:	false

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:	650139
Start date and time: 22/06/202207:42:56	2022-06-22 07:42:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 7s
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:	6231
Exit Code:	133
Exit Code Info:	
Killed:	False
Standard Output:	

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

Process Tree

- **system is lnxubuntu20**
- Mozi.m (PID: 6231, Parent: 6129, 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
6231.1.0000000010bd2900.00000000e293fe0c.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

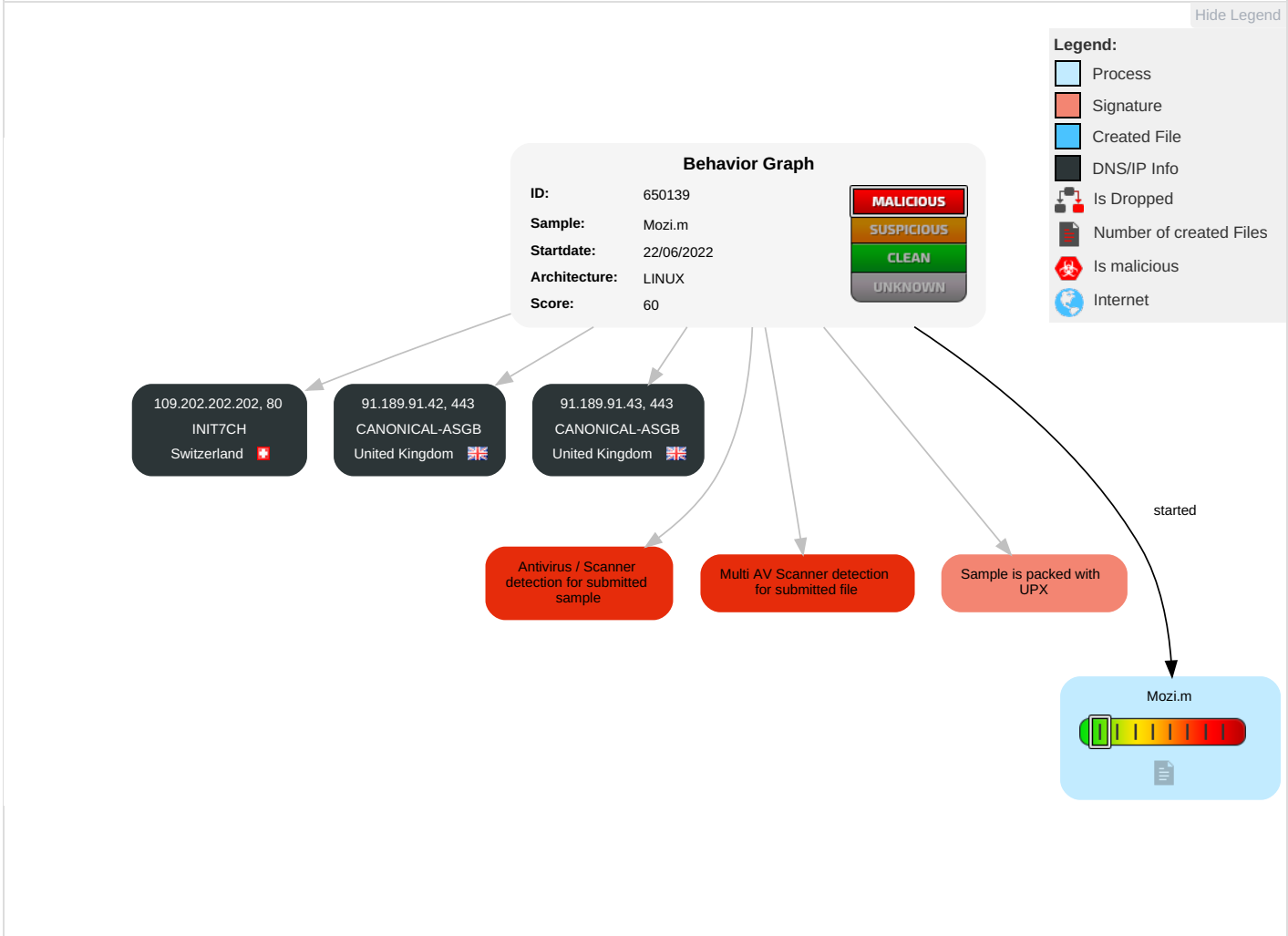
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 1 Obfuscated 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 Application Layer Protocol	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.m	66%	Virustotal		Browse
Mozi.m	41%	Metadefender		Browse
Mozi.m	71%	ReversingLabs	Linux.Trojan.Mirai	
Mozi.m	100%	Avira	LINUX/Mirai.dpaeh	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

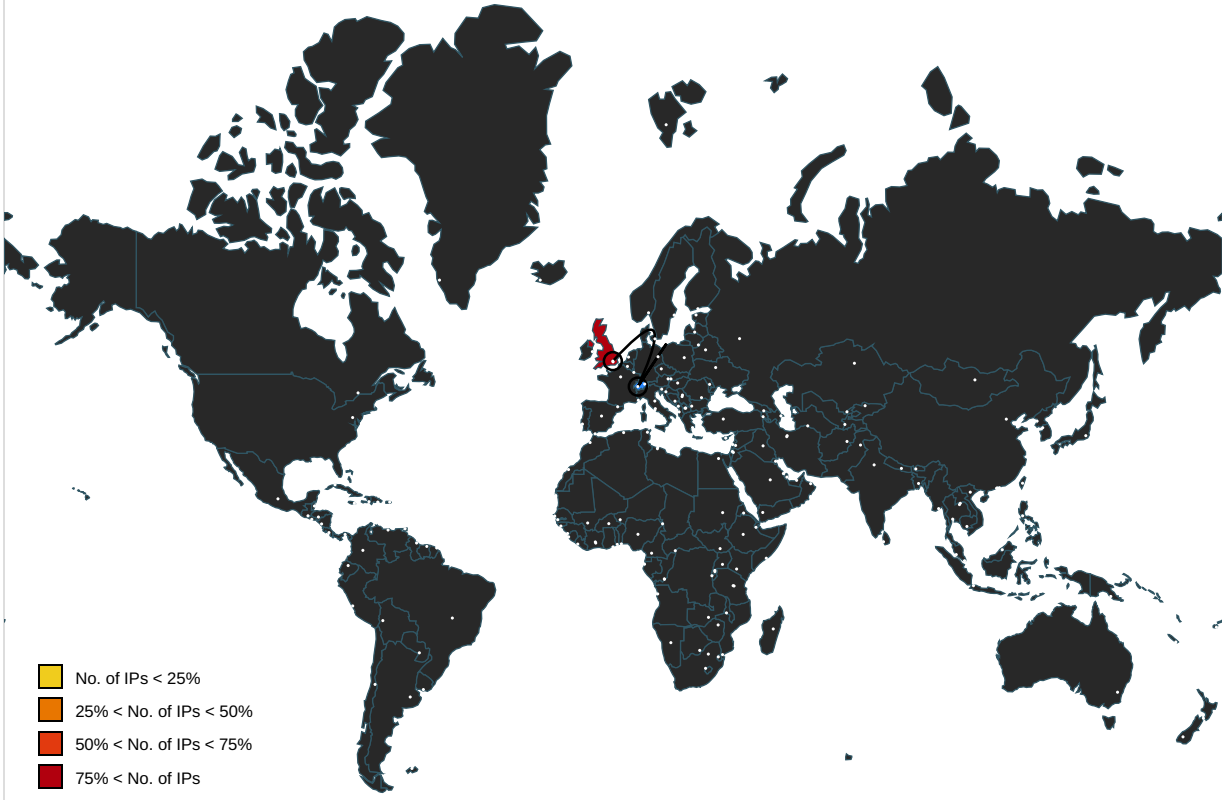
Domains and IPs

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
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:phNlHuBafLeBtfCzpta8xlBIOdVo3/4sxLJ10xioP:p3lOYoaja8xzx/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

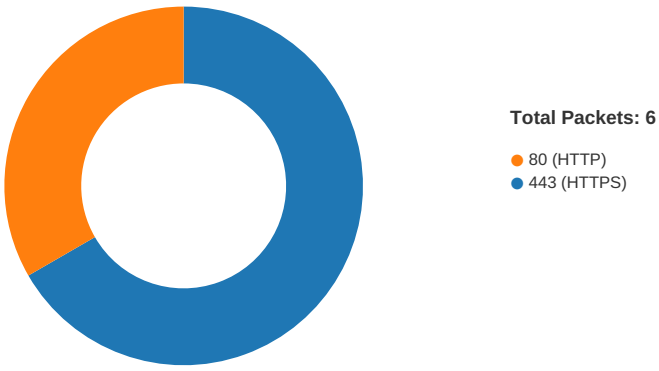
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

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



TCP Packets

System Behavior

Analysis Process: Mozi.m PID: 6231, Parent PID: 6129

General

Start time:	07:43:41
Start date:	22/06/2022
Path:	/tmp/Mozi.m
Arguments:	/tmp/Mozi.m
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read