ID: 604041
Sample Name: mozi.m
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:15:35
Date: 06/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

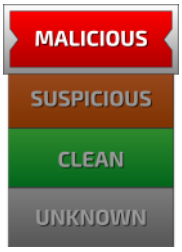
mozi.m

Overview

General Information

Sample Name:	mozi.m
Analysis ID:	604041
MD5:	3849f30b51a5c4..
SHA1:	61c74136534b82..
SHA256:	f6c97b1e2ed025..
Infos:	

Detection

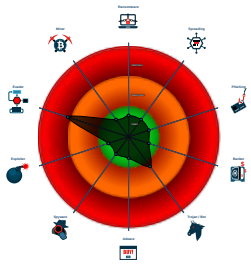


Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Yara signature match
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…

Classification



Analysis Advice

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.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	604041
Start date and time:	2022-04-06 14:15:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 29s
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:	5229
Exit Code:	133
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 5 (Trace/breakpoint trap) - core dumped

Copyright Joe Security LLC 2022

Process Tree

- **system is lnxubuntu20**
- mozi.m (PID: 5229, Parent: 5122, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) 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	• 0x20ec8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x20f37:$s2: $Id: UPX • 0x20ee8:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
5229.1.0000000006c36974.00000000324761c7.r-x.sdmp	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x20ec8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x20f37:$s2: $Id: UPX • 0x20ee8:$s3: $Info: This file is packed with the UPX executable packer

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

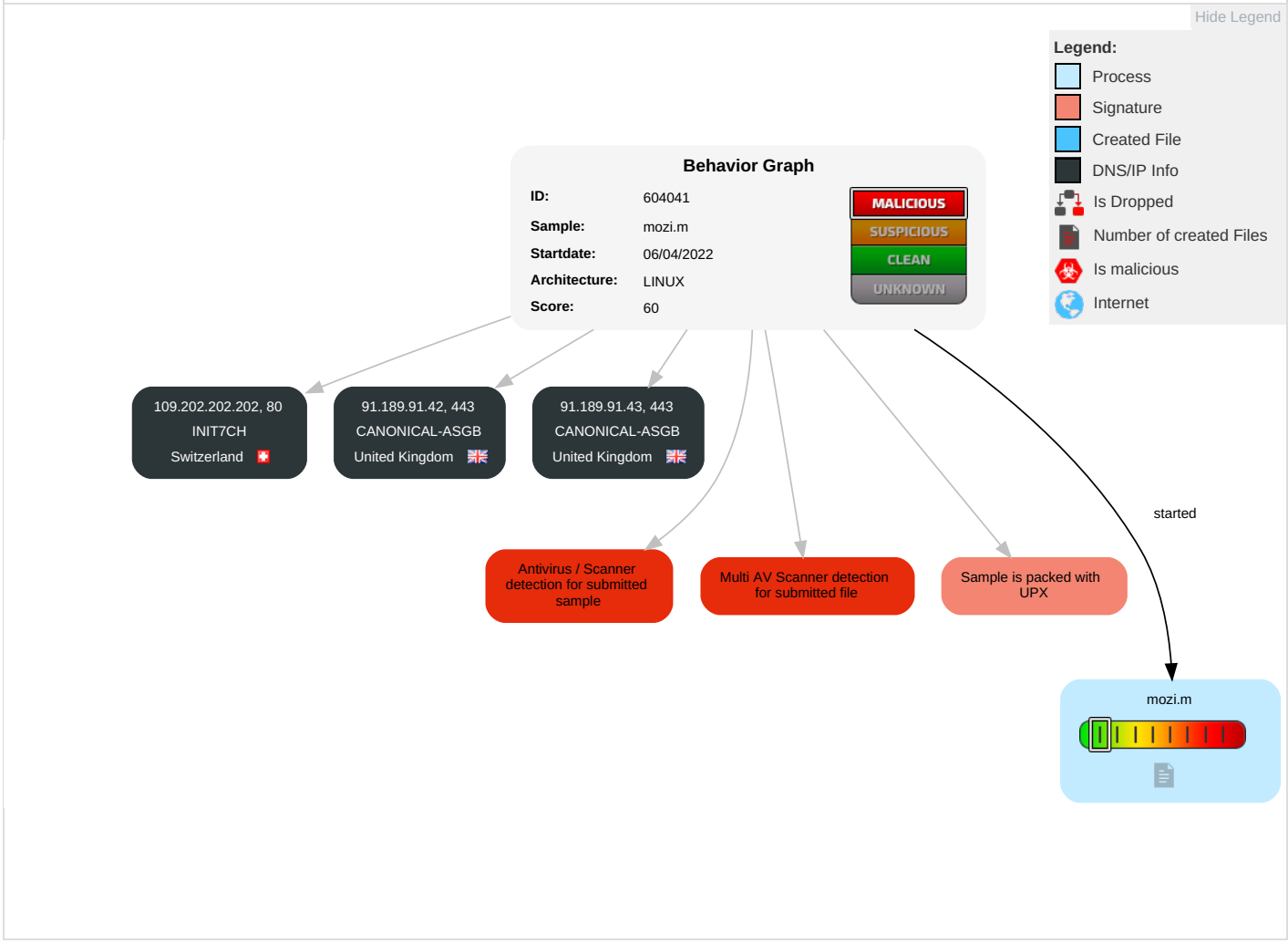
Mitre Att&ck Matrix

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 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
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	67%	Virustotal		Browse
mozi.m	49%	Metadefender		Browse
mozi.m	71%	ReversingLabs	Linux.Trojan.Mirai	
mozi.m	100%	Avira	LINUX/Mirai.trcie	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2022

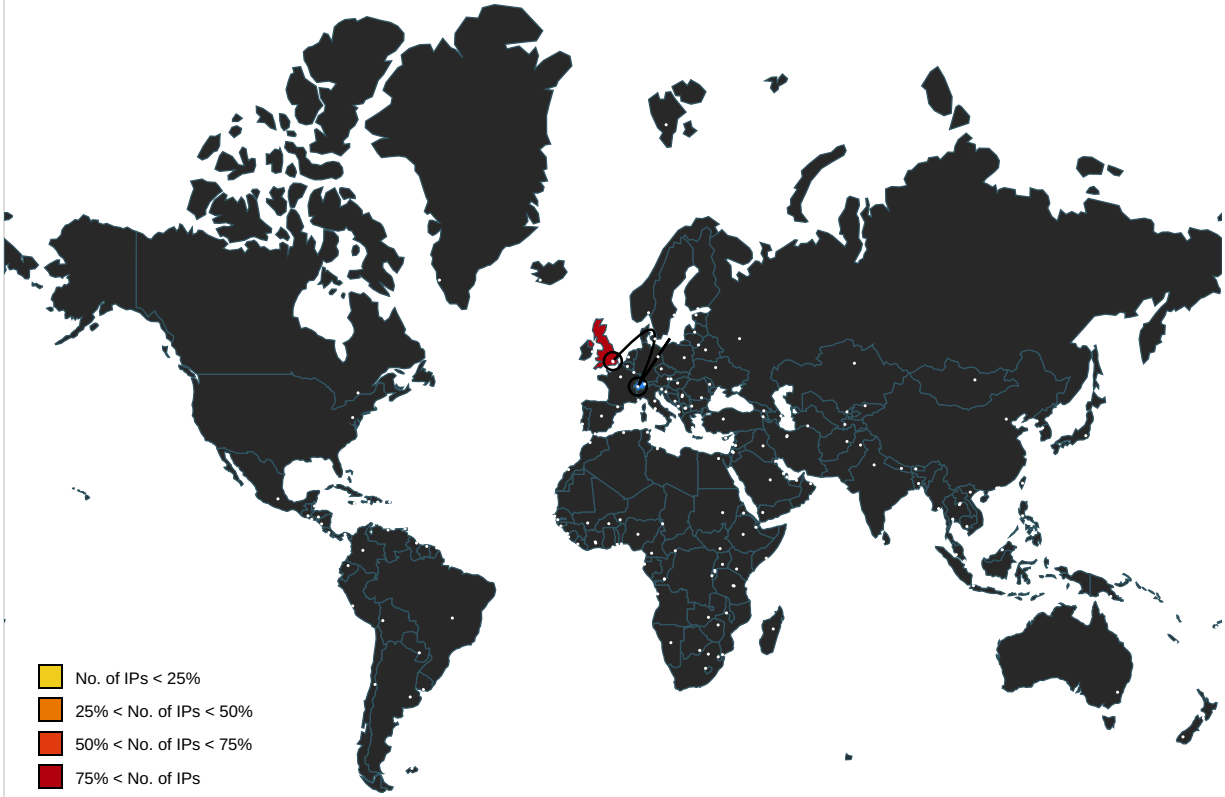
Domains and IPs

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

Copyright Joe Security LLC 2022

Dropped Files

No context

Created / dropped Files

No created / dropped files found

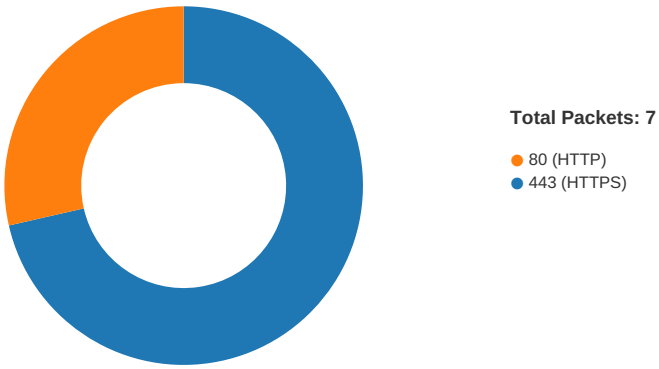
Static File Info

General

File type:	
Entropy (8bit):	7.812868686187402
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	mozi.m
File size:	137480
MD5:	3849f30b51a5c49e8d1546960cc206c7
SHA1:	61c74136534b826059c63221a2373dc0613a47b7
SHA256:	f6c97b1e2ed02578ca1066c8235ba4f991e645f89012406c639dbccc6582eec8
SHA512:	43d79293d1fbf716111c27e50df95a0860a0d706079625fa2b8a6b57c5ee06fa7b5b6b8c0acae33714a2181686426728513c990534e44b6f03a05dde0629ab86
SSDEEP:	3072:biMYFJvw6Yh0b1gKobtCGCmCRlrisfrYm:fYFJvwe1gKCYVl2szN
TLSH:	59D31322D3130C4FC02579FA7A2BE62A39873E6A24CE449C45F5D66A2FB7084ED71753
File Content Preview:	.ELF.....p.B.4.....4. ...(.....@...@.....C...C...../.....UPX!0.....].....?d..ELF.....`.@.....4.p..... ...(.....- ....@.....n'.....H..._....=..Q.td.....@.....

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: mozi.m PID: **5229**, Parent PID: **5122**

General	
Start time:	16:16:20
Start date:	06/04/2022
Path:	/tmp/mozi.m
Arguments:	/tmp/mozi.m
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read