ID: 337641
Sample Name: Mozi.m
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:45:57
Date: 09/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report Mozi.m

Overview

General Information

Sample Name:	Mozi.m
Analysis ID:	337641
MD5:	59ce0baba11893..
SHA1:	5857a7dd621c4c..
SHA256:	4293c1d8574dc8..

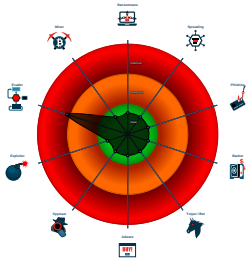
Detection

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…
- Uses the "uname" system call to qu…
- Yara signature match

Classification



Startup

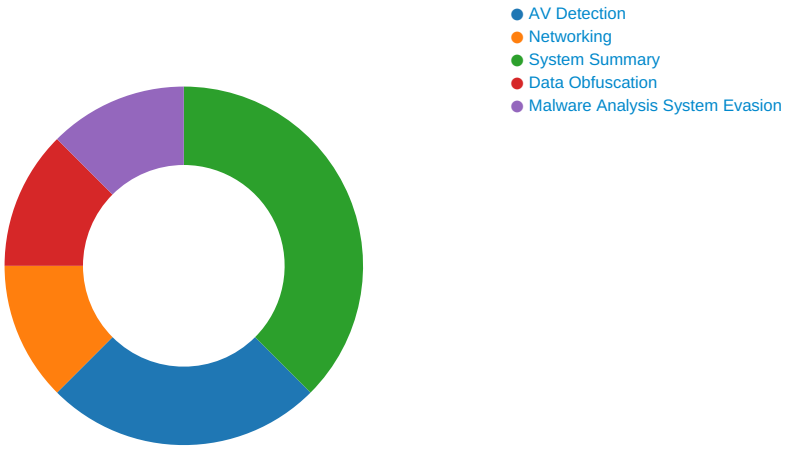
- **system is lnxubuntu1**
  - Mozi.m (PID: 4562, Parent: 4519, MD5: 59ce0baba11893f90527fc951ac69912) Arguments: /usr/bin/qemu-mips /tmp/Mozi.m
- upstart New Fork (PID: 4581, Parent: 3310)
  - sh (PID: 4581, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4582, Parent: 4581)
    - date (PID: 4582, Parent: 4581, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4583, Parent: 4581)
    - apport-checkreports (PID: 4583, Parent: 4581, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 4608, Parent: 3310)
  - sh (PID: 4608, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4609, Parent: 4608)
    - date (PID: 4609, Parent: 4608, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4618, Parent: 4608)
    - apport-gtk (PID: 4618, Parent: 4608, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- upstart New Fork (PID: 4635, Parent: 3310)
  - sh (PID: 4635, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4640, Parent: 4635)
    - date (PID: 4640, Parent: 4635, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4641, Parent: 4635)
    - apport-gtk (PID: 4641, Parent: 4635, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- **cleanup**

Yara Overview

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

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

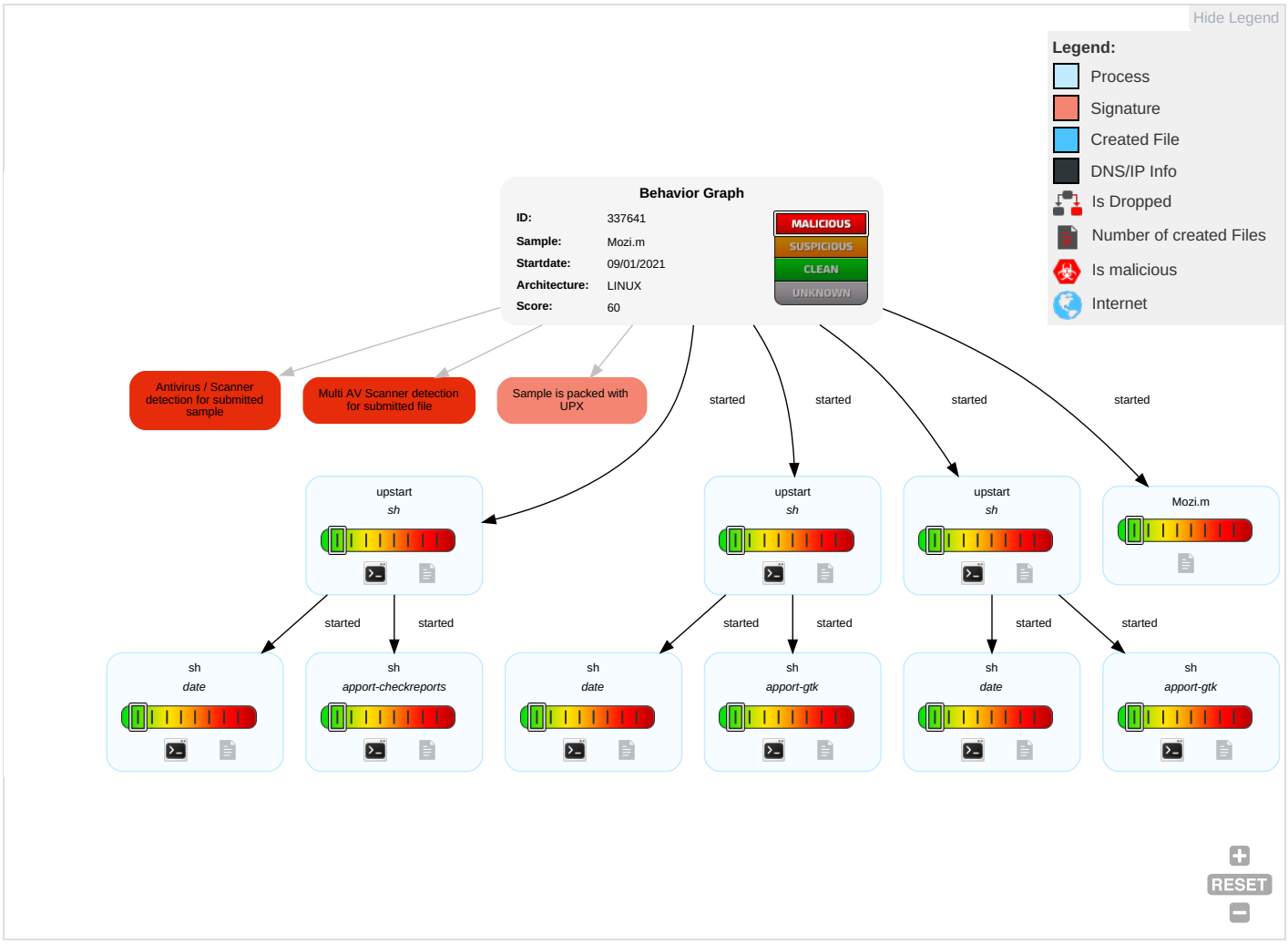
Data Obfuscation:

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	Obfuscated Files or Information 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Mozi.m	57%	Virustotal		Browse
Mozi.m	66%	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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337641
Start date:	09.01.2021
Start time:	00:45:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Mozi.m
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 16.04 x64 (Kernel 4.4.0-116, Firefox 59.0, Document Viewer 3.18.2, LibreOffice 5.1.6.2, OpenJDK 1.8.0_171)
Detection:	MAL
Classification:	mal60.evad.linM@0/2@0/0

Runtime Messages

Command:	/tmp/Mozi.m
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

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/var/crash/_usr_share_apport_apport-checkreports.1000.crash	
Process:	/usr/share/apport/apport-checkreports
File Type:	ASCII text
Category:	dropped
Size (bytes):	14915
Entropy (8bit):	4.692513303891342
Encrypted:	false
SSDEEP:	96:yBAgWi7qWy5faLrPP4uPeoi7JExK89E2lVzZQkQ4n/rJN2xEkh1LSEyKawggPICg:yBMMPP4dExtlVzKkQ4n1kmEmgPIehbM
MD5:	E33FF96345C09078D2C34698E54DB20E
SHA1:	D4173FAC622B564956EC584B3B1F3B04F58F93C6
SHA-256:	BA04C8CD364737CE5A20454ABDF719F0333857B47777B18029846BED36C72D96
SHA-512:	0A6F1BCE421560F87BE3D93AF0B1C6563E32F485E4A491E0BEBAD1F8C5C9AE304DC114DEDADFFAEF7BF39DE86A97B7BE78B8FECA6DB1791DB32B65DAF7166450
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Sat Jan 9 01:46:28 2021.ExecutablePath: /usr/share/apport/apport-checkreports.ExecutableTimestamp: 1514927430.InterpreterPath: /usr/bin/python3.5.ProcCmdline: /usr/bin/python3 /usr/share/apport/apport-checkreports --system.ProcCwd: /home/user.ProcEnviron:. LANGUAGE=en_US. PATH=(custom, user). XDG_RUNTIME_DIR=<set>. LANG=en_US.UTF-8. SHELL=/bin/bash.ProcMaps:. 00400000-007a9000 r-xp 00000000 fc:00 217 /usr/bin/python3.5. 009a9000-009ab000 r--p 003a9000 fc:00 217 /usr/bin/python3.5. 009ab000-00a42000 rw-p 003ab000 fc:00 217 /usr/bin/python3.5. 00a42000-00a73000 rw-p 00000000 00:00 0 . 026f3000-02a4b000 rw-p 00000000 00:00 0 [heap]. 7f28fa8ec000-7f28faa6d000 rw-p 00000000 00:00 0 . 7f28faa6d000-7f28faa84000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f28faa84000-7f28fac83000 ---p 00017000 fc:0

/var/crash/_usr_share_apport_apport-gtk.1000.crash	
Process:	/usr/share/apport/apport-gtk
File Type:	ASCII text
Category:	dropped
Size (bytes):	47094
Entropy (8bit):	4.497447016534422
Encrypted:	false
SSDEEP:	768:DPA5b5vuLJnU/R/U/R/KIM3uVIDmUc7PxkEqXxZ:m5vuLJU/R/U/R/8DmUc7PxkEqXxZ
MD5:	1D42EB982A5DA0526C3466D53C85368A
SHA1:	826061E42CE45136B609038CE73A6B7F34F2F2D4
SHA-256:	8E8F7DF9BFDA98C7F10ACFBA013BF5A316B4094547D1531293E87D88B3AA9C0A
SHA-512:	AADF54810905FAB19670699A06EB617F498DD09AA42EF23CD5FA9F1380D14C7A61C0A82838994952440F9D5E886E53DFCA9AB1D0122C5AEA34ACA15376968CF
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Sat Jan 9 01:46:28 2021.ExecutablePath: /usr/share/apport/apport-gtk.ExecutableTimestamp: 1514927430.InterpreterPath: /usr/bin/python3.5.ProcCmdline: /usr/bin/python3 /usr/share/apport/apport-gtk.ProcCwd: /home/user.ProcEnviron:. LANGUAGE=en_US. PATH=(custom, user). XDG_RUNTIME_DIR=<set>. LANG=en_US.UTF-8. SHELL=/bin/bash.ProcMaps:. 00400000-007a9000 r-xp 00000000 fc:00 217 /usr/bin/python3.5. 009a9000-009ab000 r--p 003a9000 fc:00 217 /usr/bin/python3.5. 009ab000-00a42000 rw-p 003ab000 fc:00 217 /usr/bin/python3.5. 00a42000-00a73000 rw-p 00000000 00:00 0 . 00ba8000-010c9000 rw-p 00000000 00:00 0 [heap]. 7f6b10517000-7f6b10617000 rw-p 00000000 00:00 0 . 7f6b10617000-7f6b1062e000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f6b1062e000-7f6b1082d000 ---p 00017000 fc:00 2382

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

General

SHA512:	c5b12797b477e5e5964a78766bb40b1c0d9fdfb8eef1f9a ee3df451e3441a40c61d325bf400ba51048811b68e1c70a 95f15e4166b7a65a4eca0c624864328647
SSDEEP:	3072:phNlHuBafLeBtfCzpta8xlBIOdVo3/4sxLJ10xioP:p 3lOYoaja8xzx/0wsxzSi2
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
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	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x210f2	0x210f2	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x92fd8	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: Mozi.m PID: 4562 Parent PID: 4519

General

Start time:	00:46:27
Start date:	09/01/2021
Path:	/tmp/Mozi.m
Arguments:	/usr/bin/qemu-mips /tmp/Mozi.m
File size:	135784 bytes
MD5 hash:	59ce0baba11893f90527fc951ac69912

File Activities

File Read

Analysis Process: upstart PID: 4581 Parent PID: 3310

General

Start time:	00:46:27
Start date:	09/01/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4581 Parent PID: 3310

General

Start time:	00:46:27
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 4582 Parent PID: 4581

General

Start time:	00:46:27
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4582 Parent PID: 4581

General

Start time:	00:46:27
Start date:	09/01/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4583 Parent PID: 4581

General

Start time:	00:46:27
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 4583 Parent PID: 4581

General

Start time:	00:46:27
Start date:	09/01/2021
Path:	/usr/share/apport/apport-checkreports
Arguments:	/usr/bin/python3 /usr/share/apport/apport-checkreports --system
File size:	1269 bytes
MD5 hash:	1a7d84ebc34df04e55ca3723541f48c9

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: upstart PID: 4608 Parent PID: 3310

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4608 Parent PID: 3310

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 4609 Parent PID: 4608

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4609 Parent PID: 4608

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4618 Parent PID: 4608

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4618 Parent PID: 4608

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: upstart PID: 4635 Parent PID: 3310

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4635 Parent PID: 3310

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: 4640 Parent PID: 4635

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4640 Parent PID: 4635

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4641 Parent PID: 4635

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4641 Parent PID: 4635

General

Start time:	00:46:28
Start date:	09/01/2021
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

Directory Enumerated