

JOeSandbox Cloud BASIC



ID: 384609

Sample Name: Mozi.m

Cookbook:

defaultlinuxfilecookbook.jbs

Time: 14:30:34

Date: 09/04/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report Mozi.m	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Yara Overview	4
Initial Sample	4
Signature Overview	4
AV Detection:	5
Data Obfuscation:	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	7
Contacted IPs	7
General Information	7
Runtime Messages	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASN	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	8
Static File Info	8
General	8
Static ELF Info	9
ELF header	9
Program Segments	9
Network Behavior	9
UDP Packets	9
System Behavior	9
Analysis Process: Mozi.m PID: 4581 Parent PID: 4519	9
General	9
File Activities	10
File Read	10
Analysis Process: upstart PID: 4598 Parent PID: 3310	10
General	10
Analysis Process: sh PID: 4598 Parent PID: 3310	10
General	10
File Activities	10
File Read	10
Analysis Process: sh PID: 4599 Parent PID: 4598	10
General	10
Analysis Process: date PID: 4599 Parent PID: 4598	10
General	10
File Activities	10
File Read	10
Analysis Process: sh PID: 4602 Parent PID: 4598	11

General	11
Analysis Process: apport-checkreports PID: 4602 Parent PID: 4598	11
General	11
File Activities	11
File Read	11
File Written	11
Directory Enumerated	11
Analysis Process: upstart PID: 4625 Parent PID: 3310	11
General	11
Analysis Process: sh PID: 4625 Parent PID: 3310	11
General	11
File Activities	11
File Read	12
Analysis Process: sh PID: 4626 Parent PID: 4625	12
General	12
Analysis Process: date PID: 4626 Parent PID: 4625	12
General	12
File Activities	12
File Read	12
Analysis Process: sh PID: 4627 Parent PID: 4625	12
General	12
Analysis Process: apport-gtk PID: 4627 Parent PID: 4625	12
General	12
File Activities	12
File Read	12
File Written	13
Directory Enumerated	13
Analysis Process: upstart PID: 4652 Parent PID: 3310	13
General	13
Analysis Process: sh PID: 4652 Parent PID: 3310	13
General	13
File Activities	13
File Read	13
Analysis Process: sh PID: 4653 Parent PID: 4652	13
General	13
Analysis Process: date PID: 4653 Parent PID: 4652	13
General	13
File Activities	13
File Read	14
Analysis Process: sh PID: 4655 Parent PID: 4652	14
General	14
Analysis Process: apport-gtk PID: 4655 Parent PID: 4652	14
General	14
File Activities	14
File Read	14
Directory Enumerated	14

Analysis Report Mozi.m

Overview

General Information

Sample Name:	Mozi.m
Analysis ID:	384609
MD5:	fbe51695e97a45d.
SHA1:	1ed14334b5b717..
SHA256:	2e4506802aede..
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

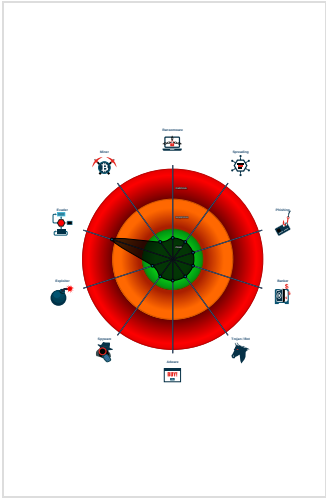
UNKNOWN

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

Classification



Startup

- system is Inxubuntu1
 - Mozi.m (PID: 4581, Parent: 4519, MD5: fbe51695e97a45dc61967dc3241a37dc) Arguments: /usr/bin/qemu-mips /tmp/Mozi.m
 - upstart New Fork (PID: 4598, Parent: 3310)
 - sh (PID: 4598, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
 - sh New Fork (PID: 4599, Parent: 4598)
 - date (PID: 4599, Parent: 4598, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
 - sh New Fork (PID: 4602, Parent: 4598)
 - apport-checkreports (PID: 4602, Parent: 4598, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
 - upstart New Fork (PID: 4625, Parent: 3310)
 - sh (PID: 4625, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
 - sh New Fork (PID: 4626, Parent: 4625)
 - date (PID: 4626, Parent: 4625, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
 - sh New Fork (PID: 4627, Parent: 4625)
 - apport-gtk (PID: 4627, Parent: 4625, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
 - upstart New Fork (PID: 4652, Parent: 3310)
 - sh (PID: 4652, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
 - sh New Fork (PID: 4653, Parent: 4652)
 - date (PID: 4653, Parent: 4652, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
 - sh New Fork (PID: 4655, Parent: 4652)
 - apport-gtk (PID: 4655, Parent: 4652, 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_Compessed_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

Signature Overview

- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Malware Analysis System Evasion



💡 Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Data Obfuscation:



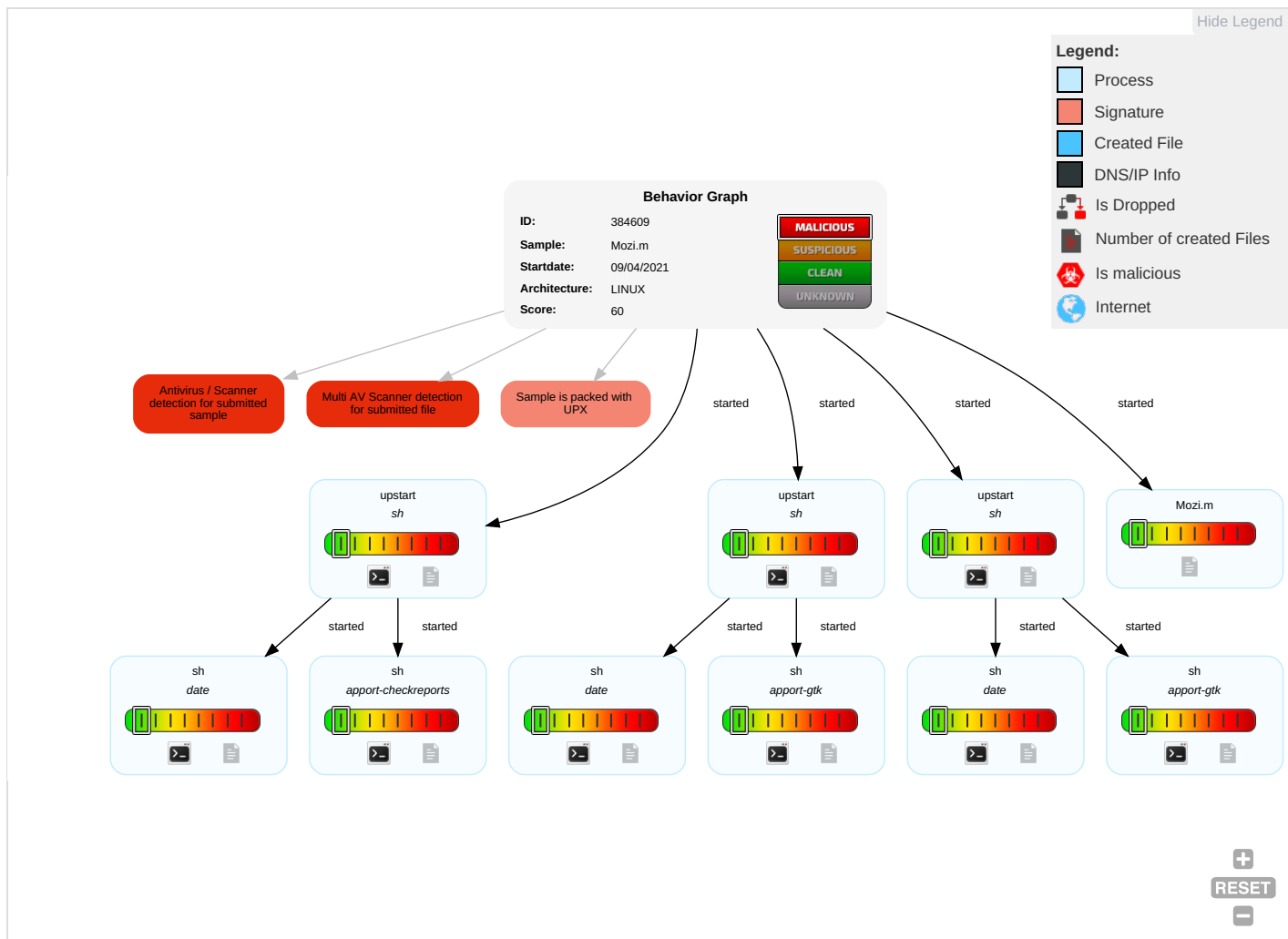
Sample is packed with UPX

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	59%	Virustotal		Browse
Mozi.m	42%	Metadefender		Browse
Mozi.m	67%	ReversingLabs	Linux.Trojan.Mirai	
Mozi.m	100%	Avira	LINUX/Mirai.souoo	

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 Emerald
Analysis ID:	384609
Start date:	09.04.2021
Start time:	14:30:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 47s
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)
Analysis Mode:	default
Detection:	MAL
Classification:	mal60.evad.linM@0/2@0/0
Warnings:	Show All

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):	14916
Entropy (8bit):	4.652650762078051
Encrypted:	false
SSDEEP:	192:wizrqYhhX17sQ8B3FO2Si9C8H2EAEBoPIYhbM:Jsh6+p2E6o
MD5:	A34A2946F7A3A056EB218AA265B867E8
SHA1:	2BA920A691FA0754C789039714A7A34894551E83
SHA-256:	144823131B1D8BFCF5E44D1A9921EE1B6D00A9C9DC2D3F653227566C33F2B192
SHA-512:	699D101E1CB40FEF7C01D9FC139193B7B4C3BE81BD4B02703A58B19AA22DC9FE8612074ABEA70CD322E2845CB79DF7ECEA0C34DF1B230AEF034ECBCE1007E173
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Fri Apr 9 16:31:03 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 . 01348000-016a0000 rw-p 00000000 00:00 0 [heap]. 7fd09cf56000-7fd09d0d7000 rw-p 00000000 00:00 0 . 7fd09d0d7000-7fd09d0ee000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7fd09d0ee000-7fd09d2ed000 ---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):	4.496719707041699
Encrypted:	false
SSDEEP:	768:qxpkmf/v/F/5/FIE38YcldDWlo6jyLsO2e2:Ukmf/v/F/5/xYcldho6jyLsO2e2
MD5:	2A68E710E17B3E374226B54BFFDF8227
SHA1:	B2FCCD7B82F5299796A55C33956AEF65206CD6A3
SHA-256:	3114009B0AD73EFA8CB19B753216335CD7BAB944D5EF8BCBF89EDD42C62FCADA
SHA-512:	B0CBD4C45FA6C0DA3A9A3A3608EC89ABD42C7DE8AD9CFA5CB695429A80911A4FCAF6C210196401DED917DB1AA0B6C41278BDDFC85A1C094A567825558C3CA07
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Fri Apr 9 16:31:03 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 . 014a1000-019b2000 rw-p 00000000 00:00 0 [heap]. 7f7f34c30000-7f7f34d30000 rw-p 00000000 00:00 0 . 7f7f34d30000-7f7f34d47000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f7f34d47000-7f7f34f46000 ---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):	7.813753507680382
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:	132876
MD5:	fbe51695e97a45dc61967dc3241a37dc
SHA1:	1ed14334b5b71783cd6ec14b8a704fe48e600cf0

General	
SHA256:	2e4506802aede2e6d53910dfb296323be6620ac08c4b799a879eace5923a7b6
SHA512:	c35eab56ba59beb2ec2b362e4d1aae734fadc2d9db1d720439337dcade13ec9c7b68da9d03821efc7277abaf9bace342ff35593373e04c67327d5f7db460ad8a
SSDEEP:	3072:/TNVO/QJHZcfFj4rwLQGTNO5VZLwHm7vuQTpZUyY6cot:7O/QJHZweEL/NOjCHm7FZZncl
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	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x205b2	0x205b2	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x8ac18	0x6	RW	0x10000		

Network Behavior

UDP Packets

System Behavior

Analysis Process: Mozi.m PID: 4581 Parent PID: 4519

General

Start time:	14:31:02
Start date:	09/04/2021
Path:	/tmp/Mozi.m
Arguments:	/usr/bin/qemu-mips /tmp/Mozi.m
File size:	132876 bytes
MD5 hash:	fbe51695e97a45dc61967dc3241a37dc

File Activities

File Read

Analysis Process: upstart PID: 4598 Parent PID: 3310

General

Start time:	14:31:02
Start date:	09/04/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4598 Parent PID: 3310

General

Start time:	14:31:02
Start date:	09/04/2021
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: 4599 Parent PID: 4598

General

Start time:	14:31:02
Start date:	09/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4599 Parent PID: 4598

General

Start time:	14:31:02
Start date:	09/04/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4602 Parent PID: 4598**General**

Start time:	14:31:02
Start date:	09/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 4602 Parent PID: 4598**General**

Start time:	14:31:02
Start date:	09/04/2021
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: 4625 Parent PID: 3310****General**

Start time:	14:31:03
Start date:	09/04/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4625 Parent PID: 3310**General**

Start time:	14:31:03
Start date:	09/04/2021
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: 4626 Parent PID: 4625



General



Start time:	14:31:03
Start date:	09/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4626 Parent PID: 4625



General



Start time:	14:31:03
Start date:	09/04/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read



Analysis Process: sh PID: 4627 Parent PID: 4625



General



Start time:	14:31:03
Start date:	09/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4627 Parent PID: 4625



General



Start time:	14:31:03
Start date:	09/04/2021
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: 4652 Parent PID: 3310



General



Start time:	14:31:03
Start date:	09/04/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4652 Parent PID: 3310



General



Start time:	14:31:03
Start date:	09/04/2021
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: 4653 Parent PID: 4652



General



Start time:	14:31:03
Start date:	09/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4653 Parent PID: 4652



General



Start time:	14:31:03
Start date:	09/04/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read



Analysis Process: sh PID: 4655 Parent PID: 4652



General



Start time:	14:31:03
Start date:	09/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4655 Parent PID: 4652



General



Start time:	14:31:03
Start date:	09/04/2021
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

