ID: 450743
Sample Name: Mozi.m
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 17:05:52
Date: 19/07/2021
Version: 33.0.0 White Diamond

Table of Contents

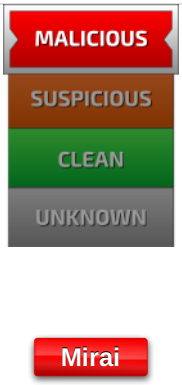
Linux Analysis Report Mozi.m

Overview

General Information

Sample Name:	Mozi.m
Analysis ID:	450743
MD5:	e957309c9cb381..
SHA1:	3589d0f624deb03.
SHA256:	54dfe49f5b11403..
Infos:	

Detection

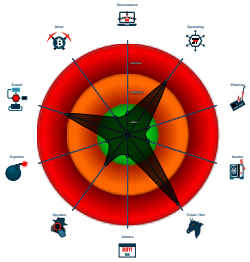


Score:	96
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Mirai
- Yara detected Mirai
- Yara detected Mirai
- Yara detected Mirai
- Found strings indicative of a multi-pl…
- Sample is packed with UPX
- Sample contains only a LOAD segm…
- Sample contains strings indicative o…
- Sample contains strings indicative o…
- Sample contains strings that are not

Classification



Analysis Advice

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 not execute correctly on this machine

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	450743
Start date:	19.07.2021
Start time:	17:05:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
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:	mal96.spre.troj.evad.linM@0/2@0/0
Warnings:	Show All

Process Tree

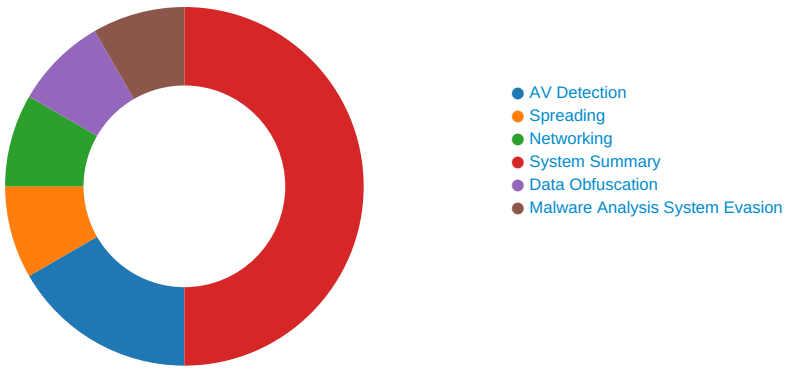
- **system is lnxubuntu1**
  - Mozi.m (PID: 4568, Parent: 4498, MD5: e957309c9cb381574c622b2d2a6798c0) Arguments: /usr/bin/qemu-mips /tmp/Mozi.m
- upstart New Fork (PID: 4587, Parent: 3310)
  - sh (PID: 4587, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4588, Parent: 4587)
    - date (PID: 4588, Parent: 4587, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4589, Parent: 4587)
    - apport-checkreports (PID: 4589, Parent: 4587, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 4614, Parent: 3310)
  - sh (PID: 4614, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4615, Parent: 4614)
    - date (PID: 4615, Parent: 4614, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4632, Parent: 4614)
    - apport-gtk (PID: 4632, Parent: 4614, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- upstart New Fork (PID: 4641, Parent: 3310)
  - sh (PID: 4641, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4643, Parent: 4641)
    - date (PID: 4643, Parent: 4641, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4659, Parent: 4641)
    - apport-gtk (PID: 4659, Parent: 4641, 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	• 0x1fce8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x1fd57:$s2: $Id: UPX • 0x1fd08:$s3: $Info: This file is packed with the UPX executable packer
Mozi.m	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x37450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x374c0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37530:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x375a0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x37610:$xo1: oMXKNNC\x0D\x17\x0C\x12
Mozi.m	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Mozi.m	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
Mozi.m	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
Click to see the 1 entries				

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Spreading:

Found strings indicative of a multi-platform dropper

Data Obfuscation:

Sample is packed with UPX

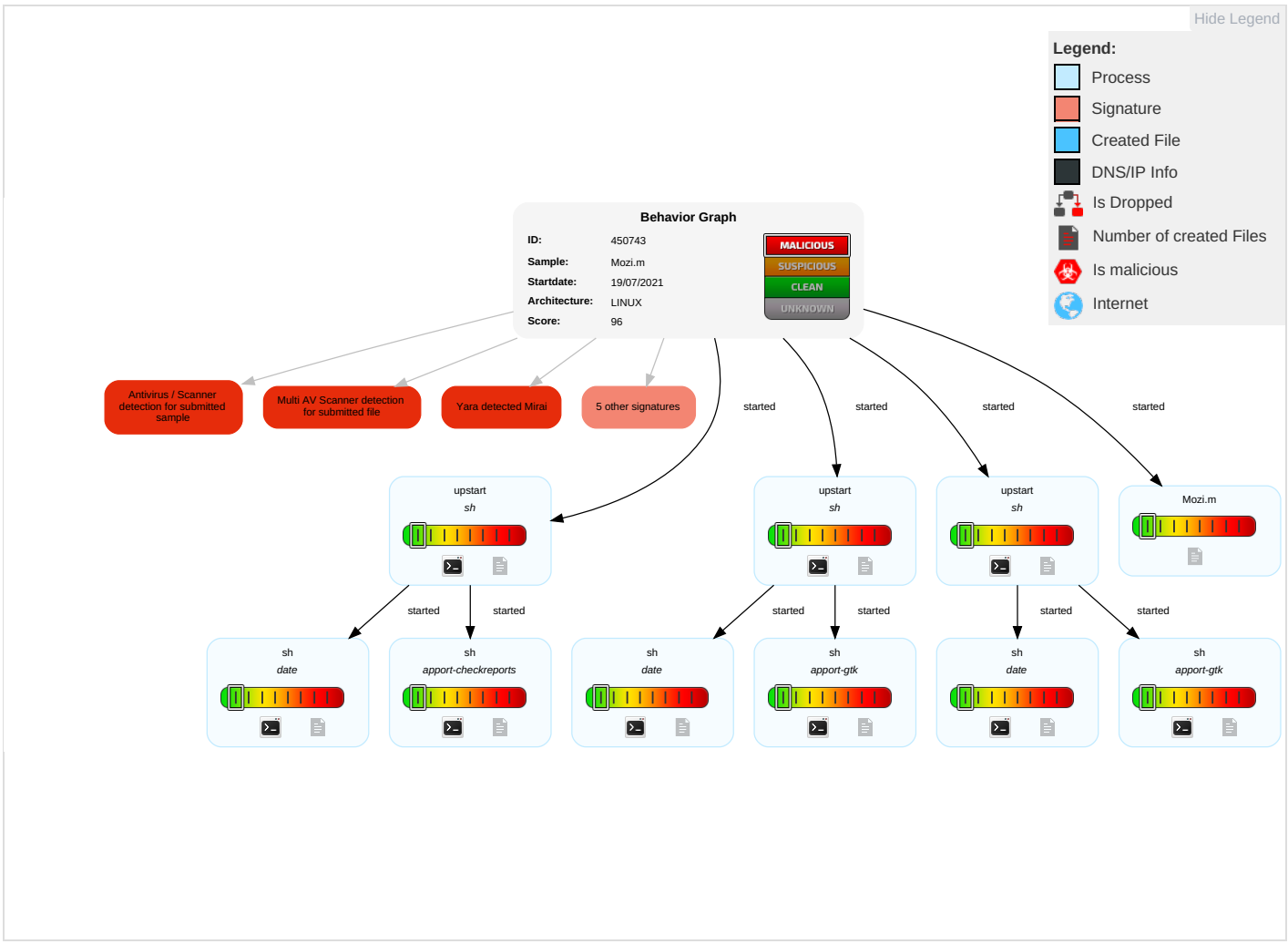
Mitre Att&ck Matrix

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	Command and Scripting Interpreter 1	Path Interception	Path Interception	Scripting 1	Brute Force 1	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
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	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	60%	Virustotal		Browse
Mozi.m	43%	Metadefender		Browse
Mozi.m	67%	ReversingLabs	Linux.Trojan.Mirai	
Mozi.m	100%	Avira	LINUX/Mirai.cuqzt	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://%s:%d/bin.sh;chmod	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;chmod	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;/tmp/Mozi.m	0%	Avira URL Cloud	safe	
http://%s:%d/bin.sh	0%	Avira URL Cloud	safe	
http://purenetworks.com/HNAP1/	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m;$	0%	Avira URL Cloud	safe	
http://HTTP/1.1	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.a;sh$	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://127.0.0.1	0%	Avira URL Cloud	safe	
http://%s:%d/Mozi.m	0%	Avira URL Cloud	safe	
http://127.0.0.1sendcmd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

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

/var/crash/_usr_share_apport_apport-checkreports.1000.crash	
Size (bytes):	14915
Entropy (8bit):	4.685592697936091
Encrypted:	false
SSDEEP:	192:gIfh25JHJ5NNhfK54aqaG0KRE4rIPIehbM:ZfMXpO5GRERo
MD5:	369014BA6E21E3A99CA5E15A3066F52A
SHA1:	58C2811B8BE49B52A3C9ABA50C23BED1F88A0F07
SHA-256:	740C55D8B9FC3B7BB62D57D162072B9902458970825D98022666CC445CD83774
SHA-512:	30035359A00BAD2127309D37FEED744D2470C8A820A530ED0DDBE5D7ABDEBA4E38B1F5E97D8F29F25D00956CD858E73B6A307D8FB1493258E5628C85952DCD1
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Mon Jul 19 19:06:24 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 . 01cc4000-0201c000 rw-p 00000000 00:00 0 [heap]. 7fdacf0b5000-7fdacf236000 rw-p 00000000 00:00 0 . 7fdacf236000-7fdacf24d000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7fdacf24d000-7fdacf44c000 ---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):	4.507687905583427
Encrypted:	false
SSDEEP:	768:L/X/+/L/Q+z6FlyxNe9Hb8fqCXdrBQKTVv:L/X/+/L/oyxNe9Hb8iCXdrBQKTVv
MD5:	BFBAC00590A85D4243E5742288EBA36F
SHA1:	EA17AE8007C0A8CA726BB6CD8AB11FA3C2B0B6ED
SHA-256:	1B7D539533FEF4C6B93F8556BE60B47018617E04FDBEA1C7D9EAA537DBD01CCC
SHA-512:	08557E8BFA541D2C69170FEABB5B46FECBD1FC75E65802A6139640128F0C22C996573F2AD06B141B8171A55267DAAC896B6154DBA04F3AD09B4498B6DD8C7F0
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Mon Jul 19 19:06:25 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 . 017fe000-01d1f000 rw-p 00000000 00:00 0 [heap]. 7fef3bb17000-7fef3bc17000 rw-p 00000000 00:00 0 . 7fef3bc17000-7fef3bc2e000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7fef3bc2e000-7fef3be2d000 ---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):	6.504782494511512
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:	307960
MD5:	e957309c9cb381574c622b2d2a6798c0
SHA1:	3589d0f624deb034ad2ac15cb1f1f0f0fde10908
SHA256:	54dfe49f5b114030c318eb1be2d86bdcfac3e10d730b08631028f992fc92c9d0
SHA512:	a1abd5f2aba76d3fdfa6404ea4a7b88513b42b9dbe3870ec30f0fba488a06a2db3feea12b4052cd82023d7a810cac16061f4ecf9764beea2260633769de2de67
SSDEEP:	6144:7O/QJHZweEL/NOjCHm7FZZnch5wKSDP99zBa77oNsKqqfPqOJ:78QpZsKCaihDSDP99zBa/HKqoPqOJ
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	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x205b2	0x205b2	4.4298	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x8ac18	0.0000	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: Mozi.m PID: 4568 Parent PID: 4498

General

Start time:	17:06:24
Start date:	19/07/2021
Path:	/tmp/Mozi.m
Arguments:	/usr/bin/qemu-mips /tmp/Mozi.m
File size:	307960 bytes
MD5 hash:	e957309c9cb381574c622b2d2a6798c0

File Activities

File Read

Analysis Process: upstart PID: 4587 Parent PID: 3310

General

Start time:	17:06:24

Start date:	19/07/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4587 Parent PID: 3310

General

Start time:	17:06:24
Start date:	19/07/2021
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: 4588 Parent PID: 4587

General

Start time:	17:06:24
Start date:	19/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4588 Parent PID: 4587

General

Start time:	17:06:24
Start date:	19/07/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4589 Parent PID: 4587

General

Start time:	17:06:24
Start date:	19/07/2021
Path:	/bin/sh
Arguments:	n/a

File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 4589 Parent PID: 4587

General

Start time:	17:06:24
Start date:	19/07/2021
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: 4614 Parent PID: 3310

General

Start time:	17:06:24
Start date:	19/07/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4614 Parent PID: 3310

General

Start time:	17:06:24
Start date:	19/07/2021
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: 4615 Parent PID: 4614

General

Start time:	17:06:24
Start date:	19/07/2021

Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4615 Parent PID: 4614

General

Start time:	17:06:24
Start date:	19/07/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4632 Parent PID: 4614

General

Start time:	17:06:24
Start date:	19/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4632 Parent PID: 4614

General

Start time:	17:06:24
Start date:	19/07/2021
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: 4641 Parent PID: 3310

General

Start time:	17:06:25
Start date:	19/07/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4641 Parent PID: 3310

General

Start time:	17:06:25
Start date:	19/07/2021
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: 4643 Parent PID: 4641

General

Start time:	17:06:25
Start date:	19/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4643 Parent PID: 4641

General

Start time:	17:06:25
Start date:	19/07/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4659 Parent PID: 4641

General

Start time:	17:06:25
Start date:	19/07/2021
Path:	/bin/sh

Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4659 Parent PID: 4641

General

Start time:	17:06:25
Start date:	19/07/2021
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