ID: 491333
Sample Name: index_2021-09-27-13_35
Cookbook: defaultlinuxfilecookbook.jbs
Time: 13:37:29
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

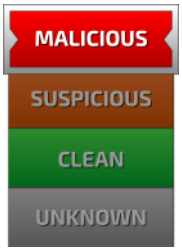
Linux Analysis Report index_2021-09-27-13_35

Overview

General Information

Sample Name:	index_2021-09-27-13_35
Analysis ID:	491333
MD5:	59ce0baba11893..
SHA1:	5857a7dd621c4c..
SHA256:	4293c1d8574dc8..
Infos:	

Detection

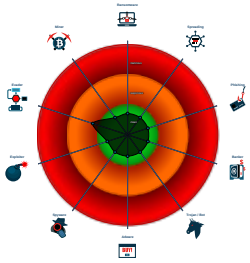


Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Uses the "uname" system call to qu…
- Sample contains only a LOAD segm…
- Yara signature match

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491333
Start date:	27.09.2021
Start time:	13:37:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	index_2021-09-27-13_35
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:	mal56.lin@0/2@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu1**
  - index_2021-09-27-13_35 (PID: 4666, Parent: 4595, MD5: 59ce0baba11893f90527fc951ac69912) Arguments: /usr/bin/qemu-mips /tmp/index_2021-09-27-13_35
- upstart New Fork (PID: 4682, Parent: 3310)
  - sh (PID: 4682, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4691, Parent: 4682)
    - date (PID: 4691, Parent: 4682, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4692, Parent: 4682)
    - apport-checkreports (PID: 4692, Parent: 4682, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 4709, Parent: 3310)
  - sh (PID: 4709, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4713, Parent: 4709)
    - date (PID: 4713, Parent: 4709, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4719, Parent: 4709)
    - apport-gtk (PID: 4719, Parent: 4709, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- upstart New Fork (PID: 4736, Parent: 3310)
  - sh (PID: 4736, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4737, Parent: 4736)
    - date (PID: 4737, Parent: 4736, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4738, Parent: 4736)
    - apport-gtk (PID: 4738, Parent: 4736, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- **cleanup**

Yara Overview

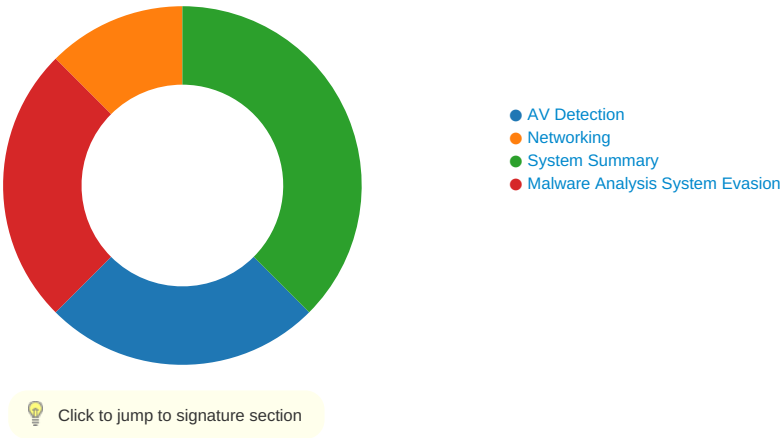
Initial Sample

Source	Rule	Description	Author	Strings
index_2021-09-27-13_35	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
4666.1.00007fab4a051000.00007fab4a073000.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

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

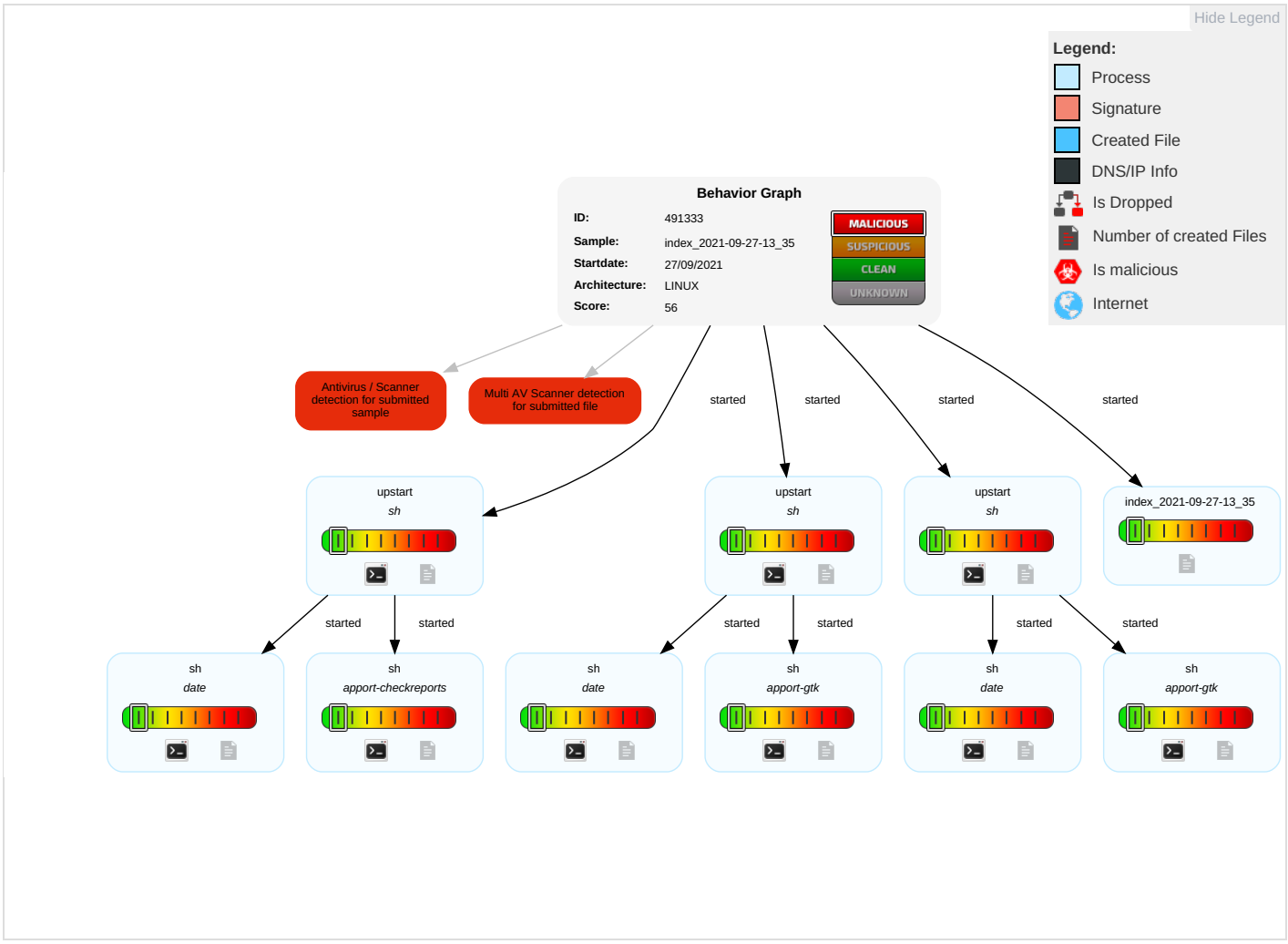
Mitre Att&ck Matrix

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	Direct Volume Access	OS Credential Dumping	Security Software Discovery 1 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

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
index_2021-09-27-13_35	41%	Metadefender		Browse
index_2021-09-27-13_35	75%	ReversingLabs	Linux.Trojan.Mirai	
index_2021-09-27-13_35	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

Runtime Messages

Command:	/tmp/index_2021-09-27-13_35
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):	4.689140449240036
Encrypted:	false
SSDEEP:	192:5Zn741jDzZI6W/f/i5tSLggsOu1CiE6SPIvhbM:Di2/f/+SEgviEhf
MD5:	B348B0AAB8C4900DAFD960395972EB0E
SHA1:	494BCA751DBA56B66A2ACF3934F977B5DF392160
SHA-256:	AE8313CC91BA2145FB9D0008BBD7D6850E939788CBEBA3230B7A5A23DA913E97
SHA-512:	6255F4B4FD0325F09A70BEDE7DFF79AD9CD6D0AC191104D0A0FC92F7D8FCB6A73A01D43A3398EECBF7A9F75692DD7A60603FAD431683F4871827F0AEB3C6A39
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Mon Sep 27 15:38:13 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 . 028a1000-02bf9000 rw-p 00000000 00:00 0 [heap]. 7f7531e3b000-7f7531fbc000 rw-p 00000000 00:00 0 . 7f7531fbc000-7f7531fd3000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f7531fd3000-7f75321d2000 ---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):	4.513446911970088
Encrypted:	false
SSDEEP:	768:PS0WZ8ppi/5/k/x/xz2He07PhlLy0M1neWwvrl2s7nAGN9LK4VfxL74SPrB:BWZ8y/5/k/x/WPhlLy0M1neWwvrl2s7R
MD5:	84DF76BC59442ED382EF38B0CB00E7AC
SHA1:	048EDFF7BC49CC3EB50EFBB3965A475E4160BA05
SHA-256:	26BD9E935C2EF68688AEC922C83036416905E87036DB1F0A1528D3895868E473
SHA-512:	54840F91D9525B3D4DBD467640EF1391C1E24306DA8D0790EDB9F6A495FF62295AB2D097C6F3340E60F1A6E17179DBBF40FB80581B4B4F0238592011D6B608D6
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Mon Sep 27 15:38:14 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 . 014f5000-01a16000 rw-p 00000000 00:00 0 [heap]. 7ff8cce36000-7ff8ccf36000 rw-p 00000000 00:00 0 . 7ff8ccf36000-7ff8ccf4d000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7ff8ccf4d000-7ff8cd14c000 ---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:	index_2021-09-27-13_35
File size:	135784
MD5:	59ce0baba11893f90527fc951ac69912
SHA1:	5857a7dd621c4c3ebb0b5a3bec915d409f70d39f
SHA256:	4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7
SHA512:	c5b12797b477e5e5964a78766bb40b1c0d9fdfb8eef1f9aee3df451e3441a40c61d325bf400ba51048811b68e1c70a95f15e4166b7a65a4eca0c624864328647

General

SSDEEP:	3072:phNlHuBafLeBtfCzpta8xlBIOdVo3/4sxLJ10xioP:p3lOYoaja8xzx/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	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x210f2	0x210f2	4.4337	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x92fd8	0.0000	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: index_2021-09-27-13_35 PID: 4666 Parent PID: 4595

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/tmp/index_2021-09-27-13_35
Arguments:	/usr/bin/qemu-mips /tmp/index_2021-09-27-13_35
File size:	135784 bytes
MD5 hash:	59ce0baba11893f90527fc951ac69912

File Activities

File Read

Analysis Process: upstart PID: 4682 Parent PID: 3310

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: 4682 Parent PID: 3310

General

Start time:	13:38:13
Start date:	27/09/2021
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: 4691 Parent PID: 4682

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4691 Parent PID: 4682

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4692 Parent PID: 4682

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 4692 Parent PID: 4682

General

Start time:	13:38:13
Start date:	27/09/2021
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: 4709 Parent PID: 3310

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: 4709 Parent PID: 3310

General

Start time:	13:38:13
Start date:	27/09/2021
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: 4713 Parent PID: 4709

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4713 Parent PID: 4709

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4719 Parent PID: 4709

General

Start time:	13:38:13
Start date:	27/09/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4719 Parent PID: 4709

General

Start time:	13:38:13
Start date:	27/09/2021
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: 4736 Parent PID: 3310

General

Start time:	13:38:14
Start date:	27/09/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: 4736 Parent PID: 3310

General

Start time:	13:38:14
Start date:	27/09/2021
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: 4737 Parent PID: 4736

General

Start time:	13:38:14
Start date:	27/09/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4737 Parent PID: 4736

General

Start time:	13:38:14
Start date:	27/09/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4738 Parent PID: 4736

General

Start time:	13:38:14
Start date:	27/09/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4738 Parent PID: 4736

General

Start time:	13:38:14
Start date:	27/09/2021
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