ID: 397473
Sample Name: s5caBnNA4u
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:22:50
Date: 25/04/2021
Version: 31.0.0 Emerald

Table of Contents

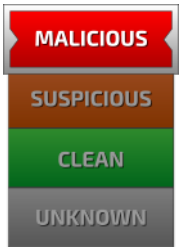
Analysis Report s5caBnNA4u

Overview

General Information

Sample Name:	s5caBnNA4u
Analysis ID:	397473
MD5:	fbe51695e97a45d.
SHA1:	1ed14334b5b717..
SHA256:	2e4506802aedea..
Infos:	

Detection

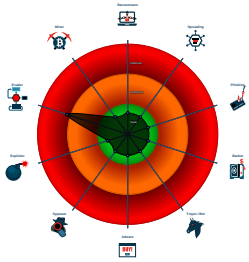


Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

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

Classification



Startup

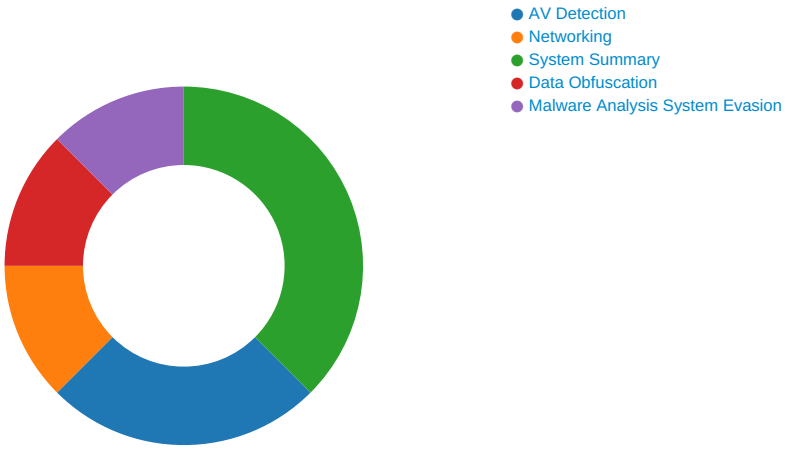
- **system is lnxubuntu1**
  - s5caBnNA4u (PID: 4557, Parent: 4497, MD5: fbe51695e97a45dc61967dc3241a37dc) Arguments: /usr/bin/qemu-mips /tmp/s5caBnNA4u
- upstart New Fork (PID: 4576, Parent: 3310)
  - sh (PID: 4576, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4577, Parent: 4576)
    - date (PID: 4577, Parent: 4576, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4588, Parent: 4576)
    - apport-checkreports (PID: 4588, Parent: 4576, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 4603, Parent: 3310)
  - sh (PID: 4603, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4604, Parent: 4603)
    - date (PID: 4604, Parent: 4603, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4605, Parent: 4603)
    - apport-gtk (PID: 4605, Parent: 4603, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- upstart New Fork (PID: 4630, Parent: 3310)
  - sh (PID: 4630, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
    - sh New Fork (PID: 4631, Parent: 4630)
    - date (PID: 4631, Parent: 4630, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4632, Parent: 4630)
    - apport-gtk (PID: 4632, Parent: 4630, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
s5caBnNA4u	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

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

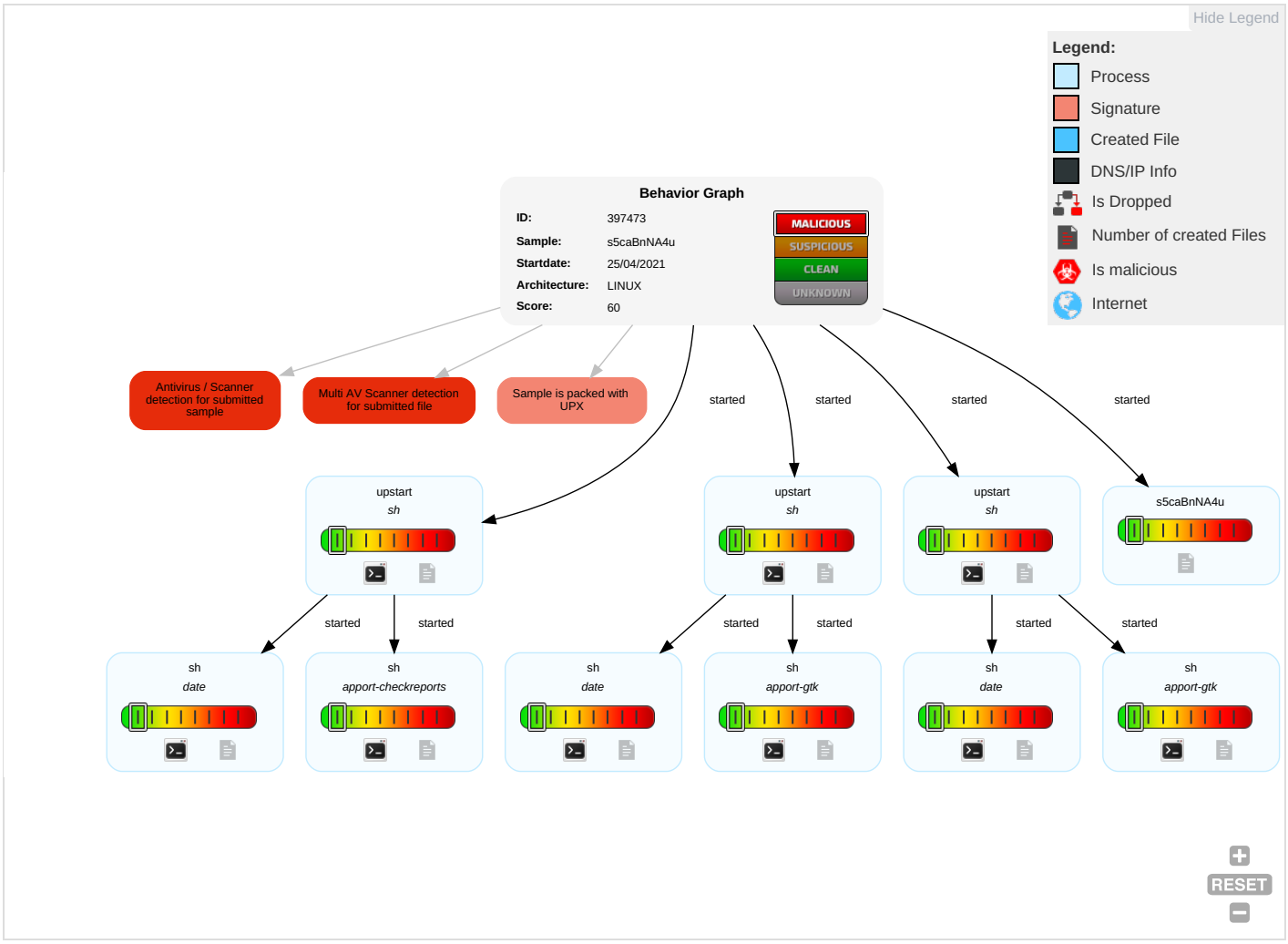
Data Obfuscation:

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
s5caBnNA4u	59%	Virustotal		Browse
s5caBnNA4u	42%	Metadefender		Browse
s5caBnNA4u	67%	ReversingLabs	Linux.Trojan.Mirai	
s5caBnNA4u	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:	397473
Start date:	25.04.2021
Start time:	21:22:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	s5caBnNA4u
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.lin@0/2@0/0

Runtime Messages

Command:	/tmp/s5caBnNA4u
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):	4.7158485336825695
Encrypted:	false
SSDEEP:	192:JB7G4JzQljNZz70l39ieHfUQQPEnTPIIhbM:JwhZ97KYPETy
MD5:	40A1A5B55A18219616F20BE0458A3DD1
SHA1:	5AAB90FDC0421EBE8EF25E4DD217AB1260CFA71F
SHA-256:	9BCB73A40FCA9C79520E48A899AAAE7ED5BB3E6DC9350FDF0B274692D95D9282
SHA-512:	F24F9633FFBDBC959A487A6F1DBF2E3691E67762AD2FA8821CE2C85BF10894AE417FE0ABC4F59C2F1C2CC60D1D45F5CA63927DEB89692DDA528186C4A3D709C
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Sun Apr 25 23:23:20 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 . 0165e000-019b7000 rw-p 00000000 00:00 0 [heap]. 7f9b81633000-7f9b817b4000 rw-p 00000000 00:00 0 . 7f9b817b4000-7f9b817cb000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f9b817cb000-7f9b819ca000 ---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):	4.511871922475535
Encrypted:	false
SSDEEP:	384:JK7mKCqo/9/H/b/betofAlekYrBv1xqqy2VHQkUKSIA0ECHQ:UC7/9/H/b/qtofiYrNy2VHQkUKSIA0m
MD5:	2DFF2AB1B16F00997F7389B6826BD397
SHA1:	31630730770ED8EDCAC0453359F7E3C937FF6D32
SHA-256:	CC03E0030631622ABED421CECE283D88545089D57DB9AC7C5A0B5F51B588215E
SHA-512:	08E3BA9778445D36931CE2F388EDFBDA67276D84215D8134B38515327D9B80FF9D324ACA3166176B4342ED6B9B45BA09CAAF622D4E1FDD6D26708A25265F634E
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Sun Apr 25 23:23:21 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 . 01252000-01773000 rw-p 00000000 00:00 0 [heap]. 7f83ed3ee000-7f83ed4ee000 rw-p 00000000 00:00 0 . 7f83ed4ee000-7f83ed505000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f83ed505000-7f83ed704000 ---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:	s5caBnNA4u
File size:	132876
MD5:	fbe51695e97a45dc61967dc3241a37dc
SHA1:	1ed14334b5b71783cd6ec14b8a704fe48e600cf0

General

SHA256:	2e4506802aedea2e6d53910dfb296323be6620ac08c4b799a879eace5923a7b6
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

No network behavior found

System Behavior

Analysis Process: s5caBnNA4u PID: 4557 Parent PID: 4497

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/tmp/s5caBnNA4u
Arguments:	/usr/bin/qemu-mips /tmp/s5caBnNA4u
File size:	132876 bytes
MD5 hash:	fbe51695e97a45dc61967dc3241a37dc

File Activities

File Read

Analysis Process: upstart PID: 4576 Parent PID: 3310

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4576 Parent PID: 3310

General

Start time:	21:23:20
Start date:	25/04/2021
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: 4577 Parent PID: 4576

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4577 Parent PID: 4576

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4588 Parent PID: 4576

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 4588 Parent PID: 4576

General

Start time:	21:23:20
Start date:	25/04/2021
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: 4603 Parent PID: 3310

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4603 Parent PID: 3310

General

Start time:	21:23:20
Start date:	25/04/2021
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: 4604 Parent PID: 4603

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4604 Parent PID: 4603

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4605 Parent PID: 4603

General

Start time:	21:23:20
Start date:	25/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4605 Parent PID: 4603

General

Start time:	21:23:20
Start date:	25/04/2021
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: 4630 Parent PID: 3310

General

Start time:	21:23:21
Start date:	25/04/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4630 Parent PID: 3310

General

Start time:	21:23:21
Start date:	25/04/2021
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: 4631 Parent PID: 4630

General

Start time:	21:23:21
Start date:	25/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4631 Parent PID: 4630

General

Start time:	21:23:21
Start date:	25/04/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4632 Parent PID: 4630

General

Start time:	21:23:21
Start date:	25/04/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4632 Parent PID: 4630

General

Start time:	21:23:21
Start date:	25/04/2021
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