



ID: 327181
Sample Name: bin.sh.1
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 00:10:39
Date: 05/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report bin.sh.1 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
System Behavior 9
Analysis Process: bin.sh.1 PID: 4568 Parent PID: 4519 9
General 9
File Activities 9
File Read 10
Analysis Process: upstart PID: 4581 Parent PID: 3310 10
General 10
Analysis Process: sh PID: 4581 Parent PID: 3310 10
General 10
File Activities 10
File Read 10
Analysis Process: sh PID: 4582 Parent PID: 4581 10
General 10
Analysis Process: date PID: 4582 Parent PID: 4581 10
General 10
File Activities 10
File Read 10
Analysis Process: sh PID: 4583 Parent PID: 4581 11
General 11

Analysis Process: apport-checkreports PID: 4583 Parent PID: 4581 11
General 11
File Activities 11
File Read 11
File Written 11
Directory Enumerated 11
Analysis Process: upstart PID: 4608 Parent PID: 3310 11
General 11
Analysis Process: sh PID: 4608 Parent PID: 3310 11
General 11
File Activities 11
File Read 11
Analysis Process: sh PID: 4609 Parent PID: 4608 12
General 12
Analysis Process: date PID: 4609 Parent PID: 4608 12
General 12
File Activities 12
File Read 12
Analysis Process: sh PID: 4610 Parent PID: 4608 12
General 12
Analysis Process: apport-gtk PID: 4610 Parent PID: 4608 12
General 12
File Activities 12
File Read 12
File Written 12
Directory Enumerated 13
Analysis Process: upstart PID: 4635 Parent PID: 3310 13
General 13
Analysis Process: sh PID: 4635 Parent PID: 3310 13
General 13
File Activities 13
File Read 13
Analysis Process: sh PID: 4636 Parent PID: 4635 13
General 13
Analysis Process: date PID: 4636 Parent PID: 4635 13
General 13
File Activities 13
File Read 13
Analysis Process: sh PID: 4637 Parent PID: 4635 14
General 14
Analysis Process: apport-gtk PID: 4637 Parent PID: 4635 14
General 14
File Activities 14
File Read 14
Directory Enumerated 14

Copyright null 2020

Analysis Report bin.sh.1

Overview

General Information

Sample Name:	bin.sh.1
Analysis ID:	327181
MD5:	a73ddd6ec22462..
SHA1:	ac6962542a4b23..
SHA256:	b5cf68c7cb5bb2d..

Detection

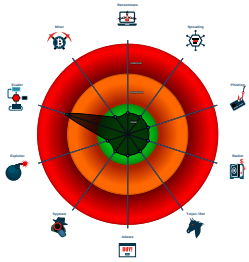


Score:	60
Range:	0 - 100
Whitelisted:	false

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**
  - bin.sh.1 (PID: 4568, Parent: 4519, MD5: a73ddd6ec22462db955439f665cad4e6) Arguments: /usr/bin/qemu-mips /tmp/bin.sh.1
- 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: 4610, Parent: 4608)
    - apport-gtk (PID: 4610, 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: 4636, Parent: 4635)
    - date (PID: 4636, Parent: 4635, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4637, Parent: 4635)
    - apport-gtk (PID: 4637, Parent: 4635, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- **cleanup**

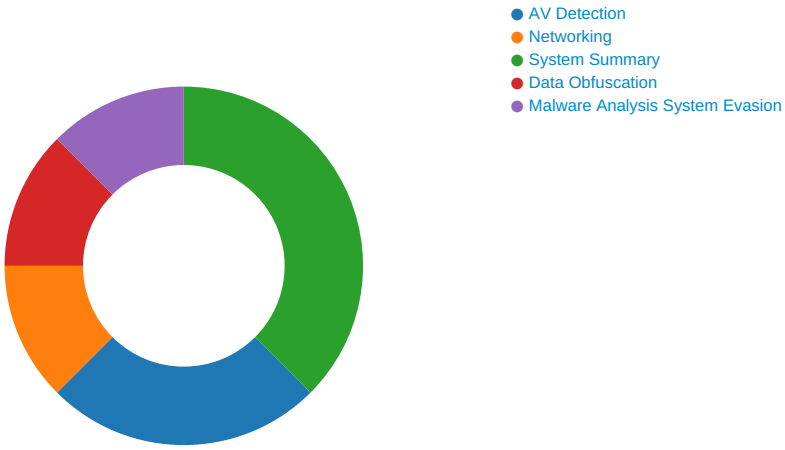
Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
bin.sh.1	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x206f8:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x20767:$s2: $Id: UPX • 0x20718:$s3: $Info: This file is packed with the UPX executable packer

Signature Overview

Copyright null 2020



Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Data Obfuscation:

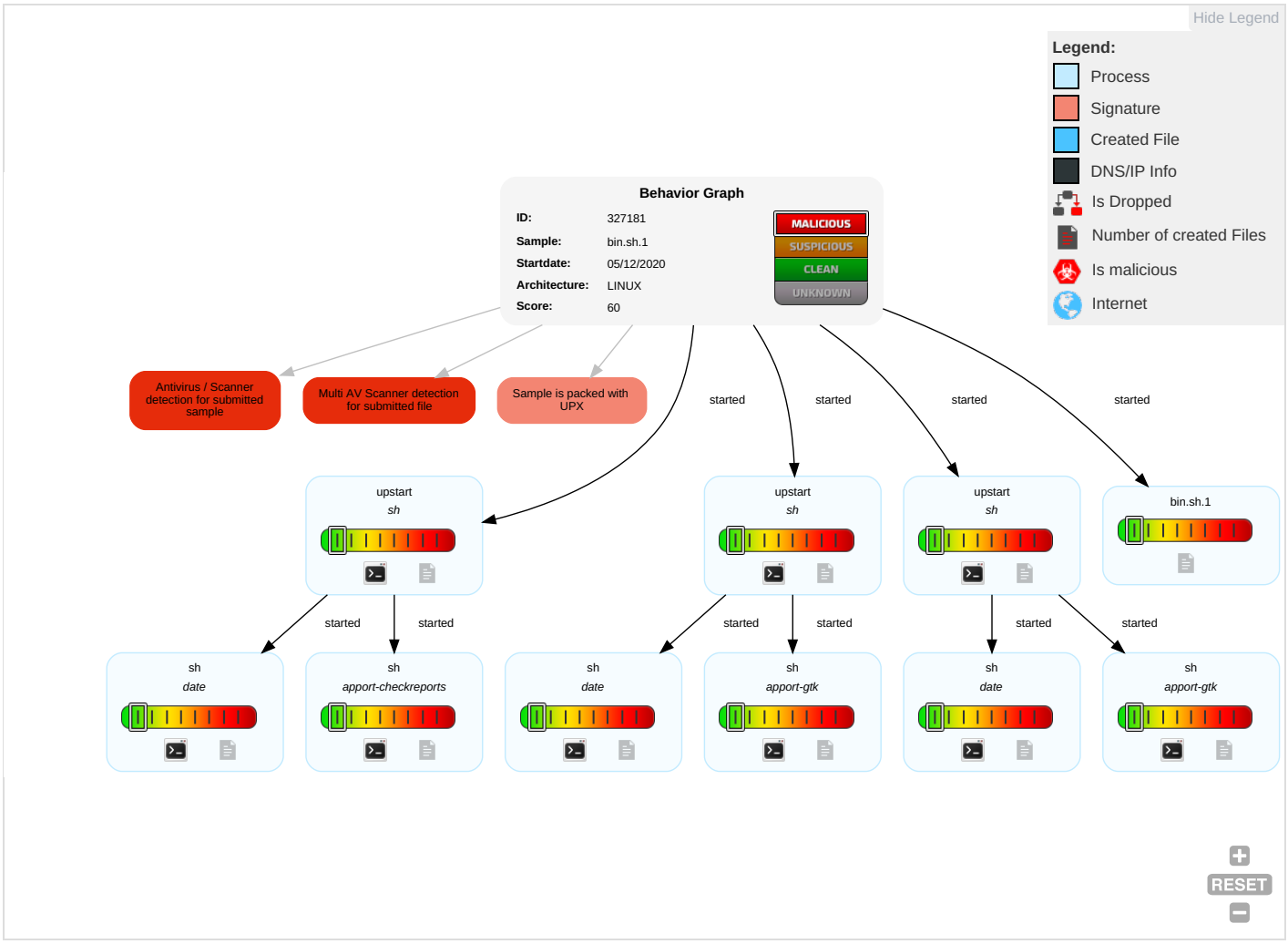


Sample is packed with UPX

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
bin.sh.1	64%	Virustotal		Browse
bin.sh.1	18%	Metadefender		Browse
bin.sh.1	59%	ReversingLabs	Linux.Trojan.Mirai	
bin.sh.1	100%	Avira	LINUX/Mirai.ccjqy	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Copyright null 2020

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	327181
Start date:	05.12.2020
Start time:	00:10:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bin.sh.1
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.lin1@0/2@0/0

Runtime Messages

Command:	/tmp/bin.sh.1
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

Copyright null 2020

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):	4.688033282283168
Encrypted:	false
SSDEEP:	192:4aXr+sr+ev0wEpGyT1LT4oHuupkpKmUEfIPl2hbM:Zr+sr+evJO1LT4oDW6EQ4
MD5:	235DBFF95A59A846E5373C3B1C66E608
SHA1:	F13A343E6225DCA43D5C1B93AFE4CDA51DEB42E7
SHA-256:	210509C9580F04055A9B8868C5C2E5FFE4EC0E22D7236A666B6B36B8552E1AC9
SHA-512:	1E9D5BD02DF001A81EB6340FC265CBB22C47E6CEF96C0237B75957432EEEB158A27F678445411EFAF1E12861ACA0BAF582F11852938407F44DCCC4ECA50D2A49
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Sat Dec 5 01:11:08 2020.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 . 02789000-02ae0000 rw-p 00000000 00:00 0 [heap]. 7f7a84d61000-7f7a84ee2000 rw-p 00000000 00:00 0 . 7f7a84ee2000-7f7a84ef9000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f7a84ef9000-7f7a850f8000 ---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):	4.5120674077760246
Encrypted:	false
SSDEEP:	384:7jcknsSSR4Fo3D/Z/g/5/7LneCArrLLzdSs1eOPz/zAcI+P+dzJNqAVbET7:PM/Z/g/5/+CArNSs1e8+dzJNqAVbo
MD5:	999C5A9227F2288110CC8791816D4CD2
SHA1:	F4525B7814BA6AEEC36401125D54635CA1617B6F
SHA-256:	A744B50BE7DF0F41AECDD66DEF80A973412331C19AFD55F3D6A34E6F814F6CDA
SHA-512:	7EA59F41817DB36C6CB5567808B7D5E1351B0EA9564D2C029EDE2B10CC9B1A6A122C95C291204E23C8B2AD28AF71F8F727B361C6382FA801493947EA15DF690
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Sat Dec 5 01:11:08 2020.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 . 026ec000-02c0d000 rw-p 00000000 00:00 0 [heap]. 7f5359719000-7f5359819000 rw-p 00000000 00:00 0 . 7f53598 19000-7f5359830000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f5359830000-7f5359a2f000 ---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):	7.813637944981102
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	bin.sh.1
File size:	135472
MD5:	a73ddd6ec22462db955439f665cad4e6
SHA1:	ac6962542a4b23ac13bddff22f8df9aeb702ef12
SHA256:	b5cf68c7cb5bb2d21d60bf6654926f61566d95bfd7c9f9e182d032f1da5b4605

General

SHA512:	92a52f68a7324c4d5876e1f7e2cb87d14b8604b057ceee2e537815568faa96abf576a22111c5c976eff72ab9015f1261b2331d4b4d711f4e62c8eb403c2377aa
SSDEEP:	3072:2glZ3FtCKXhkmHtZ9TEKzjfj/WMngyIfsJ0F7xPtoM:2IIKXhZtL7jOTyIG87Xl
File Content Preview:	.ELF.....B.x...4.....4. ...(.....@...@.....C...C.....*.*UPX!.X.....]....|.$..ELF.....@.`....4...p... ...(.....<...@.....[v.....H...`.t/._...dt.Q.....].M.....P.....

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:	0x420578
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	0x20fc2	0x20fc2	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x91f18	0x6	RW	0x10000		

Network Behavior

No network behavior found

System Behavior

Analysis Process: bin.sh.1 PID: 4568 Parent PID: 4519

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/tmp/bin.sh.1
Arguments:	/usr/bin/qemu-mips /tmp/bin.sh.1
File size:	135472 bytes
MD5 hash:	a73ddd6ec22462db955439f665cad4e6

File Activities

File Read

Analysis Process: upstart PID: 4581 Parent PID: 3310

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4581 Parent PID: 3310

General

Start time:	00:11:08
Start date:	05/12/2020
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:	00:11:08
Start date:	05/12/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4582 Parent PID: 4581

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Copyright null 2020

Analysis Process: sh PID: 4583 Parent PID: 4581

General

Start time:	00:11:08
Start date:	05/12/2020
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:	00:11:08
Start date:	05/12/2020
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:	00:11:08
Start date:	05/12/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4608 Parent PID: 3310

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Copyright null 2020

Analysis Process: sh PID: 4609 Parent PID: 4608

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4609 Parent PID: 4608

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4610 Parent PID: 4608

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4610 Parent PID: 4608

General

Start time:	00:11:08
Start date:	05/12/2020
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

Copyright null 2020

Directory Enumerated

Analysis Process: upstart PID: 4635 Parent PID: 3310

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4635 Parent PID: 3310

General

Start time:	00:11:08
Start date:	05/12/2020
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: 4636 Parent PID: 4635

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4636 Parent PID: 4635

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Copyright null 2020

Analysis Process: sh PID: 4637 Parent PID: 4635

General

Start time:	00:11:08
Start date:	05/12/2020
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4637 Parent PID: 4635

General

Start time:	00:11:08
Start date:	05/12/2020
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

Copyright Joe Security LLC 2020