



ID: 452455
Sample Name: 7EUcDDmmRE
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:36:52
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Linux Analysis Report 7EUcDDmmRE 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
General Information 4
Process Tree 4
Yara Overview 5
Jbx Signature Overview 5
AV Detection: 5
Data Obfuscation: 5
Mitre Att&ck Matrix 5
Malware Configuration 6
Behavior Graph 6
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 7
Contacted IPs 7
Runtime Messages 7
Joe Sandbox View / Context 7
IPs 7
Domains 7
ASN 7
JA3 Fingerprints 7
Dropped Files 7
Created / dropped Files 7
Static File Info 8
General 8
Static ELF Info 8
ELF header 8
Program Segments 9
Network Behavior 9
System Behavior 9
Analysis Process: 7EUcDDmmRE PID: 4588 Parent PID: 4518 9
General 9
File Activities 9
File Read 9
Analysis Process: upstart PID: 4607 Parent PID: 3310 9
General 9
Analysis Process: sh PID: 4607 Parent PID: 3310 10
General 10
File Activities 10
File Read 10
Analysis Process: sh PID: 4608 Parent PID: 4607 10
General 10
Analysis Process: date PID: 4608 Parent PID: 4607 10
General 10
File Activities 10
File Read 10
Analysis Process: sh PID: 4611 Parent PID: 4607 10
General 10
Analysis Process: apport-checkreports PID: 4611 Parent PID: 4607 11
General 11
File Activities 11
File Read 11
File Written 11
Directory Enumerated 11
Analysis Process: upstart PID: 4634 Parent PID: 3310 11
General 11
Analysis Process: sh PID: 4634 Parent PID: 3310 11
General 11
File Activities 11
File Read 11
Analysis Process: sh PID: 4642 Parent PID: 4634 11
General 11
Analysis Process: date PID: 4642 Parent PID: 4634 12
General 12
File Activities 12
File Read 12
Analysis Process: sh PID: 4644 Parent PID: 4634 12
General 12

Copyright Joe Security LLC 2021

Analysis Process: apport-gtk PID: 4644 Parent PID: 4634 12
General 12
File Activities 12
File Read 12
File Written 12
Directory Enumerated 12
Analysis Process: upstart PID: 4661 Parent PID: 3310 12
General 12
Analysis Process: sh PID: 4661 Parent PID: 3310 13
General 13
File Activities 13
File Read 13
Analysis Process: sh PID: 4662 Parent PID: 4661 13
General 13
Analysis Process: date PID: 4662 Parent PID: 4661 13
General 13
File Activities 13
File Read 13
Analysis Process: sh PID: 4663 Parent PID: 4661 13
General 13
Analysis Process: apport-gtk PID: 4663 Parent PID: 4661 14
General 14
File Activities 14
File Read 14
Directory Enumerated 14

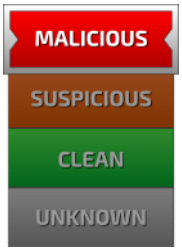
Linux Analysis Report 7EUcDDmmRE

Overview

General Information

Sample Name:	7EUcDDmmRE
Analysis ID:	452455
MD5:	ec4637f5d716f29..
SHA1:	b02af8052352d60.
SHA256:	737429af897437f..
Tags:	32 arm elf mirai
Infos:	

Detection

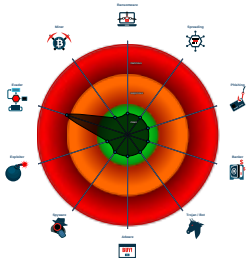


Score:	52
Range:	0 - 100
Whitelisted:	false

Signatures

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

Classification



Analysis Advice

- **Exit code information suggests that the sample terminated abnormally, try to lookup the sample's target architecture**
- **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:	452455
Start date:	22.07.2021
Start time:	11:36:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7EUcDDmmRE
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:	mal52.evad.lin@0/2@0/0

Process Tree

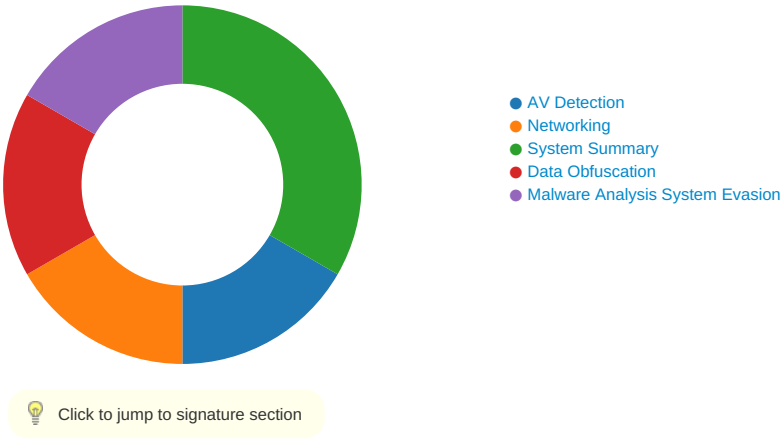
Copyright Joe Security LLC 2021

- **system is lnxubuntu1**
- 7EUcDDmmRE (PID: 4588, Parent: 4518, MD5: ec4637f5d716f29fd464b15e1c499a5a) Arguments: /usr/bin/qemu-arm /tmp/7EUcDDmmRE
- upstart New Fork (PID: 4607, Parent: 3310)
- sh (PID: 4607, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 4608, Parent: 4607)
  - date (PID: 4608, Parent: 4607, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 4611, Parent: 4607)
  - apport-checkreports (PID: 4611, Parent: 4607, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 4634, Parent: 3310)
- sh (PID: 4634, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 4642, Parent: 4634)
  - date (PID: 4642, Parent: 4634, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 4644, Parent: 4634)
  - apport-gtk (PID: 4644, Parent: 4634, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- upstart New Fork (PID: 4661, Parent: 3310)
- sh (PID: 4661, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 4662, Parent: 4661)
  - date (PID: 4662, Parent: 4661, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 4663, Parent: 4661)
  - apport-gtk (PID: 4663, Parent: 4661, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview



AV Detection:



Multi AV Scanner detection for submitted file

Data Obfuscation:



Sample is packed with UPX

Mitre Att&ck Matrix

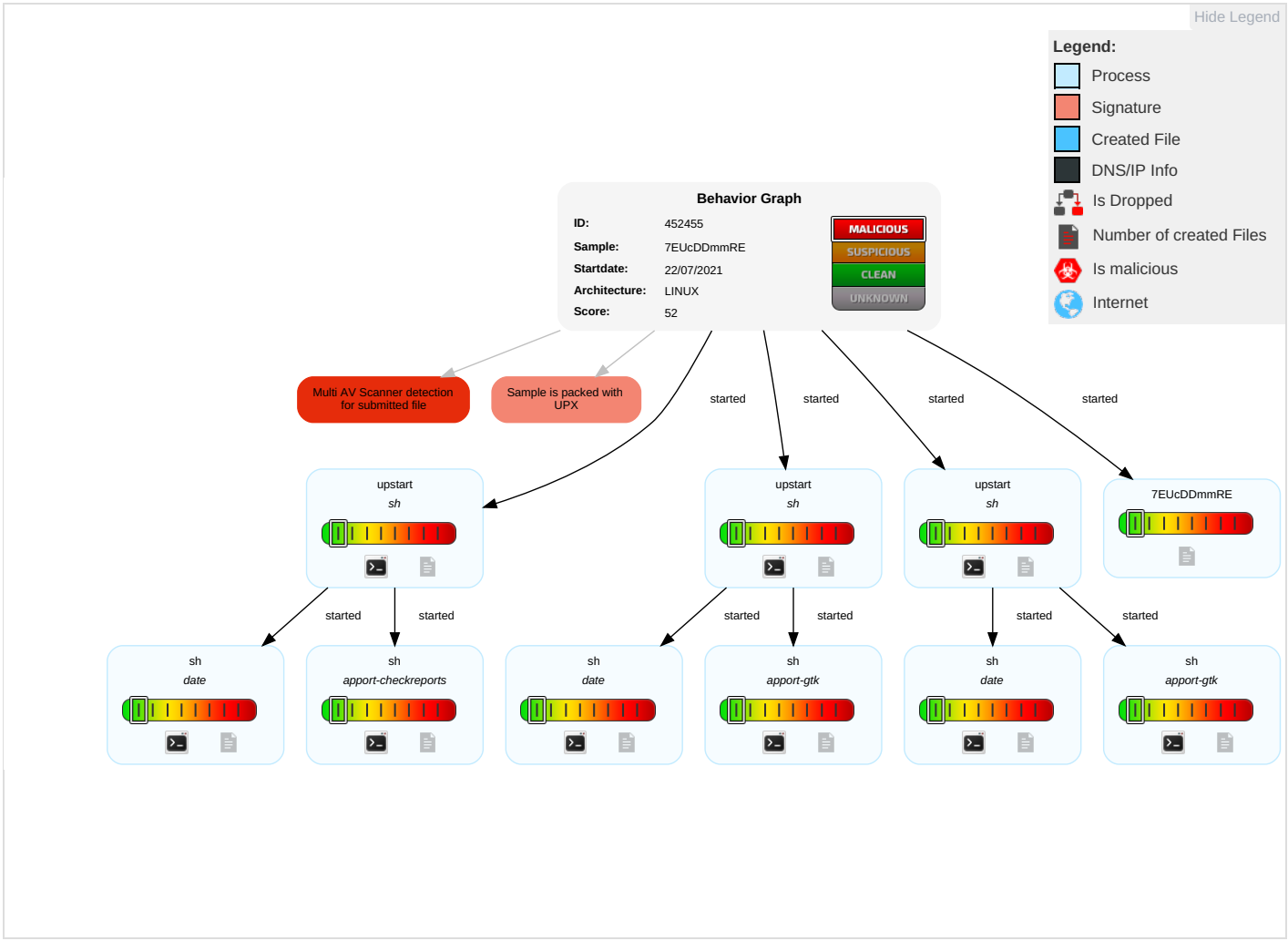
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated 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

Copyright Joe Security LLC 2021

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
7EUcDDmmRE	41%	Virustotal		Browse
7EUcDDmmRE	40%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Copyright Joe Security LLC 2021

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/7EUcDDmmRE
Exit Code:	139
Exit Code Info:	SIGSEGV (11) Segmentation fault invalid memory reference
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 11 (Segmentation fault) - 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):	4.687533212555657
Encrypted:	false

/var/crash/_usr_share_apport_apport-checkreports.1000.crash	
SSDEEP:	96:G8ck5w+6bplfn4RPfnw4AsKaRdfbvD+HPeKS+muJLOuPWEc+PI9d4YXrM:G/ARPfnw4AsDR8PeD+m2PWEc+PILhbM
MD5:	32D9EBEF40AA72B72A288B28D4B4DDA2
SHA1:	5F6D01001F61456508137C5B08C4750118258D48
SHA-256:	AA4FF4D879538ED4B8615C1D6F3A6EE3918EF8C47E9C836907E0C817032550A6
SHA-512:	5D84FDED4D780128BADC42F9159074E763F53F59FE0AAFBDBD9C66F96A988FC6DA8361F74B5C7918D08340F822A4885BDD88BA772F27CB3D45FC10CB399148B
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Thu Jul 22 13:37:25 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 . 00d47000-0109f000 rw-p 00000000 00:00 0 [heap]. 7fb3dfb6a000-7fb3dfceb000 rw-p 00000000 00:00 0 . 7fb3dfceb000-7fb3dfd02000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7fb3dfd02000-7fb3dff01000 ---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):	4.4957982542122705
Encrypted:	false
SSDEEP:	768:Ki2/4/l/a/J/YYp1a72U7wn4IwxP4MBJ+Cge://l/a/J/bU7FIwxP4MBJ+Cge
MD5:	0213F864224D719E30773752FB0B2F7F
SHA1:	E68B244F8658B304A95C3CEB75A64C3E670252BF
SHA-256:	24B8DB0263CBF2D8B22C1E772221538A06BE5E1E39C38A9068771D44EBEE2B9C
SHA-512:	EB2D76C08BDCEE0DB116EA71CF2893B804D46CF1E2B8FE3224F6B5F07A9B65FC93CE190F342A192AA5CB9920FF2344511977C10B9B4C0A6406F53B577FA1FE57
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Thu Jul 22 13:37:25 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 . 01699000-01bba000 rw-p 00000000 00:00 0 [heap]. 7f1d0b594000-7f1d0b694000 rw-p 00000000 00:00 0 . 7f1d0b694000-7f1d0b6ab000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f1d0b6ab000-7f1d0b8aa000 ---p 00017000 fc:00 2382

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.94626883299982
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	7EUcDDmmRE
File size:	29464
MD5:	ec4637f5d716f29fd464b15e1c499a5a
SHA1:	b02af8052352d60b686b3224192f132be747e331
SHA256:	737429af897437fc5315d8861d92502477a801bcd59526f10f30d78b96d88b0a
SHA512:	378d232e9e4c5834bfb4ce7f9117d83a90f4fcc7abe3d98c58eed05622e54c78e4d71a4e68502e735f1301c1b4b31b9afa8be45004eb877ab4f5fd59bf69be27
SSDEEP:	768:vusHfRavjynNKnjFcZIhQzhKMXgj9q3UEL7v:HRwynNIOQQ1KMwiL7
File Content Preview:	.ELF.....(.....4.....4. ...(.....q...q.....'..'..'.....Q.td.....OUPX!.....S.....?.E.h;....#..$..1)....tX....K.....E...%.FF..7.|.l]Z... ._.....+.. .

Static ELF Info

ELF header

Class:	ELF32

ELF header

Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0xe000
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
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	0x8000	0x8000	0x71ed	0x71ed	4.0285	0x5	R E	0x8000		
LOAD	0x2780	0x22780	0x22780	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

No network behavior found

System Behavior

Analysis Process: 7EUcDDmmRE PID: 4588 Parent PID: 4518

General

Start time:	11:37:24
Start date:	22/07/2021
Path:	/tmp/7EUcDDmmRE
Arguments:	/usr/bin/qemu-arm /tmp/7EUcDDmmRE
File size:	29464 bytes
MD5 hash:	ec4637f5d716f29fd464b15e1c499a5a

File Activities

File Read

Analysis Process: upstart PID: 4607 Parent PID: 3310

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/sbin/upstart

Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4607 Parent PID: 3310

General

Start time:	11:37:25
Start date:	22/07/2021
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: 4608 Parent PID: 4607

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4608 Parent PID: 4607

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4611 Parent PID: 4607

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 4611 Parent PID: 4607

General

Start time:	11:37:25
Start date:	22/07/2021
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: 4634 Parent PID: 3310

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4634 Parent PID: 3310

General

Start time:	11:37:25
Start date:	22/07/2021
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: 4642 Parent PID: 4634

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a

Copyright Joe Security LLC 2021

File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4642 Parent PID: 4634

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4644 Parent PID: 4634

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4644 Parent PID: 4634

General

Start time:	11:37:25
Start date:	22/07/2021
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: 4661 Parent PID: 3310

General

Start time:	11:37:25
Start date:	22/07/2021

Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4661 Parent PID: 3310

General

Start time:	11:37:25
Start date:	22/07/2021
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: 4662 Parent PID: 4661

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4662 Parent PID: 4661

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: 4663 Parent PID: 4661

General

Start time:	11:37:25
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes

Copyright Joe Security LLC 2021

MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4663 Parent PID: 4661

General

Start time:	11:37:25
Start date:	22/07/2021
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

Copyright Joe Security LLC 2021