ID: 452439
Sample Name: z0FwvGSnDF
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:03:45
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

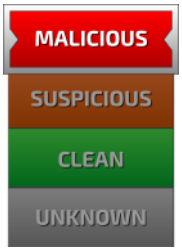
Linux Analysis Report z0FwvGSnDF

Overview

General Information

Sample Name:	z0FwvGSnDF
Analysis ID:	452439
MD5:	dafbf75b66b11d7..
SHA1:	d1736cc4d7efab8..
SHA256:	a524c003fb6dda1..
Tags:	32 elf mirai motorola
Infos:	

Detection

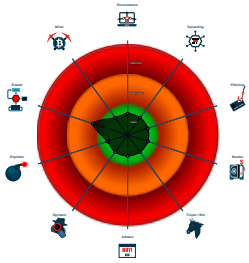


Score:	48
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Sample has stripped symbol table
- 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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452439
Start date:	22.07.2021
Start time:	11:03:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	z0FwvGSnDF
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:	mal48.lin@0/2@0/0

Process Tree

- **system is lnxubuntu1**
  - z0FwvGSnDF (PID: 4573, Parent: 4498, MD5: dafbf75b66b11d7d3b2dcd284c8ac302) Arguments: /usr/bin/qemu-m68k /tmp/z0FwvGSnDF
- 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: 4605, Parent: 4587)
    - apport-checkreports (PID: 4605, 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: 4618, Parent: 4614)
    - apport-gtk (PID: 4618, 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: 4642, Parent: 4641)
    - date (PID: 4642, Parent: 4641, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
    - sh New Fork (PID: 4645, Parent: 4641)
    - apport-gtk (PID: 4645, Parent: 4641, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

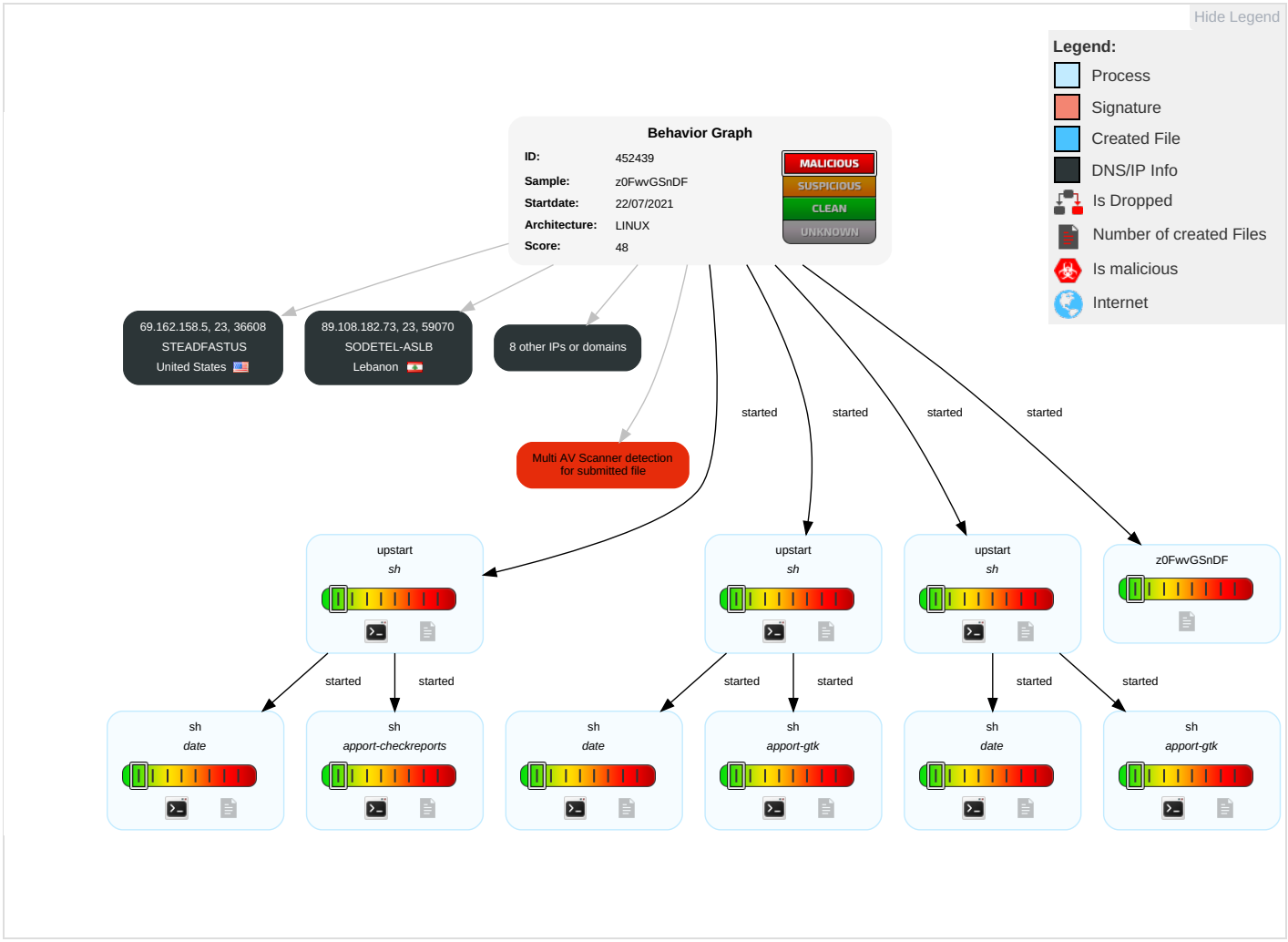
Mitre Att&ck Matrix

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	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
z0FwvGSnDF	52%	Virustotal		Browse
z0FwvGSnDF	54%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
27.207.129.233	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
112.95.114.170	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
121.134.140.247	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
62.101.96.107	unknown	Italy		12874	FASTWEBIT	false
89.108.182.73	unknown	Lebanon		31126	SODETEL-ASLB	false
212.64.174.180	unknown	Spain		12540	IDECNET-ASES	false
218.3.209.122	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
193.204.194.25	unknown	Italy		137	ASGARRConsortiumGARREU	false
116.234.228.208	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
69.162.158.5	unknown	United States		32748	STEADFASTUS	false

Runtime Messages

Command:	/tmp/z0FwvGSnDF
Exit Code:	132
Exit Code Info:	SIGILL (4) Illegal Instruction
Killed:	False
Standard Output:	
Standard Error:	qemu: uncaught target signal 4 (Illegal instruction) - core dumped

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	D1dU3jQ1Il	Get hash	malicious	Browse	• 183.188.114.224
	sDwNKSpuhB	Get hash	malicious	Browse	• 118.80.35.209
	A7X93JRxhp	Get hash	malicious	Browse	• 112.252.160.31
	8ZJ0cPowTy	Get hash	malicious	Browse	• 42.233.218.60
	92CRMNlBq8	Get hash	malicious	Browse	• 112.252.19.82
	XuQRPW44hi	Get hash	malicious	Browse	• 119.115.153.116

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Taf5zLti30	Get hash	malicious	Browse	• 171.38.232.41
	LyxN1ckWTW	Get hash	malicious	Browse	• 171.124.229.89
	U1R7Ed7940	Get hash	malicious	Browse	• 112.87.49.6
	dMTlC3Kf9l	Get hash	malicious	Browse	• 27.203.225.122
	GEso3CniSk	Get hash	malicious	Browse	• 122.140.177.221
	bPAMfuy9oa	Get hash	malicious	Browse	• 222.139.186.139
	U4r9W64doy	Get hash	malicious	Browse	• 113.6.132.80
	kb5IbEJU8c	Get hash	malicious	Browse	• 58.245.48.175
	CefN2XNyFi	Get hash	malicious	Browse	• 1.26.211.73
	7OAzOUL9cd	Get hash	malicious	Browse	• 123.131.65.248
	g516PzRL2Z	Get hash	malicious	Browse	• 175.163.76.171
	MD5OxTSc6i	Get hash	malicious	Browse	• 110.7.174.181
	Qka3fi8NpL	Get hash	malicious	Browse	• 119.27.114.19
	Xr3hmBQcmw	Get hash	malicious	Browse	• 175.170.137.64
KIXS-AS-KRKoreaTelecomKR	D1dU3jQ1Il	Get hash	malicious	Browse	• 218.158.241.237
	RsEvjl1iTt.exe	Get hash	malicious	Browse	• 121.136.102.4
	A7X93JRxhp	Get hash	malicious	Browse	• 125.137.150.28
	8ZJ0cPowTy	Get hash	malicious	Browse	• 119.215.188.3
	92CRMNlBq8	Get hash	malicious	Browse	• 183.126.251.85
	XuQRPW44hi	Get hash	malicious	Browse	• 121.170.47.64
	Taf5zLti30	Get hash	malicious	Browse	• 175.198.110.50
	5qpsqg7U0G	Get hash	malicious	Browse	• 175.239.252.125
	U5q75RGCmQ	Get hash	malicious	Browse	• 222.96.223.234
	oEF7GAiRIg	Get hash	malicious	Browse	• 121.145.187.107
	GEso3CniSk	Get hash	malicious	Browse	• 121.177.185.16
	BTNNG17tlh	Get hash	malicious	Browse	• 121.152.147.6
	bPAMfuy9oa	Get hash	malicious	Browse	• 121.177.185.53
	apep.mips	Get hash	malicious	Browse	• 121.170.84.41
	CefN2XNyFi	Get hash	malicious	Browse	• 119.193.74.164
	7OAzOUL9cd	Get hash	malicious	Browse	• 118.41.209.66
	MD5OxTSc6i	Get hash	malicious	Browse	• 61.85.109.214
	c51w5YSYdO	Get hash	malicious	Browse	• 125.153.59.17
	Xr3hmBQcmw	Get hash	malicious	Browse	• 112.174.230.242
	xjYvqOne1t	Get hash	malicious	Browse	• 183.126.2.191
CNCGROUP-SZChinaUnicomShenzennetworkCN	CGjf615z6v	Get hash	malicious	Browse	• 27.38.50.188
	yZEHOt8K7X	Get hash	malicious	Browse	• 120.87.46.204
	mssecsvr.exe	Get hash	malicious	Browse	• 58.251.111.21
	http://www.car388.com	Get hash	malicious	Browse	• 58.251.100.24
	http://https://u2867613.ct.sendgrid.net/ls/click?upn=xIoWet-2BTMg-2BVfl4m7Gz858a6bYE3yZGH61RmRbvDHYhDUUyAr1Khjkxjj-2BCUfZyREJKkLWm9kXM9xf2kpkPym7RRw-2FwPrffbBsg-2F9xfKVDnOmgo93gbmBWdQlqyAyP6o2T8m_UI-2Fa1HdcsOvWi0gT08Rm2AqxEWew-2BvQc9v-2FOJ0CFs-2Fqmzwsz0zZu1Q-2BhEiFDm76OxMI40TkUvAXI0PiE1M2-2FS3oBYErkDgrtvY8yQsueuZcmX1DOoK-2FGmjPfEq0WBdYkjBYItiWl4s0ifjNMViDKhl9pbY0wredclLKDY7HERPktB19FV8A6-2BUXfbzMfngXRV255yqgwGHIOt9NkZc15pe89ff-2FrtjvpWWMIjahF0XA-3D	Get hash	malicious	Browse	• 123.58.36.176
	JWZztRr04.exe	Get hash	malicious	Browse	• 163.177.90.125
	QQ_9.0.1.23161_setup.exe	Get hash	malicious	Browse	• 163.177.93.156
	N6T1bWei3a.apk	Get hash	malicious	Browse	• 112.90.78.173
	qq9.0.0.exe	Get hash	malicious	Browse	• 163.177.93.156
	www.777pan.cc/file-111542.html	Get hash	malicious	Browse	• 58.251.100.24

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):	4.684276917760678
Encrypted:	false
SSDEEP:	192:FbsJrszJG+PFNL0aM3AhWAFRAWHzEimaKPIihbM:A6FNLBzEie2
MD5:	C822B83B52268F71E07FEBF2368BA15A
SHA1:	A845FE0FC7EC37F3662169C187E224D5F38D34A6
SHA-256:	8541268C17C8D1B3DDABA809D1973D305AD7C9112FB35C81964116C974514C39
SHA-512:	CE35DB6B750C0FA8BEA8215803AEB39E077973912C21DD9AFA9BE1260783407048417FF1DEE9F4DADD2A207927B7C968EFA0B83BFA7A8ABBBCA132E4D26C0D5F
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Thu Jul 22 13:04:20 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 . 0177c000-01ad4000 rw-p 00000000 00:00 0 [heap]. 7f4414cad000-7f4414e2e000 rw-p 00000000 00:00 0 . 7f4414e2e000-7f4414e45000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7f4414e45000-7f4415044000 ---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):	4.499763637776248
Encrypted:	false
SSDEEP:	768:Jj/w9/Z///f/QNgrZaqGqdL/k7NA3GcA3l:JjC/Z///f/3aqGqdL/k7NA3GcA3l
MD5:	DB4D1B1AEF13086C174248ACC2C16F6F
SHA1:	F0F004B5AAC395755FF748005007C3B7F8091A67
SHA-256:	3C4F544F4DF6EC6356934C0B8FBE69922068624C67839A5393D656350D809F1C
SHA-512:	ACD9926D82775610EF381219F3933830F169E9DD8BE60F738A9A77FEEB8668A1957A24AC1715B01CC0A7B775EC591A426CF3369F826E7F89A267430EB3F0D39D
Malicious:	false
Reputation:	low
Preview:	ProblemType: Crash.Date: Thu Jul 22 13:04:20 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 . 01018000-0153c000 rw-p 00000000 00:00 0 [heap]. 7fb2b3f7e000-7fb2b407e000 rw-p 00000000 00:00 0 . 7fb2b407e000-7fb2b4095000 r-xp 00000000 fc:00 2382 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1. 7fb2b4095000-7fb2b4294000 ---p 00017000 fc:00 2382

Static File Info

General

File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.212564047873712
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	z0FwvGSnDF
File size:	53056
MD5:	dafbf75b66b11d7d3b2dcd284c8ac302
SHA1:	d1736cc4d7efab8522907550ae0ad5c2e52b296e
SHA256:	a524c003fb6dda1f77eda693accef4fff0a0d9fbe7bb0dcfeaa319e526367258

General

SHA512:	808496017ae6c062911902ca70339272371723cdb979f7039cf13e46869557b33e3a9017f9738f7aaa6b35147eb09622195c564d599816be4e34848c7daf4022
SSDEEP:	768:mLGOe2kf9e9X9nbermI7vc59QPQs5gFHviPuzWeHXpi2UJTpDnH638gZ:mL/4f8F1ef0YgFvimzpZi2UJJnHY8w
File Content Preview:	.ELF.....D...4.....4. ...(.....p..... .dt.Q.....NV..a....da.....N^NuNV..J9...pf>"y.... QJ.g.X.#.....N."y.... QJ.f.A.....J.g.Hy....N.X.....pN^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	52656
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0xc5d6	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000c67e	0xc67e	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000c68c	0xc68c	0x56e	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x8000ec00	0xcc00	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8000ec08	0xcc08	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8000ec14	0xcc14	0x15c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x8000ed70	0xcd70	0x23c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xcd70	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x80000000	0x80000000	0xcbfa	0xcbfa	4.2323	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0xcc00	0x8000ec00	0x8000ec00	0x170	0x3ac	0.2775	0x6	RW	0x2000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-11:04:21.807137	ICMP	399	ICMP Destination Unreachable Host Unreachable			192.12.76.3	192.168.2.20

TCP Packets

ICMP Packets

System Behavior

Analysis Process: z0FwvGSnDF PID: 4573 Parent PID: 4498

General

Start time:	11:04:19
Start date:	22/07/2021
Path:	/tmp/z0FwvGSnDF
Arguments:	/usr/bin/qemu-m68k /tmp/z0FwvGSnDF
File size:	53056 bytes
MD5 hash:	dafbf75b66b11d7d3b2dcd284c8ac302

File Activities

File Read

Analysis Process: upstart PID: 4587 Parent PID: 3310

General

Start time:	11:04:20
Start date:	22/07/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4587 Parent PID: 3310

General

Start time:	11:04:20
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: 4588 Parent PID: 4587

General

Start time:	11:04:20
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4588 Parent PID: 4587

General

Start time:	11:04:20
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: 4605 Parent PID: 4587

General

Start time:	11:04:20
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: 4605 Parent PID: 4587

General

Start time:	11:04:20
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: 4614 Parent PID: 3310

General

Start time:	11:04:20
Start date:	22/07/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4614 Parent PID: 3310

General

Start time:	11:04:20
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: 4615 Parent PID: 4614

General

Start time:	11:04:20
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4615 Parent PID: 4614

General

Start time:	11:04:20
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: 4618 Parent PID: 4614

General

Start time:	11:04:20

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

Analysis Process: apport-gtk PID: 4618 Parent PID: 4614

General

Start time:	11:04:20
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: 4641 Parent PID: 3310

General

Start time:	11:04:20
Start date:	22/07/2021
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	00000000000000000000000000000000

Analysis Process: sh PID: 4641 Parent PID: 3310

General

Start time:	11:04:20
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: 4641

General

Start time:	11:04:20
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: 4642 Parent PID: 4641

General

Start time:	11:04:20
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: 4645 Parent PID: 4641

General

Start time:	11:04:20
Start date:	22/07/2021
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: 4645 Parent PID: 4641

General

Start time:	11:04:20
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