ID: 511554
Sample Name: csB31kWt10
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:39:11
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

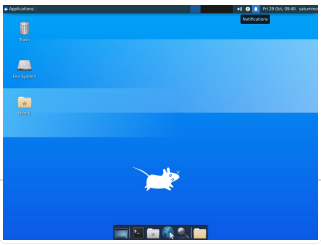
Linux Analysis Report csB31kWt10

Overview

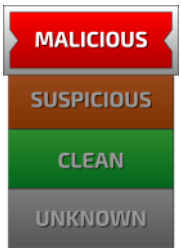
General Information

Sample Name:	csB31kWt10
Analysis ID:	511554
MD5:	df1ed6e73703ce0.
SHA1:	4b3444321f460d0.
SHA256:	1d41b0a9c3b189..
Tags:	32 elf mips mirai
Infos:	

Most interesting Screenshot:



Detection

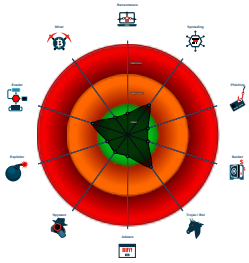


Score:	48
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample tries to kill a process (SIGK…

Classification



Analysis Advice

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

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	511554
Start date:	29.10.2021
Start time:	09:39:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	csB31kWt10
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal48.lin@0/4@0/0

Process Tree

- **system is lnxubuntu20**
  - csB31kWt10 (PID: 5241, Parent: 5119, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/csB31kWt10
    - csB31kWt10 New Fork (PID: 5244, Parent: 5241)
      - csB31kWt10 New Fork (PID: 5246, Parent: 5244)
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior
- Malware Analysis System Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

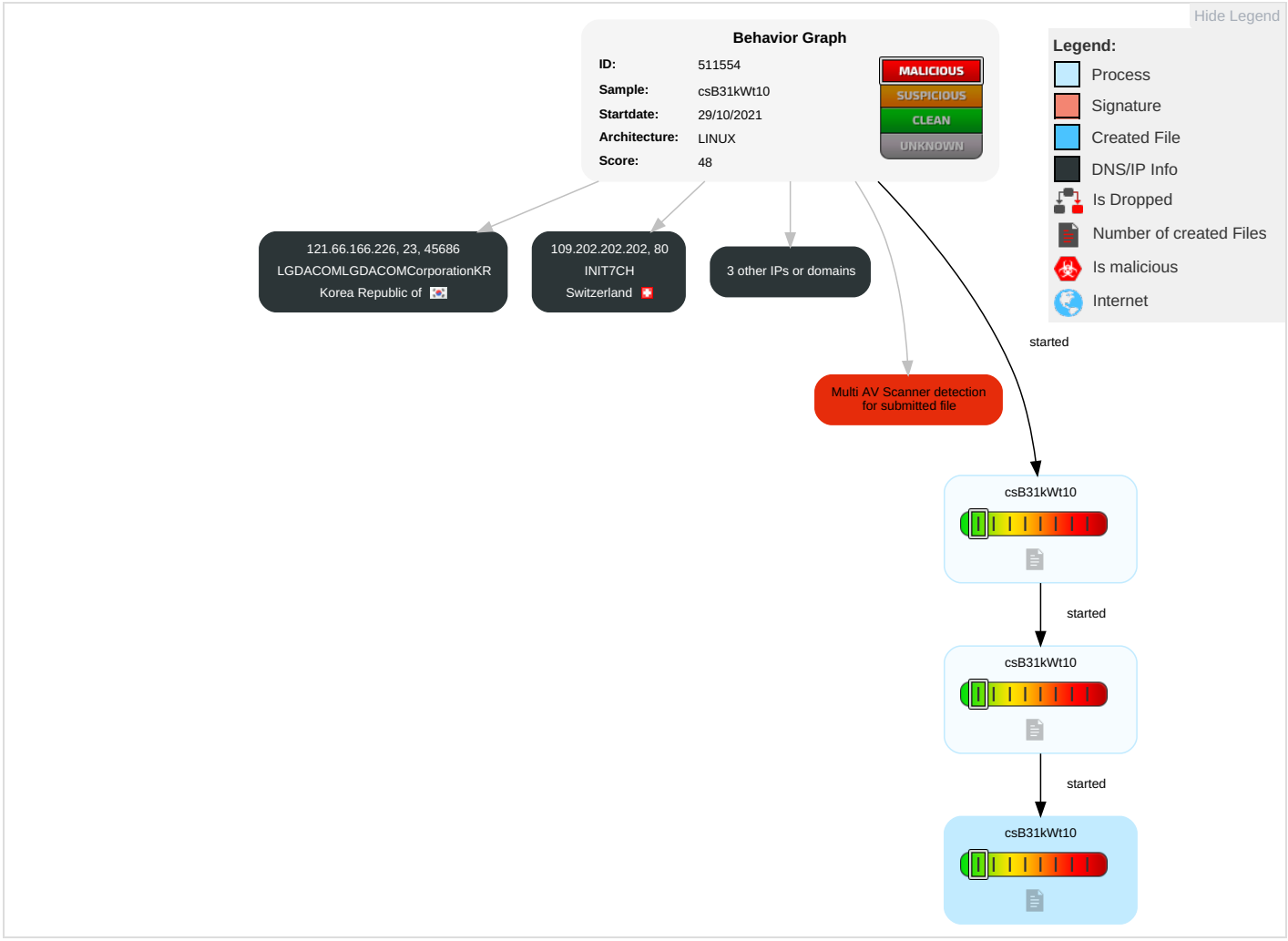
Mitre Att&ck Matrix

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 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

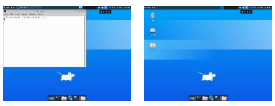
Behavior Graph

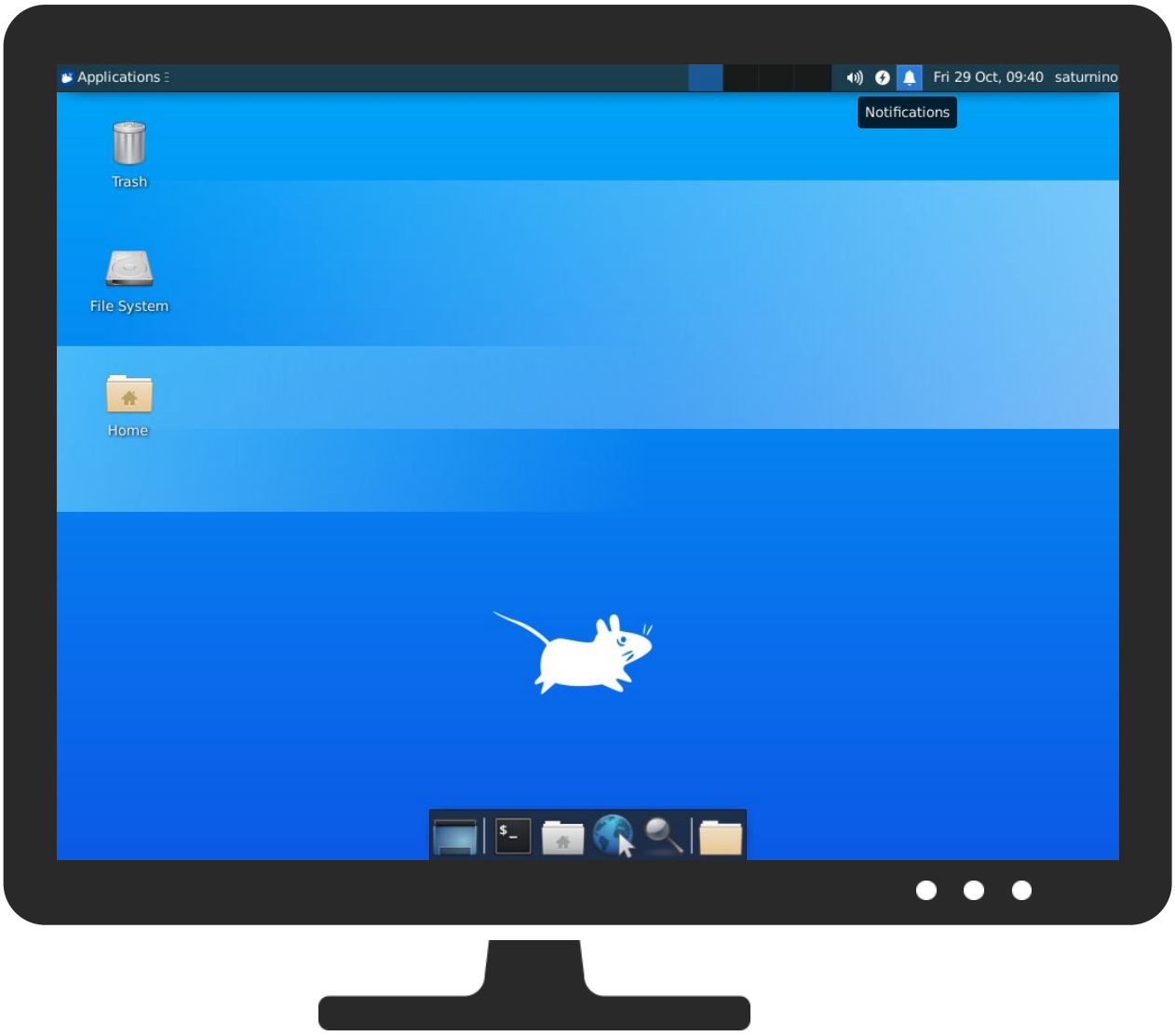


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
csB31kWt10	23%	Virustotal		Browse
csB31kWt10	25%	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
121.66.166.226	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
45.95.169.120	unknown	Croatia (LOCAL Name: Hrvatska)		42864	GIGANET-HUGigaNetInternetServiceProviderCoHU	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Runtime Messages

Command:	/tmp/csB31kWt10
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.95.169.120	QWg2NTuodY	Get hash	malicious	Browse	
	SL92Sz9pl2	Get hash	malicious	Browse	
	YpKL484IG5	Get hash	malicious	Browse	
	Y4W4j5QIqD	Get hash	malicious	Browse	
	1TnmkstVG8	Get hash	malicious	Browse	
	iksM5QEg2j	Get hash	malicious	Browse	
109.202.202.202	QWg2NTuodY	Get hash	malicious	Browse	
	6VLeGqFkPS	Get hash	malicious	Browse	
	DL5blLw1ly	Get hash	malicious	Browse	
	SL92Sz9pl2	Get hash	malicious	Browse	
	YpKL484IG5	Get hash	malicious	Browse	
	Y4W4j5QIqD	Get hash	malicious	Browse	
	1TnmkstVG8	Get hash	malicious	Browse	
	iksM5QEg2j	Get hash	malicious	Browse	
	lGJEkz80oe	Get hash	malicious	Browse	
	roV7kGaVr1	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	
	uPOWBxniTA	Get hash	malicious	Browse	
	qy5unieRgR	Get hash	malicious	Browse	
	sAzPpn6mKZ	Get hash	malicious	Browse	
	AxadDC89j9	Get hash	malicious	Browse	
	ZErnXU2XR1	Get hash	malicious	Browse	
	sTHJvS5LPJ	Get hash	malicious	Browse	
	THzHjYQ4z6	Get hash	malicious	Browse	
	jC0B6sMh1d	Get hash	malicious	Browse	
	JoLmvC65B7	Get hash	malicious	Browse	
91.189.91.43	QWg2NTuodY	Get hash	malicious	Browse	
	6VLeGqFkPS	Get hash	malicious	Browse	
	DL5blLw1ly	Get hash	malicious	Browse	
	SL92Sz9pl2	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	YpKL484IG5	Get hash	malicious	Browse	
	Y4W4j5QIqD	Get hash	malicious	Browse	
	1TnmkstVG8	Get hash	malicious	Browse	
	iksM5QEg2j	Get hash	malicious	Browse	
	lGJEkz80oe	Get hash	malicious	Browse	
	roV7kGaVr1	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	
	uPOWBxniTA	Get hash	malicious	Browse	
	qy5unieRgR	Get hash	malicious	Browse	
	sAzPpn6mKZ	Get hash	malicious	Browse	
	AxadDC89j9	Get hash	malicious	Browse	
	ZErnXU2XR1	Get hash	malicious	Browse	
	sTHJvS5LPJ	Get hash	malicious	Browse	
	THzHjYQ4z6	Get hash	malicious	Browse	
	jC0B6sMh1d	Get hash	malicious	Browse	
	JoLmvC65B7	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GIGANET-HUGigaNetInternetServiceProviderCoHU	QWg2NTuodY	Get hash	malicious	Browse	• 45.95.169.120
	SL92Sz9pl2	Get hash	malicious	Browse	• 45.95.169.120
	YpKL484IG5	Get hash	malicious	Browse	• 45.95.169.120
	Y4W4j5QIqD	Get hash	malicious	Browse	• 45.95.169.120
	1TnmkstVG8	Get hash	malicious	Browse	• 45.95.169.120
	iksM5QEg2j	Get hash	malicious	Browse	• 45.95.169.120
	RicwIfIHLK	Get hash	malicious	Browse	• 45.95.169.115
	aIY7AxjUMc	Get hash	malicious	Browse	• 45.95.169.115
	DtJmFQxtNC	Get hash	malicious	Browse	• 45.95.169.115
	Wm4CzOCmNY	Get hash	malicious	Browse	• 45.95.169.115
	vunWUzXJvC	Get hash	malicious	Browse	• 45.95.169.115
	52xhBHy9Wz	Get hash	malicious	Browse	• 45.95.169.115
	YGvwG0iCDE	Get hash	malicious	Browse	• 45.95.169.115
	dbd5O0RUTq	Get hash	malicious	Browse	• 45.95.169.115
	fHVDVj0pzO	Get hash	malicious	Browse	• 45.95.169.115
	eZPk7Fg5w7	Get hash	malicious	Browse	• 45.95.169.115
	ph5PjoFBpj	Get hash	malicious	Browse	• 45.95.169.115
	xugAk5haat	Get hash	malicious	Browse	• 45.95.169.115
	0jEbWQtzs0	Get hash	malicious	Browse	• 45.95.169.115
	8g3tc5SWwB	Get hash	malicious	Browse	• 92.52.211.220
LGDACOMLGDACOMCorporationKR	JUZVpUSH0W	Get hash	malicious	Browse	• 210.219.31.15
	2pPPNW1XSo	Get hash	malicious	Browse	• 118.128.83.148
	SL92Sz9pl2	Get hash	malicious	Browse	• 1.217.238.242
	oCN3rc0FzJ.exe	Get hash	malicious	Browse	• 115.88.24.202
	BsNj9o1U0P.exe	Get hash	malicious	Browse	• 106.241.4.103
	sMoq8eQy9U.exe	Get hash	malicious	Browse	• 211.119.84.112
	pSY2vVxk86.exe	Get hash	malicious	Browse	• 210.92.250.133
	KXSHtkFjm1.exe	Get hash	malicious	Browse	• 115.91.217.231
	e4eukUb6d1.exe	Get hash	malicious	Browse	• 115.88.24.202
	rdvL5Vuyg7.exe	Get hash	malicious	Browse	• 211.40.39.251
	9JVjZ8tdvF.exe	Get hash	malicious	Browse	• 210.92.250.133
	RgHOcm1miq.exe	Get hash	malicious	Browse	• 61.36.14.230
	ECOC8S2pt7.exe	Get hash	malicious	Browse	• 210.182.29.70
	DyTbafeDoq.exe	Get hash	malicious	Browse	• 211.119.84.112
	yZ7D7o1Z7p	Get hash	malicious	Browse	• 61.32.157.192
	VdcjZYprbt	Get hash	malicious	Browse	• 106.251.165.239
	pLoEhdXNms.exe	Get hash	malicious	Browse	• 61.36.14.230
	AQ7reGjgnP.exe	Get hash	malicious	Browse	• 211.53.202.252
	344bx4XUBN.exe	Get hash	malicious	Browse	• 211.168.197.211

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Km5KAxQLLV.exe	Get hash	malicious	Browse	• 115.88.24.202

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/tmp/qemu-open.TuD6GS (deleted)	
Process:	/tmp/csB31kWt10
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:TgBCyy:TgYf
MD5:	4A922E471FA53B8DAA0FEE8547E3E06A
SHA1:	77B255512D26AE39E42695F3E340304FC34DCBA5
SHA-256:	B269152470ED063CECFB68A18C34EB1D7986D5217862054DD313F3E7C93DF8AC
SHA-512:	7B2A9BF1B59032D221D4C8FA4EFE69F6C01C1DE7B7A91C4FAF1DC26ACCE292953B38CCB6E5F582AACC9DBD8E7EA71FC37A249FC639CB79ADC2AE7CA9B5BB4DC0
Malicious:	false
Reputation:	low
Preview:	/tmp/csB31kWt10.

/tmp/qemu-open.bKPayR (deleted)	
Process:	/tmp/csB31kWt10
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:TgBCyy:TgYf
MD5:	4A922E471FA53B8DAA0FEE8547E3E06A
SHA1:	77B255512D26AE39E42695F3E340304FC34DCBA5
SHA-256:	B269152470ED063CECFB68A18C34EB1D7986D5217862054DD313F3E7C93DF8AC
SHA-512:	7B2A9BF1B59032D221D4C8FA4EFE69F6C01C1DE7B7A91C4FAF1DC26ACCE292953B38CCB6E5F582AACC9DBD8E7EA71FC37A249FC639CB79ADC2AE7CA9B5BB4DC0
Malicious:	false
Reputation:	low
Preview:	/tmp/csB31kWt10.

/tmp/qemu-open.iXUKLT (deleted)	
Process:	/tmp/csB31kWt10
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:TgBCyy:TgYf
MD5:	4A922E471FA53B8DAA0FEE8547E3E06A
SHA1:	77B255512D26AE39E42695F3E340304FC34DCBA5
SHA-256:	B269152470ED063CECFB68A18C34EB1D7986D5217862054DD313F3E7C93DF8AC
SHA-512:	7B2A9BF1B59032D221D4C8FA4EFE69F6C01C1DE7B7A91C4FAF1DC26ACCE292953B38CCB6E5F582AACC9DBD8E7EA71FC37A249FC639CB79ADC2AE7CA9B5BB4DC0
Malicious:	false
Reputation:	low

/tmp/qemu-open.iXUKLT (deleted)	
Preview:	/tmp/csB31kWt10.

/tmp/qemu-open.mDwNfR (deleted)	
Process:	/tmp/csB31kWt10
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:TgBCyy:TgYf
MD5:	4A922E471FA53B8DAA0FEE8547E3E06A
SHA1:	77B255512D26AE39E42695F3E340304FC34DCBA5
SHA-256:	B269152470ED063CECFB68A18C34EB1D7986D5217862054DD313F3E7C93DF8AC
SHA-512:	7B2A9BF1B59032D221D4C8FA4EFE69F6C01C1DE7B7A91C4FAF1DC26ACCE292953B38CCB6E5F582AACC9DBD8E7EA71FC37A249FC639CB79ADC2AE7CA9B5BB4DC0
Malicious:	false
Reputation:	low
Preview:	/tmp/csB31kWt10.

Static File Info

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.526002031107092
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	csB31kWt10
File size:	48624
MD5:	df1ed6e73703ce09673aa4525975d129
SHA1:	4b3444321f460d0ea48f4e96eb0ea45b27b885a6
SHA256:	1d41b0a9c3b189c68bf219335a60f8156857fc6cef890e165e9ad2c48b15103a
SHA512:	6776e5c9d462128f3ae4f07c019f4d5b195890116f7158359adb4e7a24642985db262eb3e4ab832fd721030635b96343f6bf3848b3775bcf772fd6e44d2f67e0
SSDEEP:	768:n24VmMBIOoR7sYhz9ezjFFZ4GZJZTXiT+dQeEogrig0cH:PYhz98jnZ4yzy3rl5
File Content Preview:	.ELF.....`.@.4.....4. ...(.....@...@.....D...D....`).....Q.td.....<|7.'!.....'.....<X7.'!.. .....9'.. .....<(7.'!.....9

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, little 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:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	48104
Section Header Size:	40
Number of Section Headers:	13

ELF header

Header String Table Index:	12

Sections

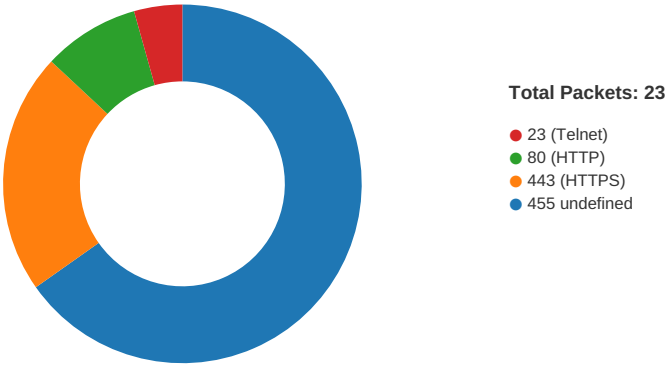
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x9bd0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x409cf0	0x9cf0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x409d50	0x9d50	0x6a0	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x44a3f4	0xa3f4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x44a3fc	0xa3fc	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x44a410	0xa410	0x1410	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x44b820	0xb820	0x370	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x44bb90	0xbb90	0x30	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x44bbc0	0xbb90	0x1194	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x61e	0xbb90	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0xbb90	0x57	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	0x400000	0x400000	0xa3f0	0xa3f0	3.1528	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xa3f4	0x44a3f4	0x44a3f4	0x179c	0x2960	2.1103	0x6	RW	0x10000		.ctors .dtors .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: csB31kWt10 PID: 5241 Parent PID: 5119

General

Start time:	09:39:54
Start date:	29/10/2021
Path:	/tmp/csB31kWt10
Arguments:	/tmp/csB31kWt10
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: csB31kWt10 PID: 5244 Parent PID: 5241

General

Start time:	09:39:55
Start date:	29/10/2021
Path:	/tmp/csB31kWt10
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: csB31kWt10 PID: 5246 Parent PID: 5244

General

Start time:	09:39:55
Start date:	29/10/2021
Path:	/tmp/csB31kWt10
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Deleted

File Read

File Written

Directory Enumerated