ID: 511528
Sample Name: SL92Sz9pl2
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:10:45
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

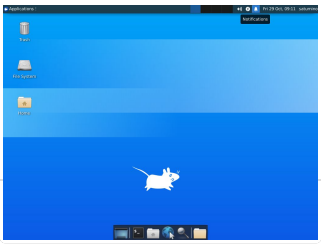
Linux Analysis Report SL92Sz9pl2

Overview

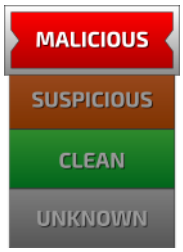
General Information

Sample Name:	SL92Sz9pl2
Analysis ID:	511528
MD5:	acf775d467b2008.
SHA1:	a51182722d62e8..
SHA256:	54999861537c5c..
Tags:	32 arm elf mirai
Infos:	

Most interesting Screenshot:



Detection

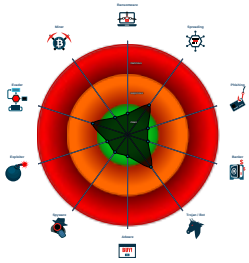


Score:	48
Range:	0 - 100
Whitelisted:	false

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:	511528
Start date:	29.10.2021
Start time:	09:10:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SL92Sz9pl2
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**
  - SL92Sz9pl2 (PID: 5244, Parent: 5119, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/SL92Sz9pl2
    - SL92Sz9pl2 New Fork (PID: 5246, Parent: 5244)
      - SL92Sz9pl2 New Fork (PID: 5248, Parent: 5246)
- **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

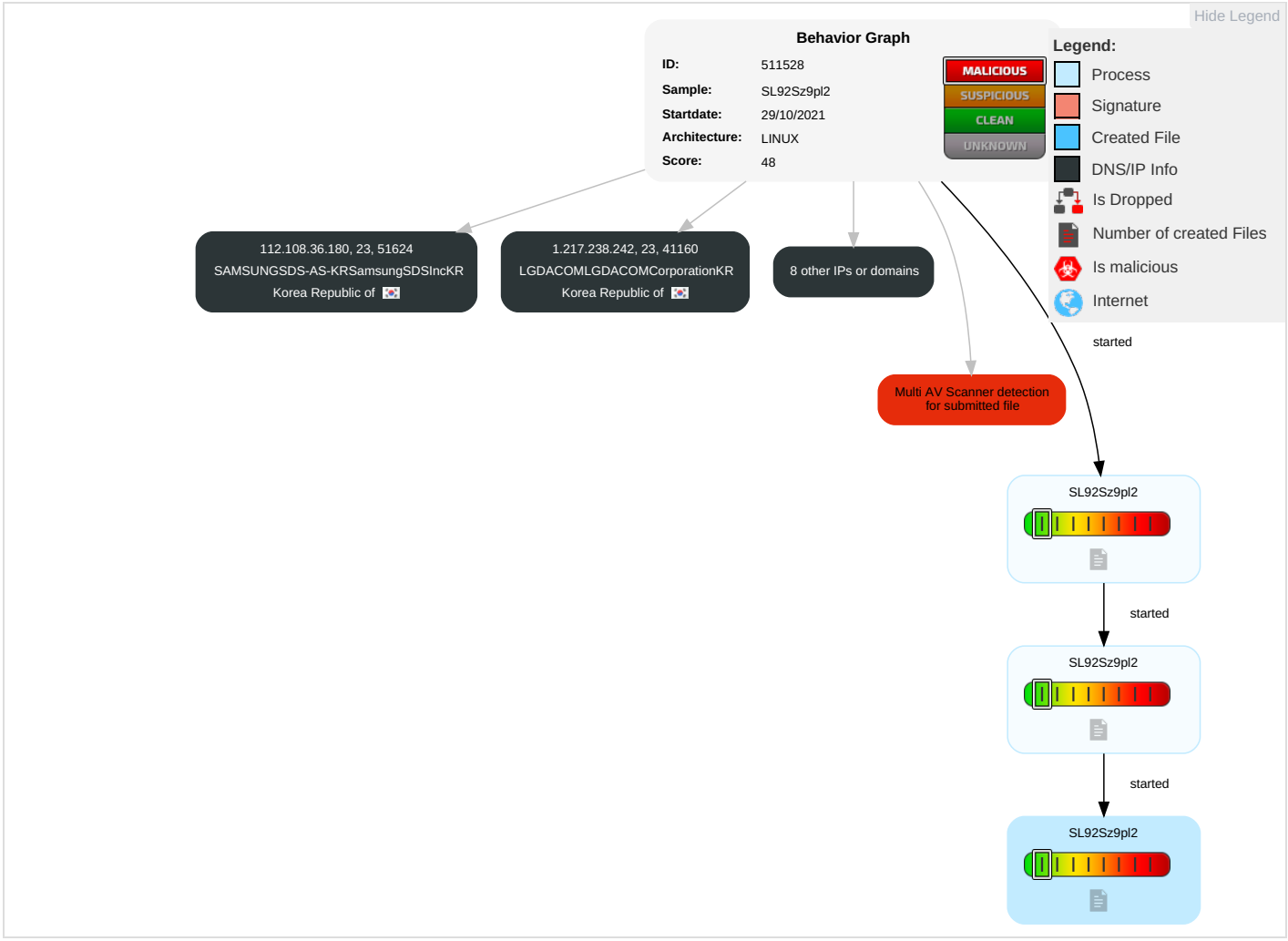
Mitre Att&ck Matrix

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

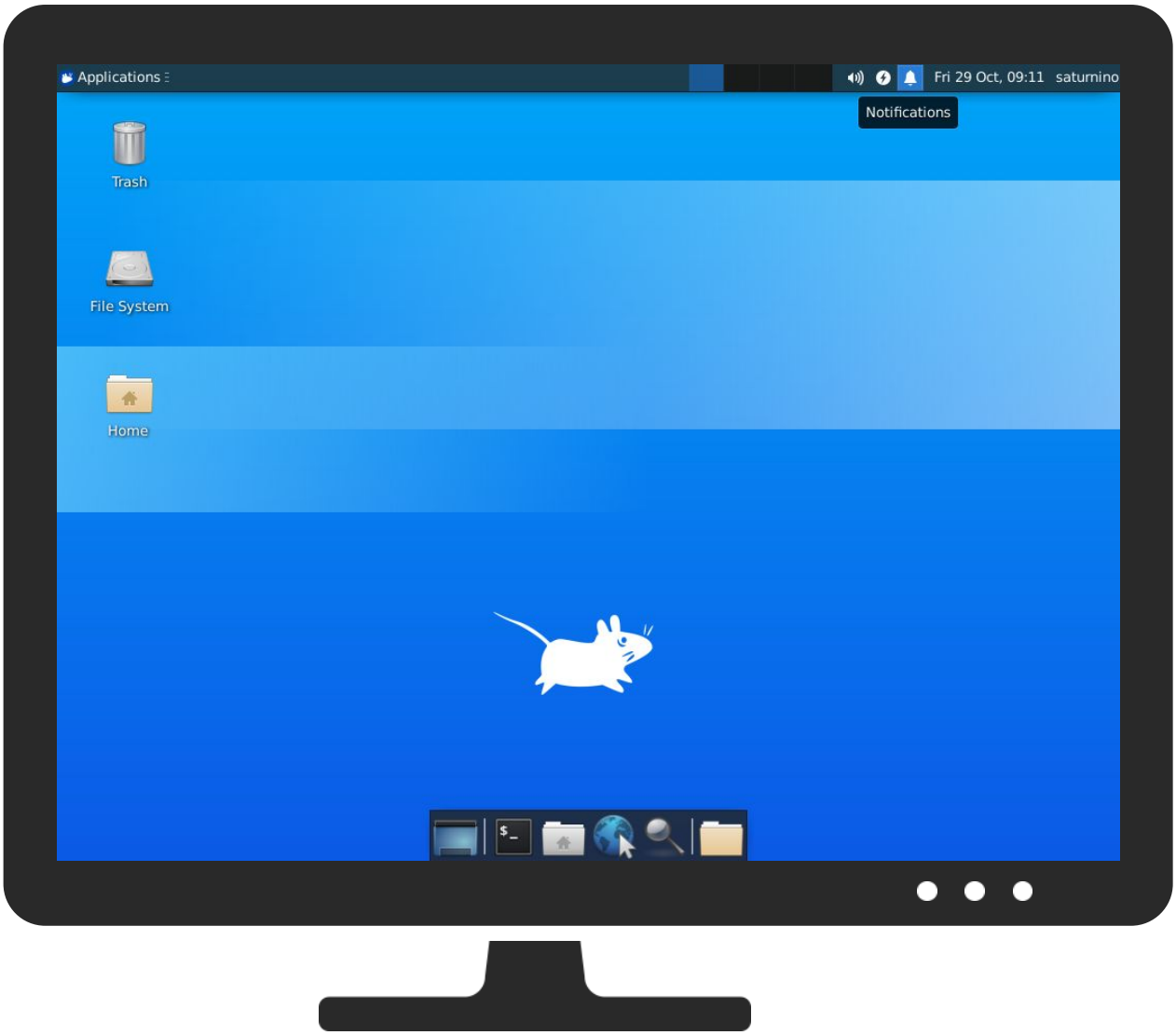
Behavior Graph



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
SL92Sz9pl2	18%	Virustotal		Browse
SL92Sz9pl2	16%	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
107.150.181.17	unknown	United States		3257	GTT-BACKBONEGTTDE	false
112.108.36.180	unknown	Korea Republic of		6619	SAMSUNGSDS-AS-KRSamsungSDSIncKR	false
45.95.169.120	unknown	Croatia (LOCAL Name: Hrvatska)		42864	GIGANET-HUGigaNetInternetServiceProviderCoHU	false
186.7.246.235	unknown	Dominican Republic		6400	CompaniaDominicanadeTelefonosSADO	false
1.217.238.242	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
122.55.159.118	unknown	Philippines		9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
121.165.132.200	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	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/SL92Sz9pl2
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	YpKL484IG5	Get hash	malicious	Browse	
	Y4W4j5QIqD	Get hash	malicious	Browse	
	1TnmkstVG8	Get hash	malicious	Browse	
	iksM5QEg2j	Get hash	malicious	Browse	
109.202.202.202	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	
	AOaKSm1cij	Get hash	malicious	Browse	
	Mozi.a	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ggbMKQDdG2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	
91.189.91.43	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	
	AOaKSm1cij	Get hash	malicious	Browse	
	Mozi.a	Get hash	malicious	Browse	
	ggbMKQDdG2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GTT-BACKBONEGTTDE	db0fa4b8db0333367e9bda3ab68b8042.x86	Get hash	malicious	Browse	• 212.222.240.78
	sora.arm	Get hash	malicious	Browse	• 195.149.138.21
	T4xP1S9Fhz	Get hash	malicious	Browse	• 213.251.29.121
	mkRkjGXjDJ	Get hash	malicious	Browse	• 195.134.205.183
	L7PID7HuZy	Get hash	malicious	Browse	• 23.44.22.7
	sora.arm	Get hash	malicious	Browse	• 77.67.233.101
	UCelJ4imjH	Get hash	malicious	Browse	• 66.7.147.49
	jMJ8Uz4Mhk	Get hash	malicious	Browse	• 173.205.42.122
	MMpysQ37RU	Get hash	malicious	Browse	• 198.144.102.13
	WSuNws5Xni	Get hash	malicious	Browse	• 213.251.29.133
	arm7	Get hash	malicious	Browse	• 149.235.225.191
	pandora.arm	Get hash	malicious	Browse	• 195.190.79.65
	s0bi9t	Get hash	malicious	Browse	• 172.231.159.148
	lCTNXNa4Bo	Get hash	malicious	Browse	• 198.60.91.95
	x.arm7	Get hash	malicious	Browse	• 204.93.45.117
	z0r0.x86	Get hash	malicious	Browse	• 74.199.193.136
	yXTRZQmYdr	Get hash	malicious	Browse	• 154.15.161.206
	9rBn8WA2An	Get hash	malicious	Browse	• 45.136.88.77
	Qr7o5ZZmz1	Get hash	malicious	Browse	• 141.136.100.52
	ii.x86	Get hash	malicious	Browse	• 204.93.45.157
GIGANET-HUGigaNetInternetServiceProviderCoHU	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	7okgnZjK06	Get hash	malicious	Browse	• 45.95.169.115
	D9efs9TYvN	Get hash	malicious	Browse	• 45.95.169.115
SAMSUNGSDS-AS-KRSamsungSDSIncKR	yZ7D7o1Z7p	Get hash	malicious	Browse	• 123.44.216.213
	4VC4C0PxQb	Get hash	malicious	Browse	• 123.47.122.175
	vLqyyo55oA	Get hash	malicious	Browse	• 123.33.181.5
	txwaNf62fv	Get hash	malicious	Browse	• 123.45.141.58
	juxSAmZoqx	Get hash	malicious	Browse	• 123.38.82.94
	lQKil1R7D9	Get hash	malicious	Browse	• 123.32.131.223
	HF0udkDj2N	Get hash	malicious	Browse	• 165.213.128.174
	x86	Get hash	malicious	Browse	• 121.253.249.8
	u9afRawaNV	Get hash	malicious	Browse	• 123.38.176.99
	7mtKAPnOCb	Get hash	malicious	Browse	• 123.36.202.141
	sora.arm7	Get hash	malicious	Browse	• 123.36.202.121
	1WL2kQmrNk	Get hash	malicious	Browse	• 112.108.82.141
	Hzcn88pPht	Get hash	malicious	Browse	• 123.45.118.154
	notabotnet.x86	Get hash	malicious	Browse	• 182.194.95.62
	ojZRw3eBpN	Get hash	malicious	Browse	• 112.107.164.182
	arm-20211013-0650	Get hash	malicious	Browse	• 157.197.246.114
	TM2ALMOZ8Q	Get hash	malicious	Browse	• 123.43.36.39
	xg5iCkP5YB	Get hash	malicious	Browse	• 123.42.125.126
	GaSBpMyVub	Get hash	malicious	Browse	• 112.107.186.95
	yir8ieZzXL	Get hash	malicious	Browse	• 203.241.150.248

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/tmp/qemu-open.8hfcY2 (deleted)	
Process:	/tmp/SL92Sz9pl2
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.375
Encrypted:	false
SSDEEP:	3:TgOcBj1:TgOcBx
MD5:	80F5614A276AEF52178A2C27B9199C12
SHA1:	15ACB1162CD414314D120C6FF7470CE30E3DCEEB
SHA-256:	217BC4BDA9FC91111B4D74B140800BE053E4D66821DA890E19C421F71D295988
SHA-512:	3C624B859C745686A0CF34D4BFCCA71A02C8F5E9742DAF8EBFDFF6C09208D2A50B380AFBA453D67E11F8BEDFF434E13132468FF130BBB045ED476F081A9F0D5
Malicious:	false
Reputation:	low
Preview:	/tmp/SL92Sz9pl2.

/tmp/qemu-open.id8Tj2 (deleted)	
Process:	/tmp/SL92Sz9pl2

/tmp/qemu-open.id8Tj2 (deleted)	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.375
Encrypted:	false
SSDEEP:	3:TgOcBj1:TgOcBx
MD5:	80F5614A276AEF52178A2C27B9199C12
SHA1:	15ACB1162CD414314D120C6FF7470CE30E3DCEEB
SHA-256:	217BC4BDA9FC91111B4D74B140800BE053E4D66821DA890E19C421F71D295988
SHA-512:	3C624B859C745686A0CF34D4BFCCA71A02C8F5E9742DAF8EBFDFF6C09208D2A50B380AFBA453D67E11F8BEDFF434E13132468FF130BBB045ED476F081A9F0D 5
Malicious:	false
Reputation:	low
Preview:	/tmp/SL92Sz9pl2.

/tmp/qemu-open.pjODa4 (deleted)	
Process:	/tmp/SL92Sz9pl2
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.375
Encrypted:	false
SSDEEP:	3:TgOcBj1:TgOcBx
MD5:	80F5614A276AEF52178A2C27B9199C12
SHA1:	15ACB1162CD414314D120C6FF7470CE30E3DCEEB
SHA-256:	217BC4BDA9FC91111B4D74B140800BE053E4D66821DA890E19C421F71D295988
SHA-512:	3C624B859C745686A0CF34D4BFCCA71A02C8F5E9742DAF8EBFDFF6C09208D2A50B380AFBA453D67E11F8BEDFF434E13132468FF130BBB045ED476F081A9F0D 5
Malicious:	false
Reputation:	low
Preview:	/tmp/SL92Sz9pl2.

/tmp/qemu-open.wcqiu3 (deleted)	
Process:	/tmp/SL92Sz9pl2
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.375
Encrypted:	false
SSDEEP:	3:TgOcBj1:TgOcBx
MD5:	80F5614A276AEF52178A2C27B9199C12
SHA1:	15ACB1162CD414314D120C6FF7470CE30E3DCEEB
SHA-256:	217BC4BDA9FC91111B4D74B140800BE053E4D66821DA890E19C421F71D295988
SHA-512:	3C624B859C745686A0CF34D4BFCCA71A02C8F5E9742DAF8EBFDFF6C09208D2A50B380AFBA453D67E11F8BEDFF434E13132468FF130BBB045ED476F081A9F0D 5
Malicious:	false
Reputation:	low
Preview:	/tmp/SL92Sz9pl2.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), s tatically linked, stripped
Entropy (8bit):	6.044993074412078
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	SL92Sz9pl2
File size:	36128
MD5:	acf775d467b2008bfad563cd934576b2
SHA1:	a51182722d62e8d152dfc4bbe8c5c6245e1a11da

General

SHA256:	54999861537c5c4f4c2ced5fdf0256b7b005603bee17b25e6ae5bb3f747e16cb
SHA512:	8b3f1c2253cf8532a819ae405ecfc2bf4245ec28cdb4d5a4156ae2e383deee3a50173d9f874680800c8a9a93881864a860328a8fb131a0e1789e2d335f19a89b
SSDEEP:	384:6iyyqQ633occCImPntbnDVHy9pr1ESW+TLs2Dy8I4YFG+KBUZ6VPoPJlcdNG6vFc:69yqd33ocVHgZKPxAUwVPYCz
File Content Preview:	.ELF...a.....(.....4.....4. ...(.....dw..dw.....hw..hw..hw.....X%.....Q.td.....-...L."..... .....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	35728
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

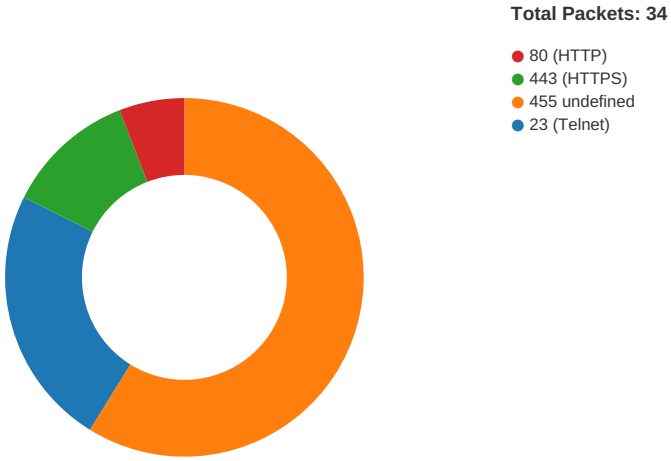
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x7030	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0xf0e0	0x70e0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0xf0f4	0x70f4	0x670	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x17768	0x7768	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x17770	0x7770	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1777c	0x777c	0x13d4	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x18b50	0x8b50	0x1170	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x8b50	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	0x8000	0x8000	0x7764	0x7764	3.1044	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x7768	0x17768	0x17768	0x13e8	0x2558	1.7449	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: SL92Sz9pl2 PID: 5244 Parent PID: 5119

General

Start time:	09:11:27
Start date:	29/10/2021
Path:	/tmp/SL92Sz9pl2
Arguments:	/tmp/SL92Sz9pl2
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: SL92Sz9pl2 PID: 5246 Parent PID: 5244

General

Start time:	09:11:27
Start date:	29/10/2021
Path:	/tmp/SL92Sz9pl2
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: SL92Sz9pl2 PID: 5248 Parent PID: 5246

General

Start time:	09:11:27
Start date:	29/10/2021
Path:	/tmp/SL92Sz9pl2

Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Deleted

File Read

File Written

Directory Enumerated