ID: 511555
Sample Name: rijsTqU0If
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:42:04
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

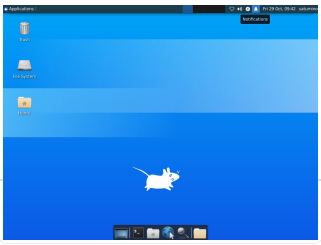
Linux Analysis Report rijsTqU0lf

Overview

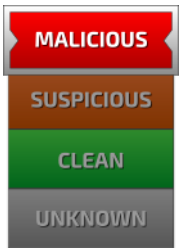
General Information

Sample Name:	rijsTqU0lf
Analysis ID:	511555
MD5:	8c305137c8b025..
SHA1:	4dc66a698ddbfbb.
SHA256:	93ca4f85d13c018..
Tags:	32 elf mips mirai
Infos:	

Most interesting Screenshot:



Detection

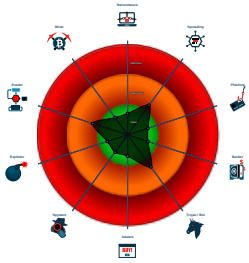


Score:	48
Range:	0 - 100
Whitelisted:	false

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:	511555
Start date:	29.10.2021
Start time:	09:42:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	rijsTqU0lf
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**
  - rijsTqU0lf (PID: 5257, Parent: 5135, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/rijsTqU0lf
    - rijsTqU0lf New Fork (PID: 5259, Parent: 5257)
      - rijsTqU0lf New Fork (PID: 5261, Parent: 5259)
- **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

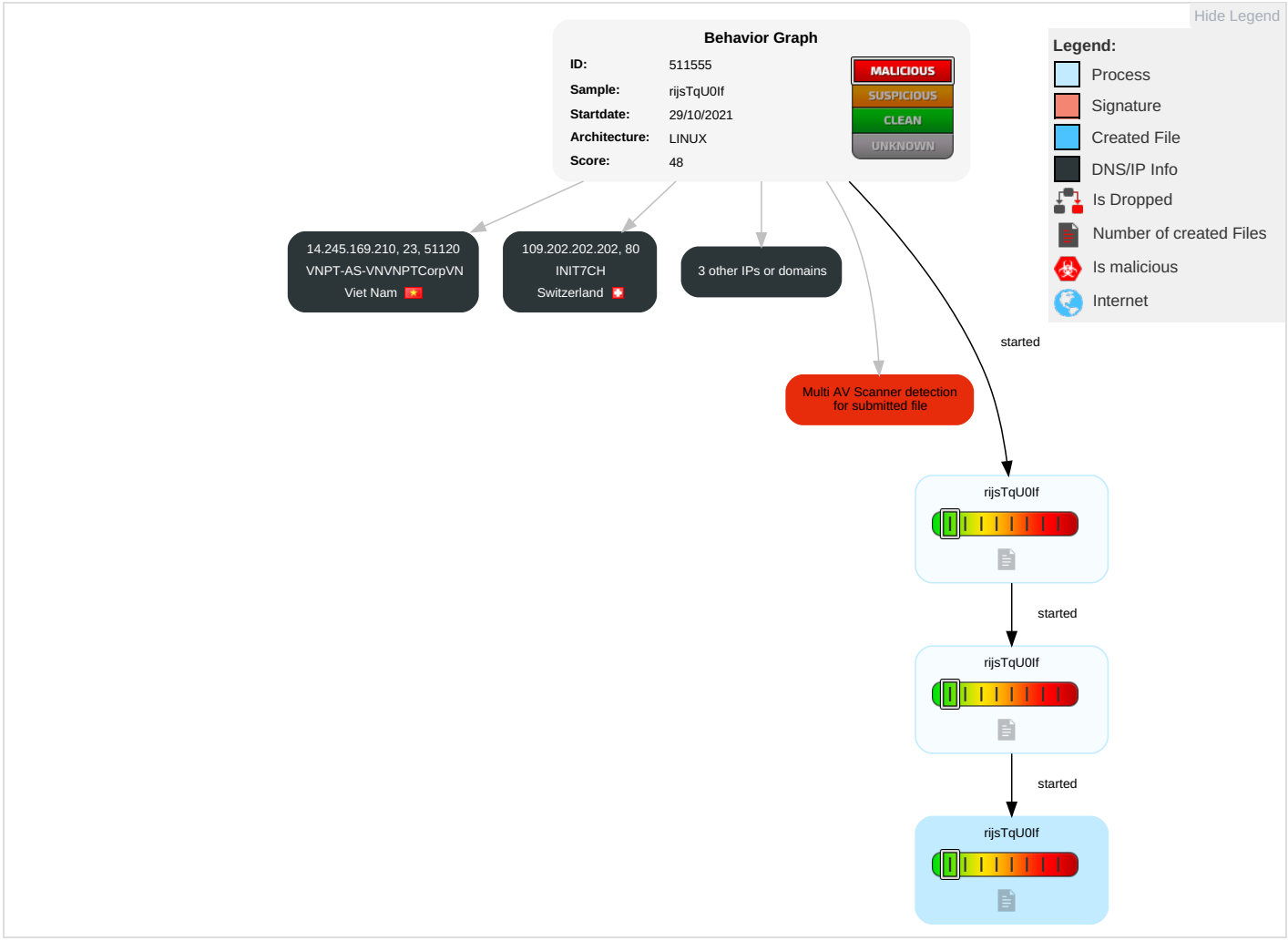
Mitre Att&ck Matrix

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

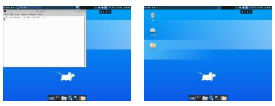
Behavior Graph

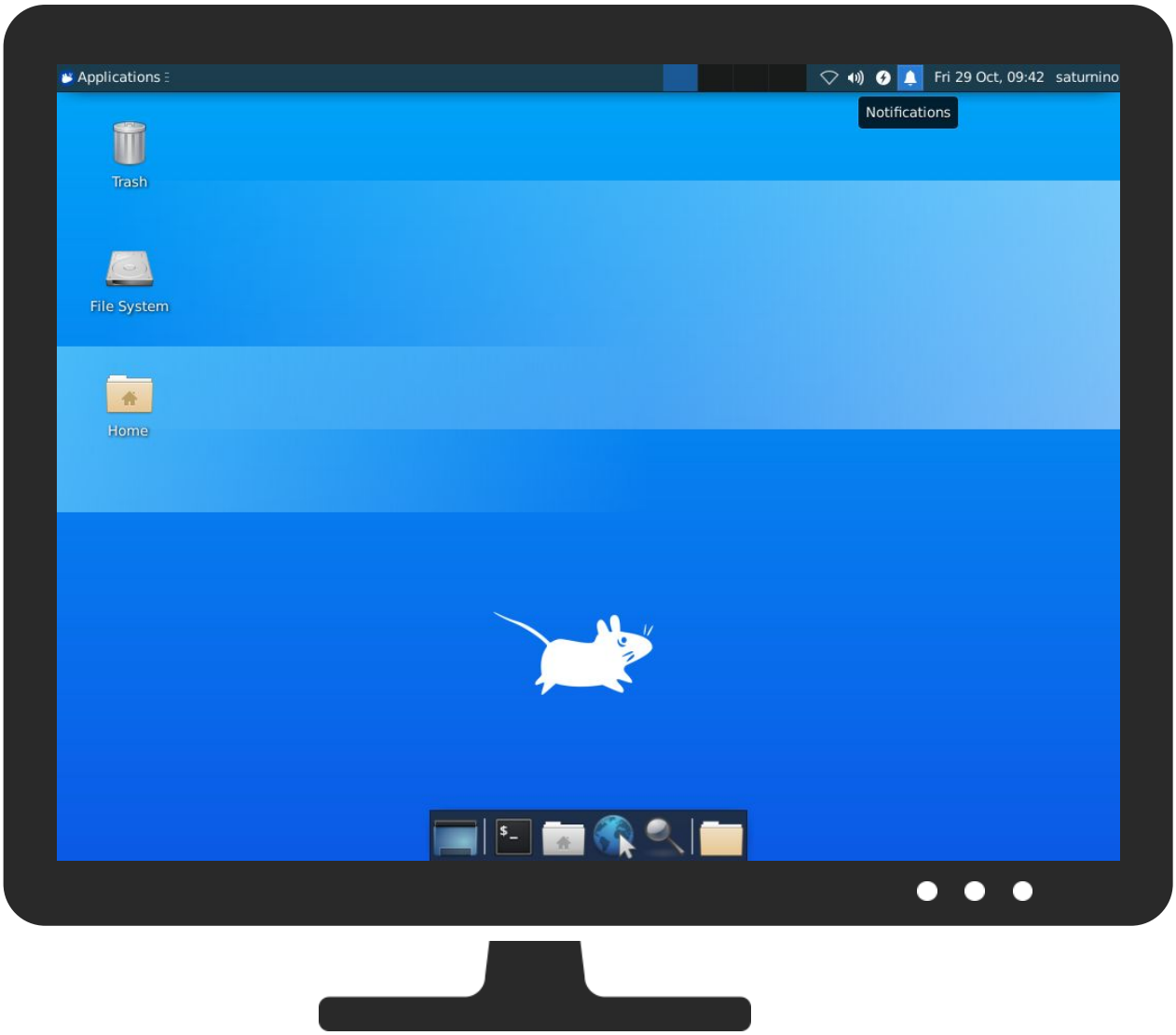


Screenshots

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
rijsTqU0If	21%	Virustotal		Browse
rijsTqU0If	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
14.245.169.210	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	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/rijsTqU0lf
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	csB31kWt10	Get hash	malicious	Browse	
	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	csB31kWt10	Get hash	malicious	Browse	
	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	
91.189.91.43	csB31kWt10	Get hash	malicious	Browse	
	QWg2NTuodY	Get hash	malicious	Browse	
	6VLeGqFkPS	Get hash	malicious	Browse	
	DL5blLw1ly	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
91.189.91.42	csB31kWt10	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GIGANET-HUGigaNetInternetServiceProviderCoHU	csB31kWt10	Get hash	malicious	Browse	• 45.95.169.120
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INIT7CH	csB31kWt10	Get hash	malicious	Browse	• 109.202.202.202
	QWg2NTuodY	Get hash	malicious	Browse	• 109.202.202.202
	6VLeGqFkPS	Get hash	malicious	Browse	• 109.202.202.202
	DL5blLw1ly	Get hash	malicious	Browse	• 109.202.202.202
	SL92Sz9pl2	Get hash	malicious	Browse	• 109.202.202.202
	YpKL484IG5	Get hash	malicious	Browse	• 109.202.202.202
	Y4W4j5QIqD	Get hash	malicious	Browse	• 109.202.202.202
	1TnmkstVG8	Get hash	malicious	Browse	• 109.202.202.202
	iksM5QEg2j	Get hash	malicious	Browse	• 109.202.202.202
	lGJEkz80oe	Get hash	malicious	Browse	• 109.202.202.202
	roV7kGaVr1	Get hash	malicious	Browse	• 109.202.202.202
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	• 109.202.202.202
	uPOWBxniTA	Get hash	malicious	Browse	• 109.202.202.202
	qy5unieRgR	Get hash	malicious	Browse	• 109.202.202.202
	sAzPpn6mKZ	Get hash	malicious	Browse	• 109.202.202.202
	AxadDC89j9	Get hash	malicious	Browse	• 109.202.202.202
	ZErnXU2XR1	Get hash	malicious	Browse	• 109.202.202.202
	sTHJvS5LPJ	Get hash	malicious	Browse	• 109.202.202.202
	THzHjYQ4z6	Get hash	malicious	Browse	• 109.202.202.202
	jC0B6sMh1d	Get hash	malicious	Browse	• 109.202.202.202
VNPT-AS-VNVNPTCorpVN	vEBWe85OY5	Get hash	malicious	Browse	• 14.253.102.15
	5mLAGfiGBf	Get hash	malicious	Browse	• 123.22.248.38
	VdcjZYprbt	Get hash	malicious	Browse	• 14.161.68.251
	x86_64	Get hash	malicious	Browse	• 14.253.102.17
	3QM8LROaOk	Get hash	malicious	Browse	• 14.243.17.127
	mdyu2wtnR8	Get hash	malicious	Browse	• 113.174.18 8.232
	4VC4C0PxQb	Get hash	malicious	Browse	• 123.29.125.18
	KfvEoN0wlw	Get hash	malicious	Browse	• 123.16.27.140
	K1fia4oWep	Get hash	malicious	Browse	• 123.22.224.13
	juxSAmZoqx	Get hash	malicious	Browse	• 123.18.32.68
	db0fa4b8db0333367e9bda3ab68b8042.x86	Get hash	malicious	Browse	• 123.22.248.34
	6NzbU4oW61	Get hash	malicious	Browse	• 123.26.120.231
	IcwrPqGkXP	Get hash	malicious	Browse	• 113.180.223.7
	sora.arm	Get hash	malicious	Browse	• 14.178.101.117
	UYnpKcFZ2s	Get hash	malicious	Browse	• 14.232.212.176
	zYMp3detVO	Get hash	malicious	Browse	• 113.175.69.143
	Tf9ATzpdKR	Get hash	malicious	Browse	• 14.237.37.63
	b3astmode.x86	Get hash	malicious	Browse	• 14.184.247.127
	JYWllP5wHP	Get hash	malicious	Browse	• 222.252.74.200
	sora.arm7	Get hash	malicious	Browse	• 14.180.176.215

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/tmp/qemu-open.FkwlI2 (deleted)	
Process:	/tmp/rijsTqU0If
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	3:TgfUX:TgfUX
MD5:	F74579562F35CBFB0F4F4CDB336291CC
SHA1:	832C3E5265179CEE8D7209B6AA96F037415D564A
SHA-256:	D6A6D223938608296B875F461E30143D0860BBDD07D17AF915F5D4EEB51D4A51
SHA-512:	337EA0D2387093EC5498EB2E43F437CEB1D73E7CD1C274924485BC96BBFA539C5FAAAB0124D786A8691BDC8A05D26220C37686CF7A8E6BB0D441BC4B9B5BA 04
Malicious:	false
Reputation:	low
Preview:	/tmp/rijsTqU0If.

/tmp/qemu-open.I72D7Z (deleted)	
Process:	/tmp/rijsTqU0If
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	3:TgfUX:TgfUX
MD5:	F74579562F35CBFB0F4F4CDB336291CC
SHA1:	832C3E5265179CEE8D7209B6AA96F037415D564A
SHA-256:	D6A6D223938608296B875F461E30143D0860BBDD07D17AF915F5D4EEB51D4A51
SHA-512:	337EA0D2387093EC5498EB2E43F437CEB1D73E7CD1C274924485BC96BBFA539C5FAAAB0124D786A8691BDC8A05D26220C37686CF7A8E6BB0D441BC4B9B5BA 04
Malicious:	false
Reputation:	low
Preview:	/tmp/rijsTqU0If.

/tmp/qemu-open.mWC470 (deleted)	
Process:	/tmp/rijsTqU0If
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	3:TgfUX:TgfUX
MD5:	F74579562F35CBFB0F4F4CDB336291CC
SHA1:	832C3E5265179CEE8D7209B6AA96F037415D564A
SHA-256:	D6A6D223938608296B875F461E30143D0860BBDD07D17AF915F5D4EEB51D4A51
SHA-512:	337EA0D2387093EC5498EB2E43F437CEB1D73E7CD1C274924485BC96BBFA539C5FAAAB0124D786A8691BDC8A05D26220C37686CF7A8E6BB0D441BC4B9B5BA 04
Malicious:	false
Reputation:	low
Preview:	/tmp/rijsTqU0If.

/tmp/qemu-open.zQV7X2 (deleted)	
Process:	/tmp/rijsTqU0If
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	3:TgfUX:TgfUX
MD5:	F74579562F35CBFB0F4F4CDB336291CC

/tmp/qemu-open.zQV7X2 (deleted)	
SHA1:	832C3E5265179CEE8D7209B6AA96F037415D564A
SHA-256:	D6A6D223938608296B875F461E30143D0860BBDD07D17AF915F5D4EEB51D4A51
SHA-512:	337EA0D2387093EC5498EB2E43F437CEB1D73E7CD1C274924485BC96BBFA539C5FAAAB0124D786A8691BDC8A05D26220C37686CF7A8E6BB0D441BC4B9B5BA/ 04
Malicious:	false
Reputation:	low
Preview:	/tmp/rijsTqU0If.

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.519592349845016
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	rijsTqU0If
File size:	48272
MD5:	8c305137c8b025af33ac608a9b5465b9
SHA1:	4dc66a698ddbfbb1bf77a67af5c85b997b99a17e
SHA256:	93ca4f85d13c01834ae5b36d93cca17bd924dcbb9b238c7a3e2d51646d0c636a
SHA512:	d7f2b6b6cc51d996d08e29006955b5283861010ae910e17168c5532f8bd56bf0b07eab51f4198ff39c82fecb7c534785c9513ef08812e868c89c8103e52d3ce4
SSDEEP:	768:JSLLLLLLLLOIqHAH1kJJ5hpnagnRqZPqtbKSWQiyn3Sb6G8dhDJ:W0TV3RqI8nyCb6lJJ
File Content Preview:	.ELF.....@.`...4.....4. ...(.....@...@.....D...D.....)`.....dt.Q.....<...'.6....!'.....<...'.5....!... ....'9... .....<...'.5....!.....'9.

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:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	47752
Section Header Size:	40
Number of Section Headers:	13
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	0x9a70	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x409b90	0x9b90	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x409bf0	0x9bf0	0x6a0	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x44a294	0xa294	0x8	0x0	0x3	WA	0	0	4

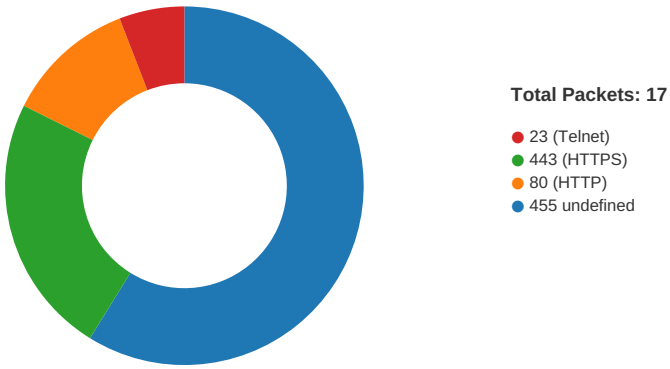
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.dtors	PROGBITS	0x44a29c	0xa29c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x44a2b0	0xa2b0	0x1410	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x44b6c0	0xb6c0	0x370	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x44ba30	0xba30	0x30	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x44ba60	0xba30	0x1194	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x61e	0xba30	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0xba30	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	0xa290	0xa290	3.1329	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xa294	0x44a294	0x44a294	0x179c	0x2960	2.1226	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: rijsTqU0lf PID: 5257 Parent PID: 5135

General

Start time:	09:42:47
Start date:	29/10/2021
Path:	/tmp/rijsTqU0lf
Arguments:	/tmp/rijsTqU0lf
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: rijsTqU0lf PID: 5259 Parent PID: 5257

General

Start time:	09:42:47
Start date:	29/10/2021
Path:	/tmp/rijsTqU0lf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: rijsTqU0lf PID: 5261 Parent PID: 5259

General

Start time:	09:42:47
Start date:	29/10/2021
Path:	/tmp/rijsTqU0lf
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Deleted

File Read

File Written

Directory Enumerated