ID: 511523
Sample Name: YpKL484IG5
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:02:12
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

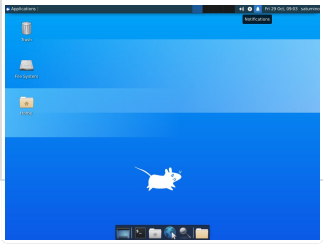
Linux Analysis Report YpKL484IG5

Overview

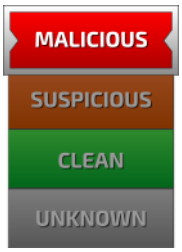
General Information

Sample Name:	YpKL484IG5
Analysis ID:	511523
MD5:	e9e2ace904c9f20..
SHA1:	dcd1a8cef227c63..
SHA256:	0ace9c1e48517f7..
Tags:	32 elf renesas
Infos:	

Most interesting Screenshot:



Detection

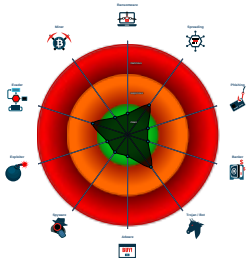


Score:	48
Range:	0 - 100
Whitelisted:	false

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

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:	511523
Start date:	29.10.2021
Start time:	09:02:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YpKL484IG5
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**
  - YpKL484IG5 (PID: 5237, Parent: 5119, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/YpKL484IG5
    - YpKL484IG5 New Fork (PID: 5239, Parent: 5237)
      - YpKL484IG5 New Fork (PID: 5241, Parent: 5239)
- **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

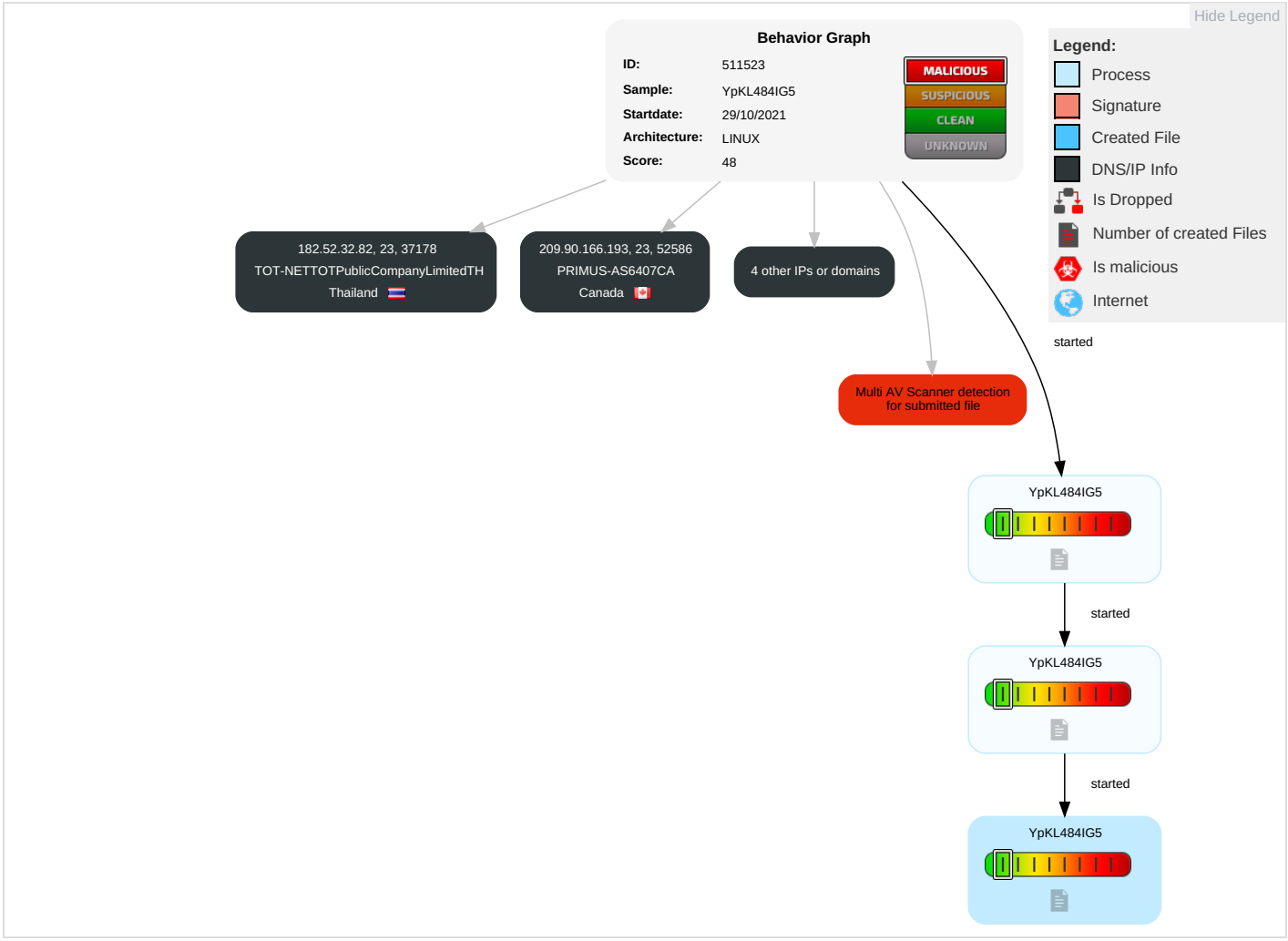
Mitre Att&ck Matrix

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

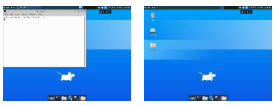
Behavior Graph

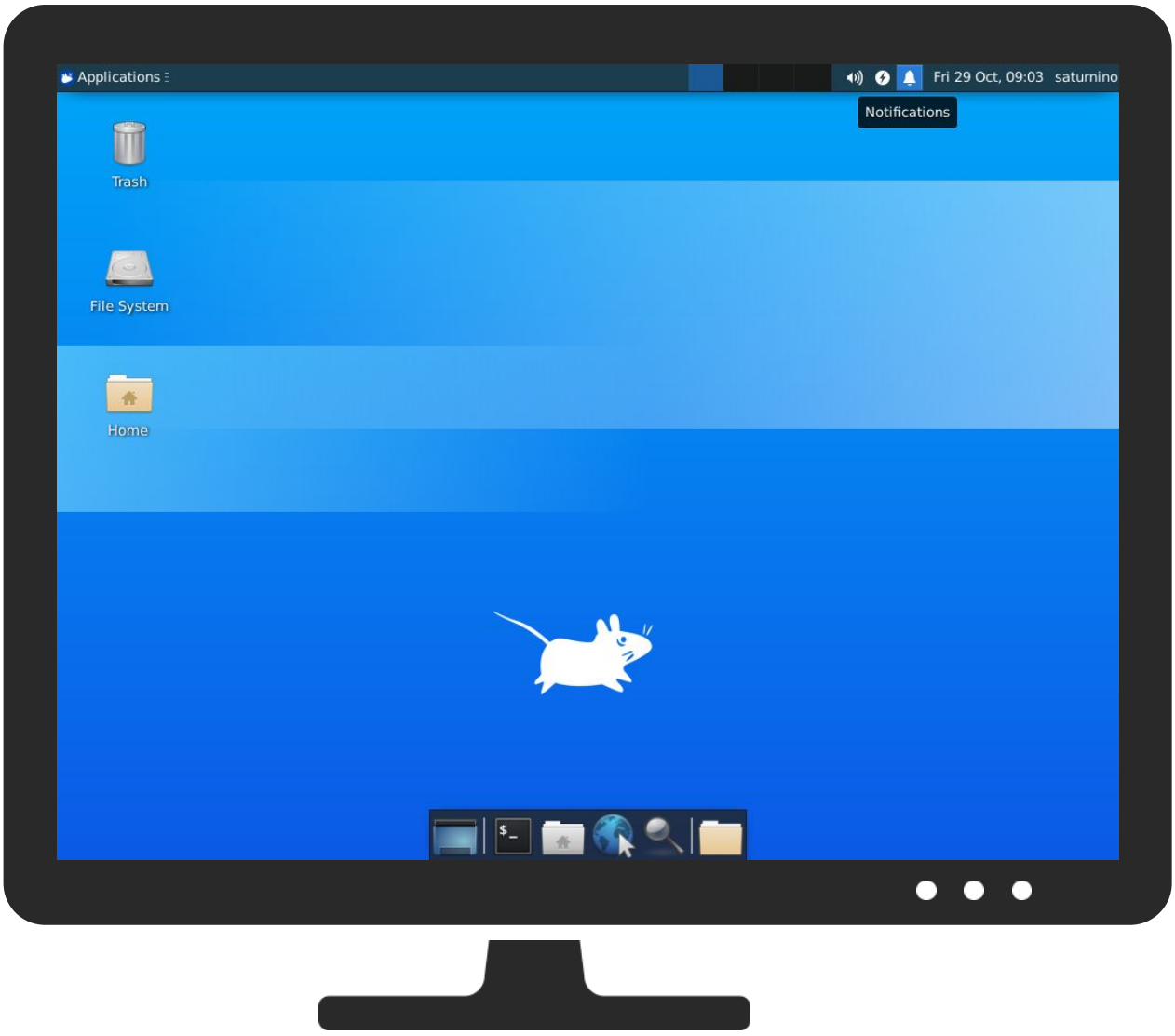


Screenshots

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
YpKL484IG5	21%	Virustotal		Browse
YpKL484IG5	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
45.95.169.120	unknown	Croatia (LOCAL Name: Hrvatska)		42864	GIGANET-HUGigaNetInternetServiceProviderCoHU	false
209.90.166.193	unknown	Canada		6407	PRIMUS-AS6407CA	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
182.52.32.82	unknown	Thailand		23969	TOT-NETTOTPublicCompanyLimitedTH	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/YpKL484IG5
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	Y4W4j5QIqD	Get hash	malicious	Browse	
	1TnmkstVG8	Get hash	malicious	Browse	
	iksM5QEg2j	Get hash	malicious	Browse	
109.202.202.202	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	
	AbriuSDkeL	Get hash	malicious	Browse	
91.189.91.43	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	

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

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PRIMUS-AS6407CA	o4wjsQMo7q	Get hash	malicious	Browse	• 204.52.2.37
	RkH17dHLZt	Get hash	malicious	Browse	• 204.52.2.46
	L1ecmEWyAw	Get hash	malicious	Browse	• 173.206.218.16
	notabotnet.arm	Get hash	malicious	Browse	• 173.206.218.20
	kqaEUydKGF	Get hash	malicious	Browse	• 204.48.48.94
	bTRSDGefHc	Get hash	malicious	Browse	• 216.181.238.32
	sora.arm	Get hash	malicious	Browse	• 173.206.243.26
	ho4yrUrdk1	Get hash	malicious	Browse	• 216.254.194.50
	dark.arm	Get hash	malicious	Browse	• 204.52.2.67
	sora.arm	Get hash	malicious	Browse	• 207.116.25.36
	KzWXGmiJxS	Get hash	malicious	Browse	• 207.116.49.59
	hzD4UBTK5H	Get hash	malicious	Browse	• 108.63.164.212
	BqfM9JwIC5	Get hash	malicious	Browse	• 204.52.83.211
	R0zLx1X0D0	Get hash	malicious	Browse	• 204.48.2.5
	TwlnaihoCK	Get hash	malicious	Browse	• 207.116.49.15
	sA0dlWB3al	Get hash	malicious	Browse	• 64.56.254.247
	3f7zmNN0nQ	Get hash	malicious	Browse	• 209.227.129.123
	KoknEiNL8U	Get hash	malicious	Browse	• 216.254.182.70
	3etkq3iOPQ	Get hash	malicious	Browse	• 173.206.218.72
	peach.arm7	Get hash	malicious	Browse	• 216.254.194.81
GIGANET-HUGigaNetInternetServiceProviderCoHU	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
	7okgnZjK06	Get hash	malicious	Browse	• 45.95.169.115
	D9efs9TYvN	Get hash	malicious	Browse	• 45.95.169.115
	LlE7nUUjmA	Get hash	malicious	Browse	• 45.95.169.115
INIT7CH	Y4W4j5QIqD	Get hash	malicious	Browse	• 109.202.202.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	JoLmvC65B7	Get hash	malicious	Browse	• 109.202.202.202
	AOaKSm1cij	Get hash	malicious	Browse	• 109.202.202.202
	Mozi.a	Get hash	malicious	Browse	• 109.202.202.202
	ggbMKQDdG2	Get hash	malicious	Browse	• 109.202.202.202
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	• 109.202.202.202
	AbriuSDkeL	Get hash	malicious	Browse	• 109.202.202.202

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/tmp/qemu-open.1prlPu (deleted)	
Process:	/tmp/YpKL484IG5
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:TgIJ:Tgo
MD5:	6BEB25EF1CFC2913704E086EDFA828E7
SHA1:	6A4BEAF98F707CBEE3FB5537560BB6982E564F02
SHA-256:	4E3BE4C49C92511634294722FA7FB5B93A90F751E18A8CB94DA0C67BEAC7E51A
SHA-512:	81F690A68C4E2B246176B7868FFF7C1468AB7640B4829910940B3B219347090AA57EC945656D5FB41FA7901D9831202000A8AD290C979F0634AE723FF9583F9B
Malicious:	false
Reputation:	low
Preview:	/tmp/YpKL484IG5.

/tmp/qemu-open.F9rJYt (deleted)	
Process:	/tmp/YpKL484IG5
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:TgIJ:Tgo
MD5:	6BEB25EF1CFC2913704E086EDFA828E7
SHA1:	6A4BEAF98F707CBEE3FB5537560BB6982E564F02
SHA-256:	4E3BE4C49C92511634294722FA7FB5B93A90F751E18A8CB94DA0C67BEAC7E51A
SHA-512:	81F690A68C4E2B246176B7868FFF7C1468AB7640B4829910940B3B219347090AA57EC945656D5FB41FA7901D9831202000A8AD290C979F0634AE723FF9583F9B
Malicious:	false
Reputation:	low
Preview:	/tmp/YpKL484IG5.

/tmp/qemu-open.g4pvNs (deleted)	
Process:	/tmp/YpKL484IG5
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:TgIJ:Tgo
MD5:	6BEB25EF1CFC2913704E086EDFA828E7
SHA1:	6A4BEAF98F707CBEE3FB5537560BB6982E564F02
SHA-256:	4E3BE4C49C92511634294722FA7FB5B93A90F751E18A8CB94DA0C67BEAC7E51A
SHA-512:	81F690A68C4E2B246176B7868FFF7C1468AB7640B4829910940B3B219347090AA57EC945656D5FB41FA7901D9831202000A8AD290C979F0634AE723FF9583F9B
Malicious:	false
Reputation:	low
Preview:	/tmp/YpKL484IG5.

/tmp/qemu-open.v6w7Qw (deleted)	
Process:	/tmp/YpKL484IG5
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.625
Encrypted:	false
SSDEEP:	3:TgIJ:Tgo
MD5:	6BEB25EF1CFC2913704E086EDFA828E7
SHA1:	6A4BEAF98F707CBEE3FB5537560BB6982E564F02
SHA-256:	4E3BE4C49C92511634294722FA7FB5B93A90F751E18A8CB94DA0C67BEAC7E51A
SHA-512:	81F690A68C4E2B246176B7868FFF7C1468AB7640B4829910940B3B219347090AA57EC945656D5FB41FA7901D9831202000A8AD290C979F0634AE723FF9583F9B
Malicious:	false
Reputation:	low
Preview:	/tmp/YpKL484IG5.

Static File Info

General

File type:	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.667136040804854
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	YpKL484IG5
File size:	32140
MD5:	e9e2ace904c9f2049ee2d16403868e50
SHA1:	dcd1a8cef227c63725ed272a8b9e83f8306104d8

General

SHA256:	0ace9c1e48517f73c6385f9ebdf3f67a9e7a37bddca6503e1d8f5f6ad7dc91a6
SHA512:	f4bf61bbc2cd88641adddceb7544e53b2f9abae6e62f03bc2898cc1e2f714135e340ad2abde01beadc71064320c494dbfb5159c18675f0a448c22a795f380177
SSDEEP:	384:D+kUtKh11Cj3vHN2btttaukXT0oPaqO7LPaokol9rH/WUqBUMt9CH7Kzgsb:D+kUtKtCj3vHCEDGqpol9rfX+Ce
File Content Preview:	.ELF.....*.....@.4....{.....4. ...(.....@...@..g...g.....g...gA..gA.....X%.....Q.td....././"O.n.....#.*@.....#.*@.`...o&O.n...l....././.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	31740
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

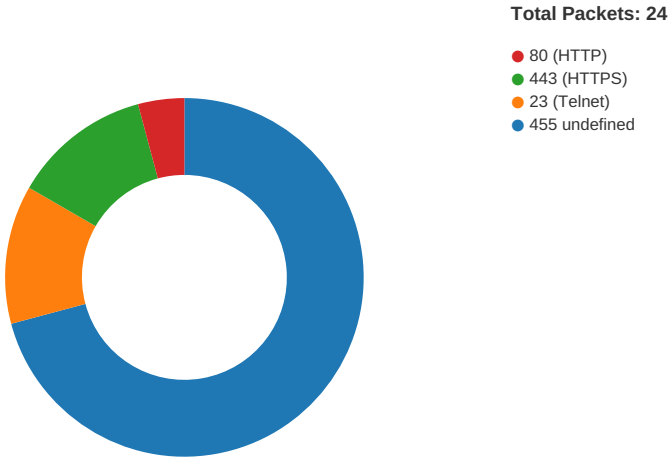
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0x60c0	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x4061a0	0x61a0	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x4061c4	0x61c4	0x610	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x4167d8	0x67d8	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x4167e0	0x67e0	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x4167ec	0x67ec	0x13d0	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x417bbc	0x7bbc	0x1174	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x7bbc	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	0x400000	0x400000	0x67d4	0x67d4	4.7784	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x67d8	0x4167d8	0x4167d8	0x13e4	0x2558	1.7679	0x6	RW	0x10000		.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: YpKL484IG5 PID: 5237 Parent PID: 5119

General

Start time:	09:02:59
Start date:	29/10/2021
Path:	/tmp/YpKL484IG5
Arguments:	/tmp/YpKL484IG5
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: YpKL484IG5 PID: 5239 Parent PID: 5237

General

Start time:	09:03:00
Start date:	29/10/2021
Path:	/tmp/YpKL484IG5
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: YpKL484IG5 PID: 5241 Parent PID: 5239

General

Start time:	09:03:00
Start date:	29/10/2021
Path:	/tmp/YpKL484IG5

Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Deleted

File Read

File Written

Directory Enumerated