ID: 511561
Sample Name: qlmOM0y98B
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:52:38
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

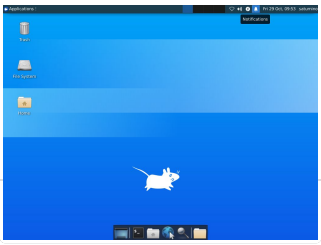
Linux Analysis Report qlmOM0y98B

Overview

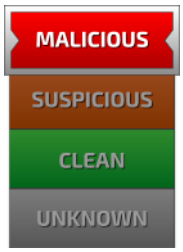
General Information

Sample Name:	qlmOM0y98B
Analysis ID:	511561
MD5:	6c982efa63458b4.
SHA1:	199fd3f587ed36e..
SHA256:	1b20443752270c..
Tags:	32 elf mirai powerpc
Infos:	

Most interesting Screenshot:



Detection

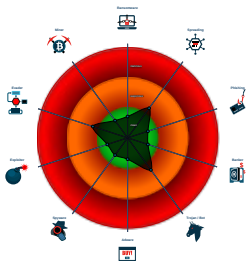


Score:	48
Range:	0 - 100
Whitelisted:	false

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:	511561
Start date:	29.10.2021
Start time:	09:52:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qlmOM0y98B
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**
- qlmOM0y98B (PID: 5241, Parent: 5117, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/qlmOM0y98B
  - qlmOM0y98B New Fork (PID: 5243, Parent: 5241)
    - qlmOM0y98B New Fork (PID: 5245, Parent: 5243)
- **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

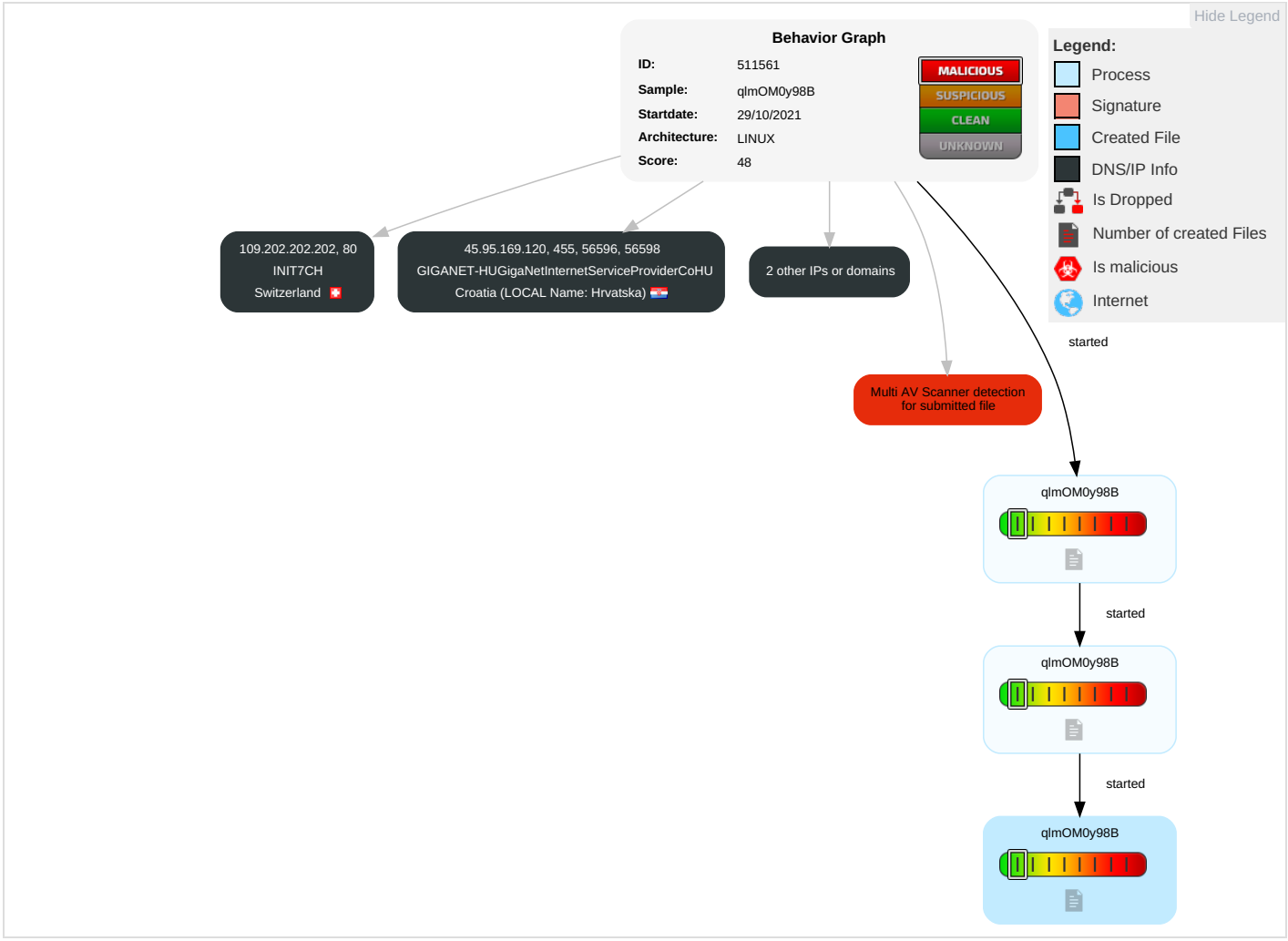
Mitre Att&ck Matrix

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

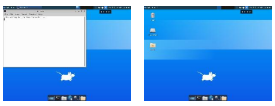
Behavior Graph

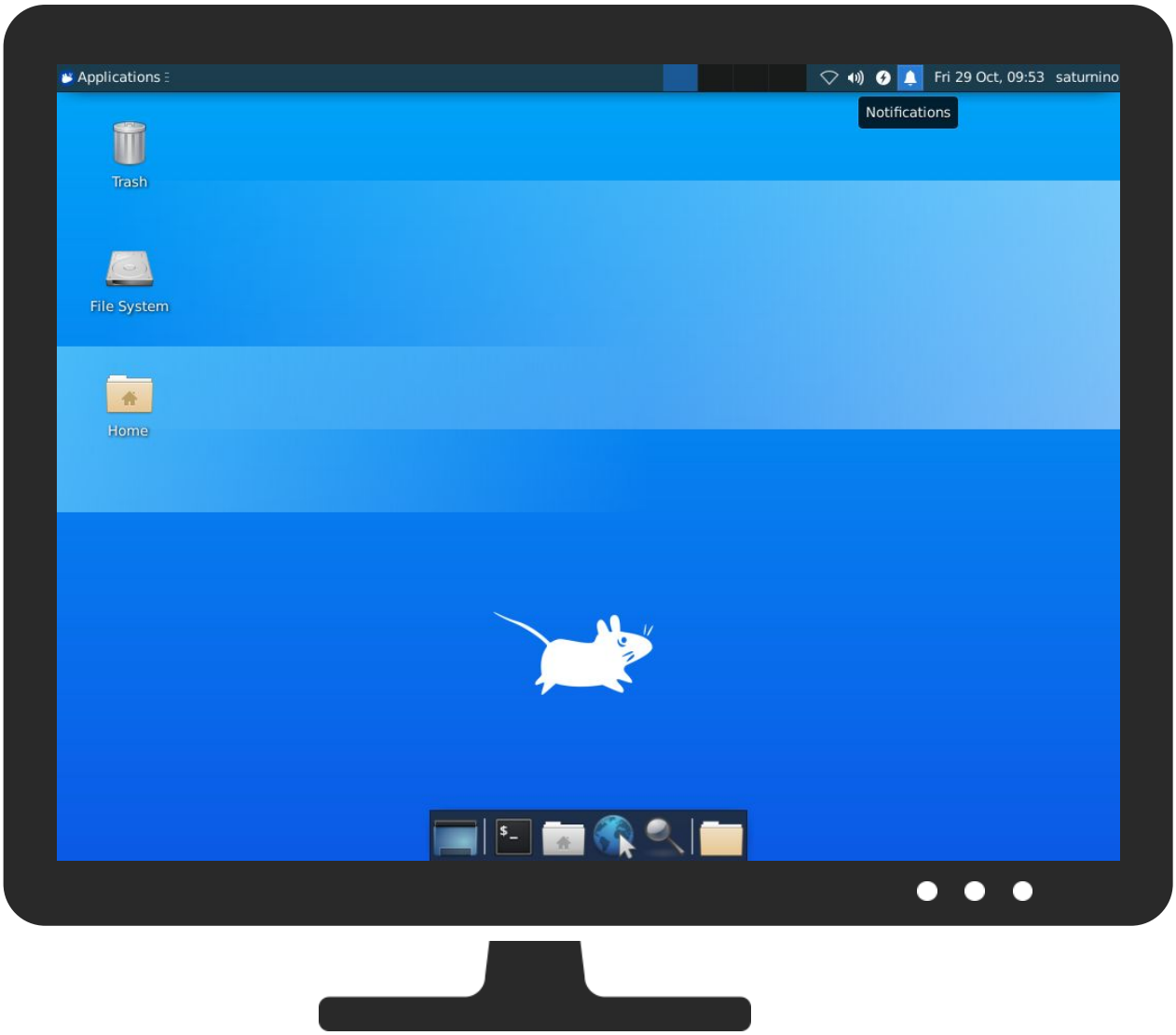


Screenshots

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
qlmOM0y98B	21%	Virustotal		Browse
qlmOM0y98B	18%	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
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/qlmOM0y98B
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	3tgXa7CGc1	Get hash	malicious	Browse	
	rijsTqU0lf	Get hash	malicious	Browse	
	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	WXMAqjlcvg	Get hash	malicious	Browse	
	3tgXa7CGc1	Get hash	malicious	Browse	
	rijsTqU0lf	Get hash	malicious	Browse	
	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	
91.189.91.43	WXMAqjlcvg	Get hash	malicious	Browse	
	3tgXa7CGc1	Get hash	malicious	Browse	
	rijsTqU0lf	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
91.189.91.42	WXMAqjlcvg	Get hash	malicious	Browse	
	3tgXa7CGc1	Get hash	malicious	Browse	
	rijsTqU0lf	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CANONICAL-ASGB	WXMAqjlcvg	Get hash	malicious	Browse	• 91.189.91.42
	3tgXa7CGc1	Get hash	malicious	Browse	• 91.189.91.42
	rijsTqU0lf	Get hash	malicious	Browse	• 91.189.91.42
	csB31kWt10	Get hash	malicious	Browse	• 91.189.91.42
	QWg2NTuodY	Get hash	malicious	Browse	• 91.189.91.42
	6VLeGqFkPS	Get hash	malicious	Browse	• 91.189.91.42
	DL5blLw1ly	Get hash	malicious	Browse	• 91.189.91.42
	SL92Sz9pl2	Get hash	malicious	Browse	• 91.189.91.42
	YpKL484IG5	Get hash	malicious	Browse	• 91.189.91.42
	Y4W4j5QIqD	Get hash	malicious	Browse	• 91.189.91.42
	1TnmkstVG8	Get hash	malicious	Browse	• 91.189.91.42
	iksM5QEg2j	Get hash	malicious	Browse	• 91.189.91.42
	lGJEkz80oe	Get hash	malicious	Browse	• 91.189.91.42
	roV7kGaVr1	Get hash	malicious	Browse	• 91.189.91.42
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	• 91.189.91.42
	uPOWBxniTA	Get hash	malicious	Browse	• 91.189.91.42
	qy5unieRgR	Get hash	malicious	Browse	• 91.189.91.42
	sAzPpn6mKZ	Get hash	malicious	Browse	• 91.189.91.42
	AxadDC89j9	Get hash	malicious	Browse	• 91.189.91.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ZErnXU2XR1	Get hash	malicious	Browse	• 91.189.91.42
CANONICAL-ASGB	WXMAqjlcvg	Get hash	malicious	Browse	• 91.189.91.42
	3tgXa7CGc1	Get hash	malicious	Browse	• 91.189.91.42
	rijsTqU0lf	Get hash	malicious	Browse	• 91.189.91.42
	csB31kWt10	Get hash	malicious	Browse	• 91.189.91.42
	QWg2NTuodY	Get hash	malicious	Browse	• 91.189.91.42
	6VLeGqFkPS	Get hash	malicious	Browse	• 91.189.91.42
	DL5blLw1ly	Get hash	malicious	Browse	• 91.189.91.42
	SL92Sz9pl2	Get hash	malicious	Browse	• 91.189.91.42
	YpKL484IG5	Get hash	malicious	Browse	• 91.189.91.42
	Y4W4j5QIqD	Get hash	malicious	Browse	• 91.189.91.42
	1TnmkstVG8	Get hash	malicious	Browse	• 91.189.91.42
	iksM5QEg2j	Get hash	malicious	Browse	• 91.189.91.42
	lGJEkz80oe	Get hash	malicious	Browse	• 91.189.91.42
	roV7kGaVr1	Get hash	malicious	Browse	• 91.189.91.42
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	• 91.189.91.42
	uPOWBxniTA	Get hash	malicious	Browse	• 91.189.91.42
	qy5unieRgR	Get hash	malicious	Browse	• 91.189.91.42
	sAzPpn6mKZ	Get hash	malicious	Browse	• 91.189.91.42
	AxadDC89j9	Get hash	malicious	Browse	• 91.189.91.42
	ZErnXU2XR1	Get hash	malicious	Browse	• 91.189.91.42
GIGANET-HUGigaNetInternetServiceProviderCoHU	3tgXa7CGc1	Get hash	malicious	Browse	• 45.95.169.120
	rijsTqU0lf	Get hash	malicious	Browse	• 45.95.169.120
	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
INIT7CH	WXMAqjlcvg	Get hash	malicious	Browse	• 109.202.202.202
	3tgXa7CGc1	Get hash	malicious	Browse	• 109.202.202.202
	rijsTqU0lf	Get hash	malicious	Browse	• 109.202.202.202
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/tmp/qemu-open.6hO9oM (deleted)	
Process:	/tmp/qlmOM0y98B
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.75
Encrypted:	false
SSDEEP:	3:Tgowl:TgoQ
MD5:	CAE7C392B7851555C9DBF864483AB04F
SHA1:	84A9D88EE93B6802DE508FEAF538033842458EDE
SHA-256:	05A76277B50E280A830A7902624F7EC52E40FEBE76C3EEF017516565B5340117
SHA-512:	98777BED328806E599EFB3EC24A3B3C340508B5E6D04400DBE8F03AF1A24E80D943DF32CF9F479E5F67B9BFD4D2C5B7BEFC82411EB5F48E62EC749552334E99E
Malicious:	false
Reputation:	low
Preview:	/tmp/qlmOM0y98B.

/tmp/qemu-open.YxTKIM (deleted)	
Process:	/tmp/qlmOM0y98B
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.75
Encrypted:	false
SSDEEP:	3:Tgowl:TgoQ
MD5:	CAE7C392B7851555C9DBF864483AB04F
SHA1:	84A9D88EE93B6802DE508FEAF538033842458EDE
SHA-256:	05A76277B50E280A830A7902624F7EC52E40FEBE76C3EEF017516565B5340117
SHA-512:	98777BED328806E599EFB3EC24A3B3C340508B5E6D04400DBE8F03AF1A24E80D943DF32CF9F479E5F67B9BFD4D2C5B7BEFC82411EB5F48E62EC749552334E99E
Malicious:	false
Reputation:	low
Preview:	/tmp/qlmOM0y98B.

/tmp/qemu-open.a4xBGL (deleted)	
Process:	/tmp/qlmOM0y98B
File Type:	ASCII text, with no line terminators
Category:	dropped

/tmp/qemu-open.a4xBGL (deleted)	
Size (bytes):	16
Entropy (8bit):	3.75
Encrypted:	false
SSDEEP:	3:Tgowl:TgoQ
MD5:	CAE7C392B7851555C9DBF864483AB04F
SHA1:	84A9D88EE93B6802DE508FEAF538033842458EDE
SHA-256:	05A76277B50E280A830A7902624F7EC52E40FEBE76C3EEF017516565B5340117
SHA-512:	98777BED328806E599EFB3EC24A3B3C340508B5E6D04400DBE8F03AF1A24E80D943DF32CF9F479E5F67B9BFD4D2C5B7BEFC82411EB5F48E62EC749552334E99E
Malicious:	false
Reputation:	low
Preview:	/tmp/qlmOM0y98B.

/tmp/qemu-open.cTqsEP (deleted)	
Process:	/tmp/qlmOM0y98B
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.75
Encrypted:	false
SSDEEP:	3:Tgowl:TgoQ
MD5:	CAE7C392B7851555C9DBF864483AB04F
SHA1:	84A9D88EE93B6802DE508FEAF538033842458EDE
SHA-256:	05A76277B50E280A830A7902624F7EC52E40FEBE76C3EEF017516565B5340117
SHA-512:	98777BED328806E599EFB3EC24A3B3C340508B5E6D04400DBE8F03AF1A24E80D943DF32CF9F479E5F67B9BFD4D2C5B7BEFC82411EB5F48E62EC749552334E99E
Malicious:	false
Reputation:	low
Preview:	/tmp/qlmOM0y98B.

Static File Info

General

File type:	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.199094302349671
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	qlmOM0y98B
File size:	35320
MD5:	6c982efa63458b428ed98b6f2fa70165
SHA1:	199fd3f587ed36e207696f3642986bd508dc0839
SHA256:	1b20443752270cfe8fcd3f4d21ca7fbb9094e150d1b508826eaf1a454280d40b
SHA512:	73c07c0aeec003579fa0784f907e85a0db89cb4197b7565a99ad08fa463b9e8ffc789f6426f1ed73e4284bffc6587cbfd82262f3762274f102acde9e62cc00c8
SSDEEP:	384:I391PeYMJpZr3ZMrnk8VcAUpNTMOfQYQkmxgAqFP1lhlKTnaNOOHtNNDmV3azu:e9hmXrck86AUYnY3c2NzNNNDa
File Content Preview:	.ELF.....4.....4. ...(.....s...s.....s...s...s.....%`.....dt.Q.....!..|.....$H...H.l=...$8!. |...N.. .!..|.....?.....8.../...@..\?.....s..+../...A..$8...})....s.N..

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1

ELF header

Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x100001f0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	34840
Section Header Size:	40
Number of Section Headers:	12
Header String Table Index:	11

Sections

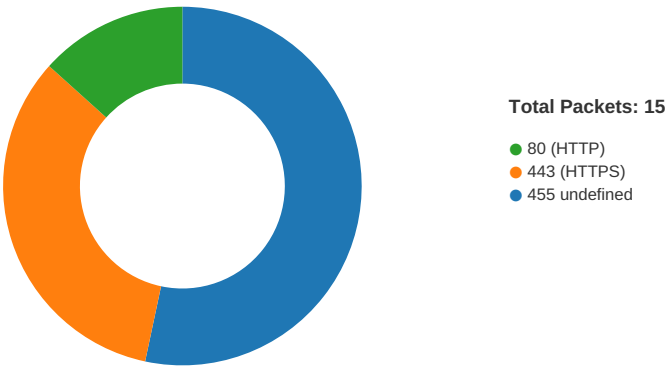
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100000b8	0xb8	0x6c94	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x10006d4c	0x6d4c	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x10006d6c	0x6d6c	0x670	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x100173e0	0x73e0	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x100173e8	0x73e8	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x100173f8	0x73f8	0x13ac	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x100187a4	0x87a4	0x28	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x100187cc	0x87cc	0x6c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x10018838	0x87cc	0x1108	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x87cc	0x4b	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	0x10000000	0x10000000	0x73dc	0x73dc	3.9857	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x73e0	0x100173e0	0x100173e0	0x13ec	0x2560	1.7661	0x6	RW	0x10000		.ctors .dtors .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: qlmOM0y98B PID: 5241 Parent PID: 5117

General

Start time:	09:53:18
Start date:	29/10/2021
Path:	/tmp/qlmOM0y98B
Arguments:	/tmp/qlmOM0y98B
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: qlmOM0y98B PID: 5243 Parent PID: 5241

General

Start time:	09:53:18
Start date:	29/10/2021
Path:	/tmp/qlmOM0y98B
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: qlmOM0y98B PID: 5245 Parent PID: 5243

General

Start time:	09:53:18
Start date:	29/10/2021
Path:	/tmp/qlmOM0y98B
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Deleted

File Read

File Written

Directory Enumerated