ID: 491781
Sample Name: CTKpl4Eflw
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 22:13:21
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

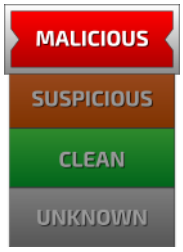
Linux Analysis Report CTKpl4Eflw

Overview

General Information

Sample Name:	CTKpl4Eflw
Analysis ID:	491781
MD5:	abee54d0880d98..
SHA1:	b25744cdc5d79b..
SHA256:	a8e150eebb41bfb.
Tags:	32 arm elf mirai
Infos:	

Detection

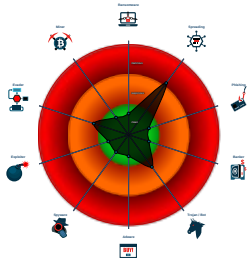


Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Opens /proc/net/* files useful for find…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…

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:	33.0.0 White Diamond
Analysis ID:	491781
Start date:	27.09.2021
Start time:	22:13:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CTKpl4Eflw
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:	mal60.spre.lin@0/0@0/0

Process Tree

- **system is lnxubuntu20**
  - CTKpl4Eflw (PID: 5226, Parent: 5109, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/CTKpl4Eflw
    - CTKpl4Eflw New Fork (PID: 5228, Parent: 5226)
    - CTKpl4Eflw New Fork (PID: 5230, Parent: 5226)
      - CTKpl4Eflw New Fork (PID: 5232, Parent: 5230)
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

- AV Detection
- Spreading
- Networking
- System Summary
- Malware Analysis System Evasion

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Spreading:

Opens /proc/net/* files useful for finding connected devices and routers

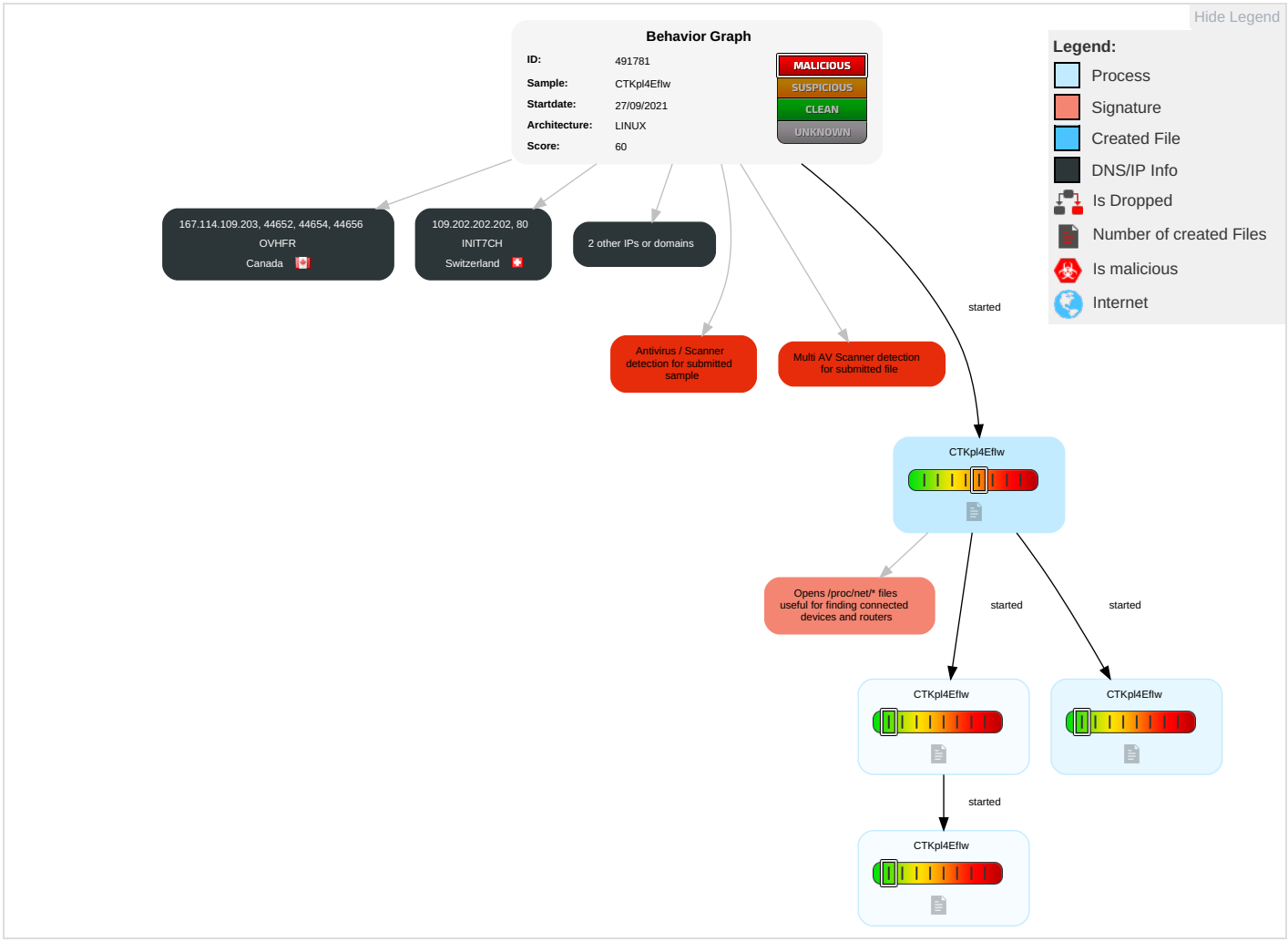
Mitre Att&ck Matrix

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	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 Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Remote System Discovery 1	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 Lockout
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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CTKpl4Eflw	38%	Virustotal		Browse
CTKpl4Eflw	44%	ReversingLabs	Linux.Trojan.Gafgyt	
CTKpl4Eflw	100%	Avira	LINUX/Gafgyt.opnd	

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
167.114.109.203	unknown	Canada		16276	OVHFR	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/CTKpl4Eflw
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	gosh that chinese family at the other table sure ate alot
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
167.114.109.203	imqksAx51T	Get hash	malicious	Browse	
	8eyaMuD9DY	Get hash	malicious	Browse	
	tnMrX1z0d5	Get hash	malicious	Browse	
	X86_64	Get hash	malicious	Browse	
109.202.202.202	imqksAx51T	Get hash	malicious	Browse	
	8eyaMuD9DY	Get hash	malicious	Browse	
	tnMrX1z0d5	Get hash	malicious	Browse	
	H3NaLv48NK	Get hash	malicious	Browse	
	i07CkTx8C4	Get hash	malicious	Browse	
	p22l26A3Wu	Get hash	malicious	Browse	
	fVNp9NC9l9	Get hash	malicious	Browse	
	wlJuLkUpqE	Get hash	malicious	Browse	
	cAoLg1WlGi	Get hash	malicious	Browse	
	77sa4X7MY2	Get hash	malicious	Browse	
	X86_64	Get hash	malicious	Browse	
	rrVvnZMcFs	Get hash	malicious	Browse	
	pAu4km62R9	Get hash	malicious	Browse	
	kUFNxyzq7h	Get hash	malicious	Browse	
	QMVi2eFA3O	Get hash	malicious	Browse	
	ZkoBOcJ402	Get hash	malicious	Browse	
	BPJoS4yXO5	Get hash	malicious	Browse	
	ryXG31Qpen	Get hash	malicious	Browse	
	V6nVmla0r8	Get hash	malicious	Browse	
	ETZr9gYnOG	Get hash	malicious	Browse	
91.189.91.43	imqksAx51T	Get hash	malicious	Browse	
	8eyaMuD9DY	Get hash	malicious	Browse	
	tnMrX1z0d5	Get hash	malicious	Browse	
	H3NaLv48NK	Get hash	malicious	Browse	
	i07CkTx8C4	Get hash	malicious	Browse	
	p22l26A3Wu	Get hash	malicious	Browse	
	fVNp9NC9l9	Get hash	malicious	Browse	
	wlJuLkUpqE	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cAoLg1WlGi	Get hash	malicious	Browse	
	77sa4X7MY2	Get hash	malicious	Browse	
	X86_64	Get hash	malicious	Browse	
	rrVvnZMcFs	Get hash	malicious	Browse	
	pAu4km62R9	Get hash	malicious	Browse	
	kUFNxyzq7h	Get hash	malicious	Browse	
	QMVi2eFA3O	Get hash	malicious	Browse	
	ZkoBOcJ402	Get hash	malicious	Browse	
	BPJoS4yXO5	Get hash	malicious	Browse	
	ryXG31Qpen	Get hash	malicious	Browse	
	V6nVmla0r8	Get hash	malicious	Browse	
	ETZr9gYnOG	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	imqksAx51T	Get hash	malicious	Browse	• 167.114.109.203
	8eyaMuD9DY	Get hash	malicious	Browse	• 167.114.109.203
	tnMrX1z0d5	Get hash	malicious	Browse	• 167.114.109.203
	X86_64	Get hash	malicious	Browse	• 167.114.109.203
	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 51.255.34.79
	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709212890.exe	Get hash	malicious	Browse	• 37.59.226.120
	ZFb3RmLJzo	Get hash	malicious	Browse	• 51.70.255.217
	Sht1aYGDIX	Get hash	malicious	Browse	• 51.178.244.189
	nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	Get hash	malicious	Browse	• 178.32.63.50
	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	Get hash	malicious	Browse	• 178.32.63.50
	Lrs8NGx6VM.exe	Get hash	malicious	Browse	• 164.132.171.176
	Claim-838392655-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111
	2PzMc3x4WP.exe	Get hash	malicious	Browse	• 87.98.153.120
	e5jVcbuCo5.exe	Get hash	malicious	Browse	• 176.31.32.199
	i7qUJCnMz0.exe	Get hash	malicious	Browse	• 176.31.32.199
	zsChlwJrkj.exe	Get hash	malicious	Browse	• 176.31.32.199
	claim.xls	Get hash	malicious	Browse	• 51.89.115.111
	9uHCz7MrjF.exe	Get hash	malicious	Browse	• 176.31.32.199
	J1IYv644YS.exe	Get hash	malicious	Browse	• 51.254.69.209
	b3astmode.arm7	Get hash	malicious	Browse	• 37.187.28.233
INIT7CH	imqksAx51T	Get hash	malicious	Browse	• 109.202.202.202
	8eyaMuD9DY	Get hash	malicious	Browse	• 109.202.202.202
	tnMrX1z0d5	Get hash	malicious	Browse	• 109.202.202.202
	H3NaLv48NK	Get hash	malicious	Browse	• 109.202.202.202
	i07CkTx8C4	Get hash	malicious	Browse	• 109.202.202.202
	p22l26A3Wu	Get hash	malicious	Browse	• 109.202.202.202
	fVNp9NC9l9	Get hash	malicious	Browse	• 109.202.202.202
	wlJuLkUpqE	Get hash	malicious	Browse	• 109.202.202.202
	cAoLg1WlGi	Get hash	malicious	Browse	• 109.202.202.202
	77sa4X7MY2	Get hash	malicious	Browse	• 109.202.202.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	X86_64	Get hash	malicious	Browse	• 109.202.202.202
	rrVvnZMcFs	Get hash	malicious	Browse	• 109.202.202.202
	pAu4km62R9	Get hash	malicious	Browse	• 109.202.202.202
	kUFNxyzq7h	Get hash	malicious	Browse	• 109.202.202.202
	QMVi2eFA3O	Get hash	malicious	Browse	• 109.202.202.202
	ZkoBOcJ402	Get hash	malicious	Browse	• 109.202.202.202
	BPJoS4yXO5	Get hash	malicious	Browse	• 109.202.202.202
	ryXG31Qpen	Get hash	malicious	Browse	• 109.202.202.202
	V6nVmla0r8	Get hash	malicious	Browse	• 109.202.202.202
	ETZr9gYnOG	Get hash	malicious	Browse	• 109.202.202.202

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.019182865076585
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	CTKpl4Eflw
File size:	90612
MD5:	abee54d0880d98307d664c8a12d060d2
SHA1:	b25744cdc5d79b96b601161da0a358c8325c381e
SHA256:	a8e150eebb41bfbb84f75ba3c3bc0662219ca3271af960b9f37b5f532d601f71
SHA512:	37a029df1dbffebf79a9d490b2f619e59b38c365de6b6685dd80b5fa4be3285ff635ad153437d1ae1ccaed397f6f170ed1c1e938c5b9ce5e57dc180abf7b4484
SSDEEP:	1536:dmjnaOU7w+N62KBfISGHFxBpqRP/1yoQt/NeOCOlCvV4bb:7OR+N62w5GHFERPcFNerKbb
File Content Preview:	.ELF...a.....(.....4...._.....4. ...(.....L...L.....P...P...P.....h.....Q.td.....-...L."....H.....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

ELF header

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:	90092
Section Header Size:	40
Number of Section Headers:	13
Header String Table Index:	12

Sections

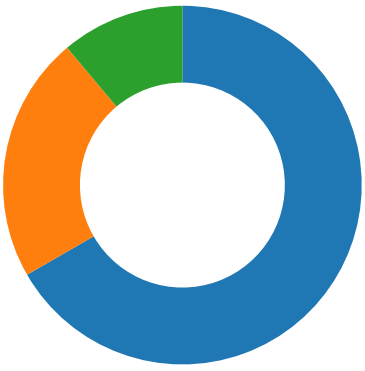
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x1235c	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x1a40c	0x1240c	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1a420	0x12420	0x2868	0x0	0x2	A	0	0	4
.eh_frame	PROGBITS	0x1cc88	0x14c88	0x4	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x25000	0x15000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x25008	0x15008	0x8	0x0	0x3	WA	0	0	4
.jcr	PROGBITS	0x25010	0x15010	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x25014	0x15014	0x3ac	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x253c0	0x153c0	0x6458	0x0	0x3	WA	0	0	4
.comment	PROGBITS	0x0	0x153c0	0xbd4	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x15f94	0x56	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	0x14c8c	0x14c8c	3.5346	0x5	R E	0x8000		.init .text .fini .rodata .eh_frame
LOAD	0x15000	0x25000	0x25000	0x3c0	0x6818	1.6527	0x6	RW	0x8000		.ctors .dtors .jcr .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



Total Packets: 18

- 80 (HTTP)
- 443 (HTTPS)
- 6525 undefined

TCP Packets

System Behavior

Analysis Process: CTKpl4Eflw PID: 5226 Parent PID: 5109

General

Start time:	22:14:04
Start date:	27/09/2021
Path:	/tmp/CTKpl4Eflw
Arguments:	/tmp/CTKpl4Eflw
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: CTKpl4Eflw PID: 5228 Parent PID: 5226

General

Start time:	22:14:04
Start date:	27/09/2021
Path:	/tmp/CTKpl4Eflw
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: CTKpl4Eflw PID: 5230 Parent PID: 5226

General

Start time:	22:14:04
Start date:	27/09/2021
Path:	/tmp/CTKpl4Eflw
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: CTKpl4Eflw PID: 5232 Parent PID: 5230

General

Start time:	22:14:04
Start date:	27/09/2021
Path:	/tmp/CTKpl4Eflw
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1