ID: 511517
Sample Name: Y4W4j5QIqD
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 08:58:22
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

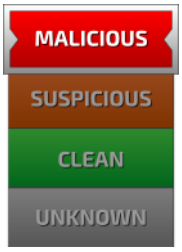
Linux Analysis Report Y4W4j5QIqD

Overview

General Information

Sample Name:	Y4W4j5QIqD
Analysis ID:	511517
MD5:	ab985a5aa90254..
SHA1:	380b0e55c98f46e.
SHA256:	871fd4ce9a1123e.
Tags:	32 elf motorola
Infos:	

Detection

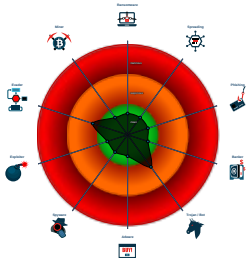


Score:	48
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample has stripped symbol table

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:	511517
Start date:	29.10.2021
Start time:	08:58:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Y4W4j5QIqD
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@0/0@0/0

Process Tree

- **system is lnxubuntu20**
  - Y4W4j5QIqD (PID: 5228, Parent: 5114, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/Y4W4j5QIqD
    - Y4W4j5QIqD New Fork (PID: 5230, Parent: 5228)
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

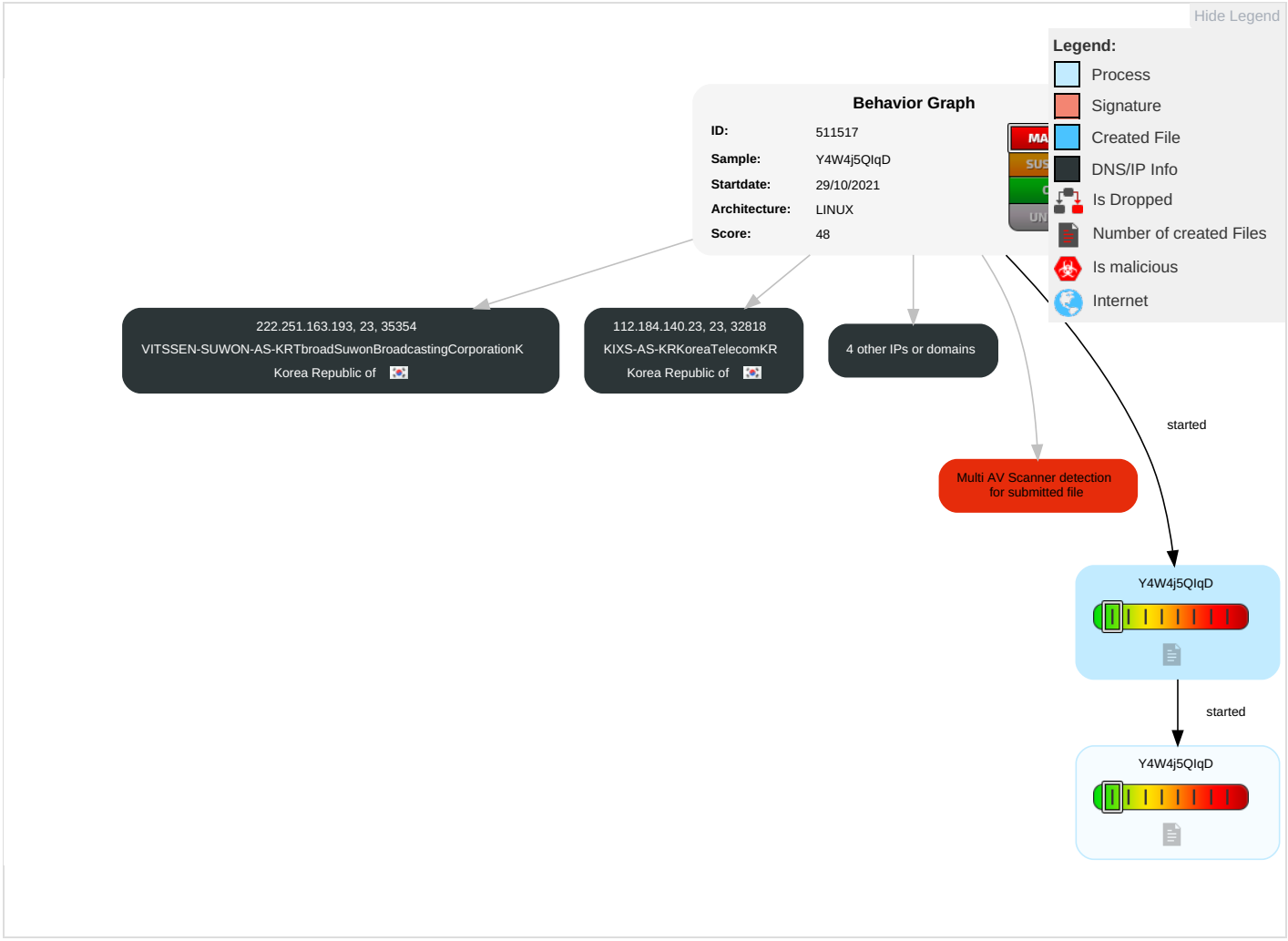
Mitre Att&ck Matrix

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	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	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 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
Y4W4j5QlqD	20%	Virustotal		Browse
Y4W4j5QlqD	14%	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
222.251.163.193	unknown	Korea Republic of		23563	VITSSEN-SUWON-AS-KRTbroadSuwonBroadcastingCorporationK	false
45.95.169.120	unknown	Croatia (LOCAL Name: Hrvatska)		42864	GIGANET-HUGigaNetInternetServiceProviderCoHU	false
112.184.140.23	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	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/Y4W4j5QIqD
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	1TnmkstVG8	Get hash	malicious	Browse	
	iksM5QEg2j	Get hash	malicious	Browse	
109.202.202.202	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	
	xjmPNreY8I	Get hash	malicious	Browse	
91.189.91.43	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	xjmPNreY8I	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VITSSEN-SUWON-AS-KRTbroadSuwonBroadcastingCorporationK	1alzsODTFe	Get hash	malicious	Browse	• 218.209.212.14
	notabotnet.x86	Get hash	malicious	Browse	• 121.254.0.118
	7EY5YH1w9q	Get hash	malicious	Browse	• 222.251.160.6
	dark.86_64	Get hash	malicious	Browse	• 114.108.48.64
	2YrqtABAvt	Get hash	malicious	Browse	• 218.209.89.138
	hoho.x86	Get hash	malicious	Browse	• 114.108.48.79
	1isequal9.x86	Get hash	malicious	Browse	• 222.251.255.72
	S6DNzkh376	Get hash	malicious	Browse	• 114.108.48.35
	1isequal9.x86	Get hash	malicious	Browse	• 121.254.0.152
	WCBzD1NEZs	Get hash	malicious	Browse	• 114.108.24.66
	cUfweIWt2x	Get hash	malicious	Browse	• 114.108.12.62
	VGi1EK6T17	Get hash	malicious	Browse	• 121.254.0.152
	SecuriteInfo.com.Trojan.Kronos.21.31435.exe	Get hash	malicious	Browse	• 114.108.58.201
	6d0000.exe	Get hash	malicious	Browse	• 114.108.58.201
	mssecsvc.exe	Get hash	malicious	Browse	• 218.209.174.90
GIGANET-HUGigaNetInternetServiceProviderCoHU	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
	LIE7nUUjmA	Get hash	malicious	Browse	• 45.95.169.115
	3HwsuWd7at	Get hash	malicious	Browse	• 45.95.169.115
KIXS-AS-KRKoreaTelecomKR	BsNj9o1U0P.exe	Get hash	malicious	Browse	• 211.229.47.232
	rdvL5Vuyg7.exe	Get hash	malicious	Browse	• 203.228.9.102
	AY5uCs0HrY.exe	Get hash	malicious	Browse	• 121.136.102.4
	9JVjZ8tdvF.exe	Get hash	malicious	Browse	• 121.136.102.4
	LCgNoeCOl6	Get hash	malicious	Browse	• 121.145.18 7.125
	RgHOcm1miq.exe	Get hash	malicious	Browse	• 220.125.1.129
	3D6Ztnqg66.exe	Get hash	malicious	Browse	• 203.228.9.102
	wannacry.exe	Get hash	malicious	Browse	• 175.211.53.106

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#202110223.exe	Get hash	malicious	Browse	• 183.111.242.26
	st2AAeCXsR	Get hash	malicious	Browse	• 119.196.59.40
	bKHI9UT0D1	Get hash	malicious	Browse	• 59.1.165.25
	1S80No4PTV	Get hash	malicious	Browse	• 112.160.41.41
	eNrYzJWFvB	Get hash	malicious	Browse	• 210.183.92.150
	pLoEhdXNms.exe	Get hash	malicious	Browse	• 14.51.96.70
	XTLR18yv0F.exe	Get hash	malicious	Browse	• 121.136.102.4
	mdOr6C8jJp	Get hash	malicious	Browse	• 59.22.201.202
	en94piXmL6	Get hash	malicious	Browse	• 210.179.35.113
	wRmHCEnowI	Get hash	malicious	Browse	• 118.49.17.164
	5BfhgIXvAy	Get hash	malicious	Browse	• 119.205.33.74
	HCyigyiCAH	Get hash	malicious	Browse	• 125.145.13 5.186

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 MSB executable, Motorola m68k, 68020, v ersion 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.256461527210843
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Y4W4j5QIqD
File size:	31984
MD5:	ab985a5aa9025467417c596d55665616
SHA1:	380b0e55c98f46ea5bcfe251f6e827bb9eccc168
SHA256:	871fd4ce9a1123ea4c4846d97d5f547eb29357871bdfedc 3a1de5b621189d9f6
SHA512:	c15924a116409293864bebedc1f8ac32c0606da57a3a88 41dbdd1181ca4f22fec04876c6164ed3f11d695eb78199d d7cd56a95ebf767e6ae2e8ad567152770fa
SSDEEP:	384:+pKH2Vg4Y3sPfMYHdJ8HASC4xv/Hsh+mUH90E V4JZBIA:mmZ38fPH8dx84mUdxV4JAA
File Content Preview:	.ELF.....D...4..{`.....4. ...(.....g>..g>. ....gD...D...D.....!|..... .dt.Q.....NV..a. ...da...atN^NuNV..J9... f>"y...\ QJ.g.X.#....\N."y...\ QJ.f.A. ....J.g.Hy..g@N.X..... N^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0

ELF header

Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	31584
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

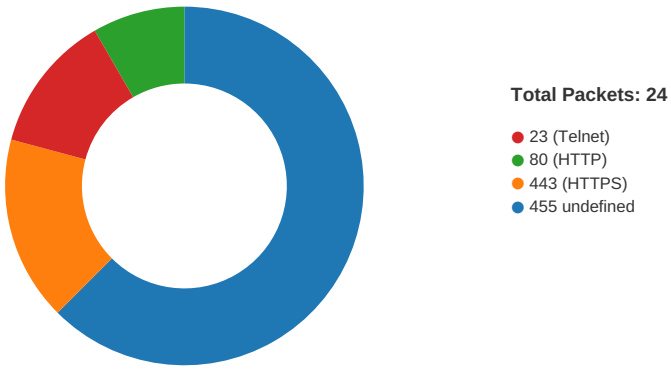
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0x619e	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x80006246	0x6246	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x80006254	0x6254	0x4ea	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x80008744	0x6744	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8000874c	0x674c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80008758	0x6758	0x13c8	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80009b20	0x7b20	0xda0	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x7b20	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	0x80000000	0x80000000	0x673e	0x673e	3.9126	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x6744	0x80008744	0x80008744	0x13dc	0x217c	1.7414	0x6	RW	0x2000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: Y4W4j5QIqD PID: 5228 Parent PID: 5114

General

Start time:	08:59:02
Start date:	29/10/2021
Path:	/tmp/Y4W4j5QIqD
Arguments:	/tmp/Y4W4j5QIqD
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: Y4W4j5QIqD PID: 5230 Parent PID: 5228

General

Start time:	08:59:02
Start date:	29/10/2021
Path:	/tmp/Y4W4j5QIqD
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc