ID: 491751
Sample Name: X86_64
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:14:51
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

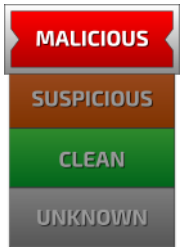
Linux Analysis Report X86_64

Overview

General Information

Sample Name:	X86_64
Analysis ID:	491751
MD5:	28007c7ac1c6c2…
SHA1:	ac64ad6324ac4c…
SHA256:	5fa70a36cc2ac68..
Tags:	elf mirai
Infos:	

Detection

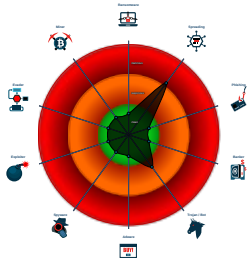


Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Opens /proc/net/* files useful for find…
- Machine Learning detection for samp…
- 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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491751
Start date:	27.09.2021
Start time:	21:14:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	X86_64
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:	mal56.spre.lin@0/0@0/0

Process Tree

- **system is lnxubuntu20**
- X86_64 (PID: 5223, Parent: 5110, MD5: 28007c7ac1c6c2880279aeaab2c25f17) Arguments: /tmp/X86_64
  - X86_64 New Fork (PID: 5224, Parent: 5223)
  - X86_64 New Fork (PID: 5225, Parent: 5223)
    - X86_64 New Fork (PID: 5226, Parent: 5225)
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

AV Detection
Spreading
Networking
System Summary

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Spreading:

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

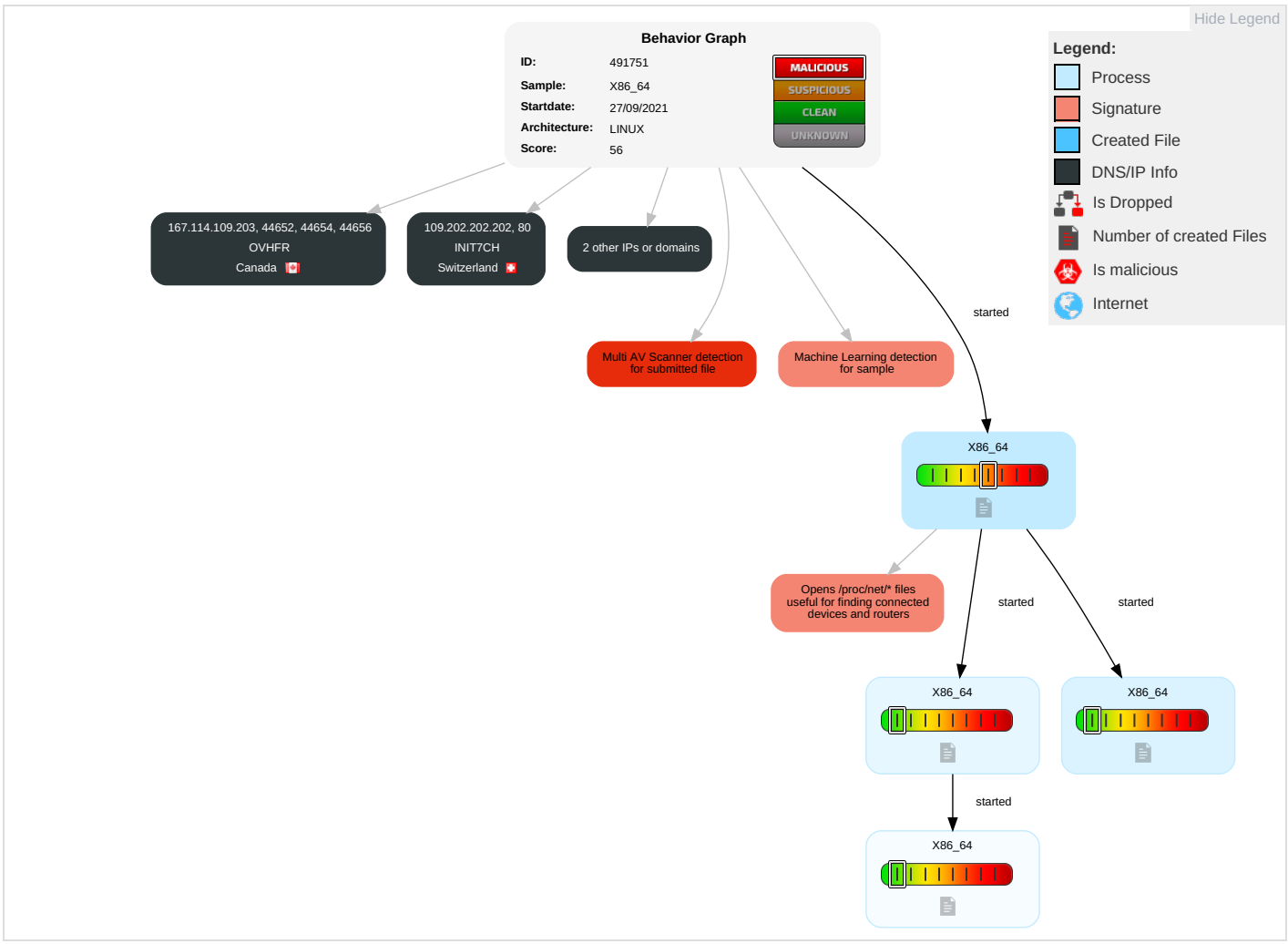
Mitre Att&ck Matrix

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	Remote System Discovery 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
X86_64	40%	Virustotal		Browse
X86_64	44%	ReversingLabs	Linux.Backdoor.Bashlite	
X86_64	100%	Joe Sandbox ML		

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/X86_64
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
109.202.202.202	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	
	wEA8Sws7Me	Get hash	malicious	Browse	
	AJ0ZSJ7K36	Get hash	malicious	Browse	
	fhPeao3t5X	Get hash	malicious	Browse	
	5ndmU5fZJW	Get hash	malicious	Browse	
	PoLc6KlROB	Get hash	malicious	Browse	
	1j9nlon8bL	Get hash	malicious	Browse	
	oBsSmO47B1	Get hash	malicious	Browse	
	r6c76MpUDj	Get hash	malicious	Browse	
	tHOi2INjNx	Get hash	malicious	Browse	
	D0kphZoxnr	Get hash	malicious	Browse	
	EL2beRAhLp	Get hash	malicious	Browse	
91.189.91.43	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	
	wEA8Sws7Me	Get hash	malicious	Browse	
	AJ0ZSJ7K36	Get hash	malicious	Browse	
	fhPeao3t5X	Get hash	malicious	Browse	
	5ndmU5fZJW	Get hash	malicious	Browse	
	PoLc6KlROB	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1j9nlon8bL	Get hash	malicious	Browse	
	oBsSmO47B1	Get hash	malicious	Browse	
	r6c76MpUDj	Get hash	malicious	Browse	
	tHOi2INjNx	Get hash	malicious	Browse	
	D0kphZoxnr	Get hash	malicious	Browse	
	EL2beRAhLp	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	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
	J7SOJRlEly.exe	Get hash	malicious	Browse	• 51.91.193.179
	SE6Hlp3GfE.exe	Get hash	malicious	Browse	• 176.31.32.199
	TxIlr8dCCJ.exe	Get hash	malicious	Browse	• 176.31.32.199
	xZqtlgwoWq.exe	Get hash	malicious	Browse	• 176.31.32.199

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.265443608550432
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	X86_64

General

File size:	81408
MD5:	28007c7ac1c6c2880279aeaab2c25f17
SHA1:	ac64ad6324ac4ccf079dfd4c8255d1cbf3175306
SHA256:	5fa70a36cc2ac68dfe216e4007848b7e90722a82acc7ca1778780b7393b3f735
SHA512:	d8b63bd73cd59f852723fdf58ea661a56bb1924746b8c4b0a9ca609cc02a532d51b3d51ccbcc798b6f734365377bbef1cf5bd706f7359f560386855ed14f7547
SSDEEP:	1536:aVnirf3qAhHvvX6YbESLAvM0gLVxoOOqjYum0Hi1pczCf3k:ahir3hPvX6YRcvapOqjXLC1pUCvk
File Content Preview:	.ELF.....>.....@.....@.....:.....@.8...@.....@.....@.....@.....*.....*.....*.....*Q.....*Q.....hr.....Q.td.....H.._.....H.....

Static ELF Info

ELF header

Class:	ELF64
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Advanced Micro Devices X86-64
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400194
Flags:	0x0
ELF Header Size:	64
Program Header Offset:	64
Program Header Size:	56
Number of Program Headers:	3
Section Header Offset:	80576
Section Header Size:	64
Number of Section Headers:	13
Header String Table Index:	12

Sections

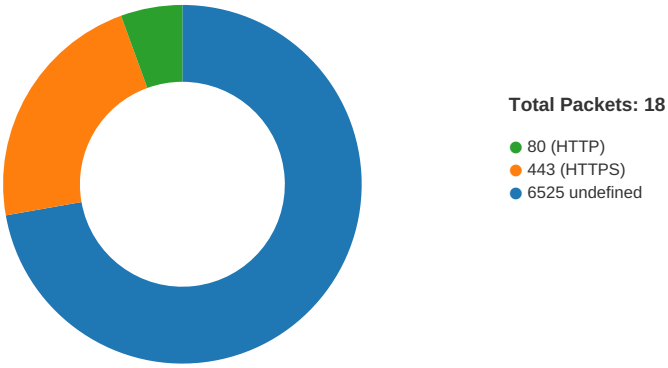
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x4000e8	0xe8	0x13	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x400100	0x100	0xf6b8	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x40f7b8	0xf7b8	0xe	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x40f7e0	0xf7e0	0x3220	0x0	0x2	A	0	0	32
.eh_frame	PROGBITS	0x412a00	0x12a00	0x4	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x512a08	0x12a08	0x10	0x0	0x3	WA	0	0	8
.dtors	PROGBITS	0x512a18	0x12a18	0x10	0x0	0x3	WA	0	0	8
.jcr	PROGBITS	0x512a28	0x12a28	0x8	0x0	0x3	WA	0	0	8
.data	PROGBITS	0x512a40	0x12a40	0x4d8	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x512f20	0x12f18	0x6d50	0x0	0x3	WA	0	0	32
.comment	PROGBITS	0x0	0x12f18	0xb52	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x13a6a	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	0x400000	0x400000	0x12a04	0x12a04	3.4215	0x5	R E	0x100000		.init .text .fini .rodata .eh_frame
LOAD	0x12a08	0x512a08	0x512a08	0x510	0x7268	1.3533	0x6	RW	0x100000		.ctors .dtors .jcr .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x8		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: X86_64 PID: 5223 Parent PID: 5110

General

Start time:	21:15:40
Start date:	27/09/2021
Path:	/tmp/X86_64
Arguments:	/tmp/X86_64
File size:	81408 bytes
MD5 hash:	28007c7ac1c6c2880279aeaab2c25f17

File Activities

File Read

Analysis Process: X86_64 PID: 5224 Parent PID: 5223

General

Start time:	21:15:41
Start date:	27/09/2021
Path:	/tmp/X86_64
Arguments:	n/a
File size:	81408 bytes
MD5 hash:	28007c7ac1c6c2880279aeaab2c25f17

Analysis Process: X86_64 PID: 5225 Parent PID: 5223

General

Start time:	21:15:41

Start date:	27/09/2021
Path:	/tmp/X86_64
Arguments:	n/a
File size:	81408 bytes
MD5 hash:	28007c7ac1c6c2880279aeaab2c25f17

Analysis Process: X86_64 PID: 5226 Parent PID: 5225

General

Start time:	21:15:41
Start date:	27/09/2021
Path:	/tmp/X86_64
Arguments:	n/a
File size:	81408 bytes
MD5 hash:	28007c7ac1c6c2880279aeaab2c25f17