ID: 491760
Sample Name: fVNp9NC9l9
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:33:29
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

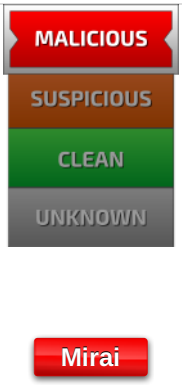
Linux Analysis Report fVNp9NC9l9

Overview

General Information

Sample Name:	fVNp9NC9l9
Analysis ID:	491760
MD5:	3ad11448f98fc08..
SHA1:	9c0d1819f9b9292.
SHA256:	40b4a8e91427b8..
Tags:	32 elf intel
Infos:	

Detection

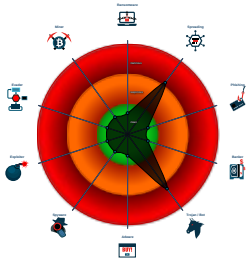


Score:	60
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Mirai
- Opens /proc/net/* files useful for find…
- Sample contains only a LOAD segm…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…

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:	491760
Start date:	27.09.2021
Start time:	21:33:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fVNp9NC9l9
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.troj.lin@0/0@0/0

Process Tree

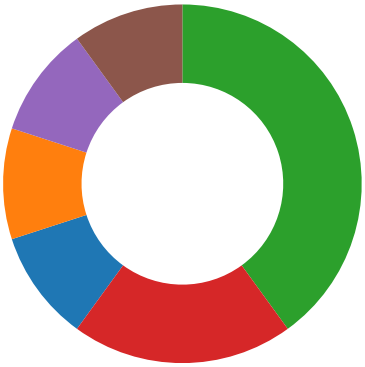
- **system is lnxubuntu20**
- fVNp9NC9l9 (PID: 5220, Parent: 5107, MD5: 3ad11448f98fc08e6c1107c4327ab97f) Arguments: /tmp/fVNp9NC9l9
  - fVNp9NC9l9 New Fork (PID: 5221, Parent: 5220)
    - fVNp9NC9l9 New Fork (PID: 5222, Parent: 5221)
- **cleanup**

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
5221.1.000000001a887bdc.00000000531557b5.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5220.1.000000001a887bdc.00000000531557b5.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Jbx Signature Overview



- AV Detection
- Spreading
- Networking
- System Summary
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Spreading:

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

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

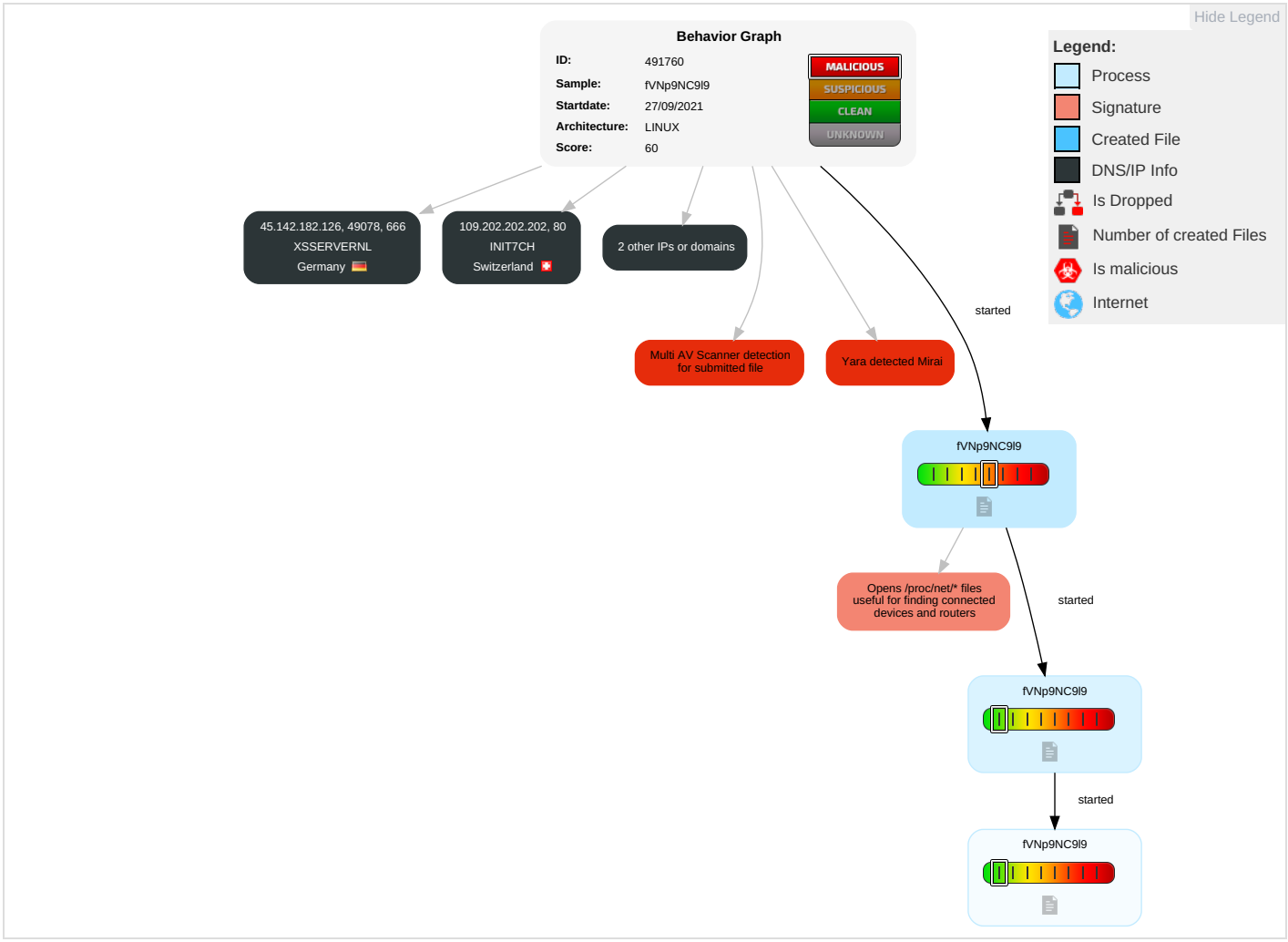
Mitre Att&ck Matrix

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
fVNp9NC9l9	28%	Virustotal		Browse
fVNp9NC9l9	46%	ReversingLabs	Linux.Trojan.Gafgyt	

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
45.142.182.126	unknown	Germany		207959	XSSERVERNL	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/fVNp9NC9l9
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
45.142.182.126	cAoLg1WlGi	Get hash	malicious	Browse	
109.202.202.202	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	
	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	
91.189.91.43	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
91.189.91.42	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	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CANONICAL-ASGB	wlJuLkUpqE	Get hash	malicious	Browse	• 91.189.91.42
	cAoLg1WlGi	Get hash	malicious	Browse	• 91.189.91.42
	77sa4X7MY2	Get hash	malicious	Browse	• 91.189.91.42
	X86_64	Get hash	malicious	Browse	• 91.189.91.42
	rrVvnZMcFs	Get hash	malicious	Browse	• 91.189.91.42
	pAu4km62R9	Get hash	malicious	Browse	• 91.189.91.42
	kUFNxyzq7h	Get hash	malicious	Browse	• 91.189.91.42
	QMVi2eFA3O	Get hash	malicious	Browse	• 91.189.91.42
	ZkoBOcJ402	Get hash	malicious	Browse	• 91.189.91.42
	BPJoS4yXO5	Get hash	malicious	Browse	• 91.189.91.42
	ryXG31Qpen	Get hash	malicious	Browse	• 91.189.91.42
	V6nVmla0r8	Get hash	malicious	Browse	• 91.189.91.42
	ETZr9gYnOG	Get hash	malicious	Browse	• 91.189.91.42
	wEA8Sws7Me	Get hash	malicious	Browse	• 91.189.91.42
	AJ0ZSJ7K36	Get hash	malicious	Browse	• 91.189.91.42
	fhPeao3t5X	Get hash	malicious	Browse	• 91.189.91.42
	5ndmU5fZJW	Get hash	malicious	Browse	• 91.189.91.42
	PoLc6KlROB	Get hash	malicious	Browse	• 91.189.91.42
	1j9nlon8bL	Get hash	malicious	Browse	• 91.189.91.42
	oBsSmO47B1	Get hash	malicious	Browse	• 91.189.91.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INIT7CH	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
	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
	wEA8Sws7Me	Get hash	malicious	Browse	• 109.202.202.202
	AJ0ZSJ7K36	Get hash	malicious	Browse	• 109.202.202.202
	fhPeao3t5X	Get hash	malicious	Browse	• 109.202.202.202
	5ndmU5fZJW	Get hash	malicious	Browse	• 109.202.202.202
	PoLc6KlROB	Get hash	malicious	Browse	• 109.202.202.202
	1j9nlon8bL	Get hash	malicious	Browse	• 109.202.202.202
	oBsSmO47B1	Get hash	malicious	Browse	• 109.202.202.202
XSSERVERNL	cAoLg1WlGi	Get hash	malicious	Browse	• 45.142.182.126
	FQp7hNtN.exe	Get hash	malicious	Browse	• 195.62.33.67
	http://https://waverpyramid.com/?email=carlos.machado.pereira@novobanco.pt	Get hash	malicious	Browse	• 195.62.46.177
	http://https://waverpyramid.com/?email=carlos.machado.pereira@novobanco.pt	Get hash	malicious	Browse	• 195.62.46.177
	http://https://tepe365-my.sharepoint.com/:b:/g/personal/bobbiewalden_workingenvironments_co_uk/EXJ3AG5SfktLpjPFRCFQUYwBsF4BUG6lJPv1ZdKpkhUsXg?e=4%3aMCOEiT&at=9	Get hash	malicious	Browse	• 195.62.46.180

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, Intel 80386, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.9515207570063025
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	fVNp9NC9l9
File size:	34108
MD5:	3ad11448f98fc08e6c1107c4327ab97f
SHA1:	9c0d1819f9b9292119560e21b8d2ff4c2f66316d
SHA256:	40b4a8e91427b81ee97fb43a56edce02dce93f88a6c55ac698c50693fb069f6b
SHA512:	ff879410a10cf41d7e6e36a53f03144bf86430e4da7f8601db78b370cb37e8a223aa2c415da1f526eaaf3ad412bccca daff49ea8e399ba2cf5d91545c507e070
SSDEEP:	768:eyIuM3Lc1tCjtmSPI6QfSxDBY1T0B1Ki9VVDkekKnnbcuyD7UryqK:Rm3Lc/Cjfya9BYV81Ki9HASnouy8mqK
File Content Preview:	.ELF.....P...4.....4. ...(.....D...D.....).....Q.td.....4.IYTS.....T...T.....U.....?..k.I/.j....\.d*nlz.ed..8.H.....{....Ax..m.....M..w.f1...F.$v.C.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x804f250
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

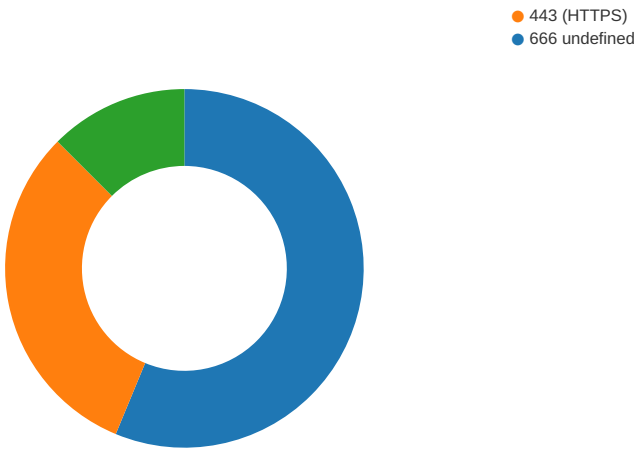
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x8444	0x8444	4.0868	0x5	R E	0x1000		
LOAD	0x0	0x8051000	0x8051000	0x0	0x129e4	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution

Total Packets: 16

- 80 (HTTP)



TCP Packets

System Behavior

Analysis Process: fVNp9NC9l9 PID: 5220 Parent PID: 5107

General

Start time:	21:34:09
Start date:	27/09/2021
Path:	/tmp/fVNp9NC9l9
Arguments:	/tmp/fVNp9NC9l9
File size:	34108 bytes
MD5 hash:	3ad11448f98fc08e6c1107c4327ab97f

File Activities

File Read

Analysis Process: fVNp9NC9l9 PID: 5221 Parent PID: 5220

General

Start time:	21:34:10
Start date:	27/09/2021
Path:	/tmp/fVNp9NC9l9
Arguments:	n/a
File size:	34108 bytes
MD5 hash:	3ad11448f98fc08e6c1107c4327ab97f

Analysis Process: fVNp9NC9l9 PID: 5222 Parent PID: 5221

General

Start time:	21:34:10
Start date:	27/09/2021
Path:	/tmp/fVNp9NC9l9

Arguments:	n/a
File size:	34108 bytes
MD5 hash:	3ad11448f98fc08e6c1107c4327ab97f