ID: 452446
Sample Name: VVrYWZ9mzZ
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:21:56
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

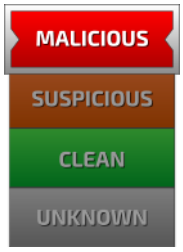
Linux Analysis Report VVrYWZ9mzZ

Overview

General Information

Sample Name:	VVrYWZ9mzZ
Analysis ID:	452446
MD5:	28ae443f54fdb93..
SHA1:	61c196c94b176f7..
SHA256:	e00e03516a774d..
Tags:	32 arm elf mirai
Infos:	

Detection

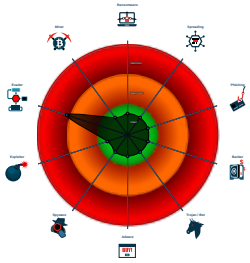


Score:	52
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Sample contains only a LOAD segm…
- Uses the "uname" system call to qu…

Classification



Analysis Advice

Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

Static ELF header machine description suggests that the sample might not execute correctly on this machine

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452446
Start date:	22.07.2021
Start time:	11:21:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VVrYWZ9mzZ
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 16.04 x64 (Kernel 4.4.0-116, Firefox 59.0, Document Viewer 3.18.2, LibreOffice 5.1.6.2, OpenJDK 1.8.0_171)
Analysis Mode:	default
Detection:	MAL
Classification:	mal52.evad.lin@0/0@0/0

Process Tree

- **system is lnxubuntu1**
  - VVrYWZ9mzZ (PID: 4594, Parent: 4519, MD5: 28ae443f54fdb93adc756778ad76ef90) Arguments: /usr/bin/qemu-arm /tmp/VVrYWZ9mzZ
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Data Obfuscation:

Sample is packed with UPX

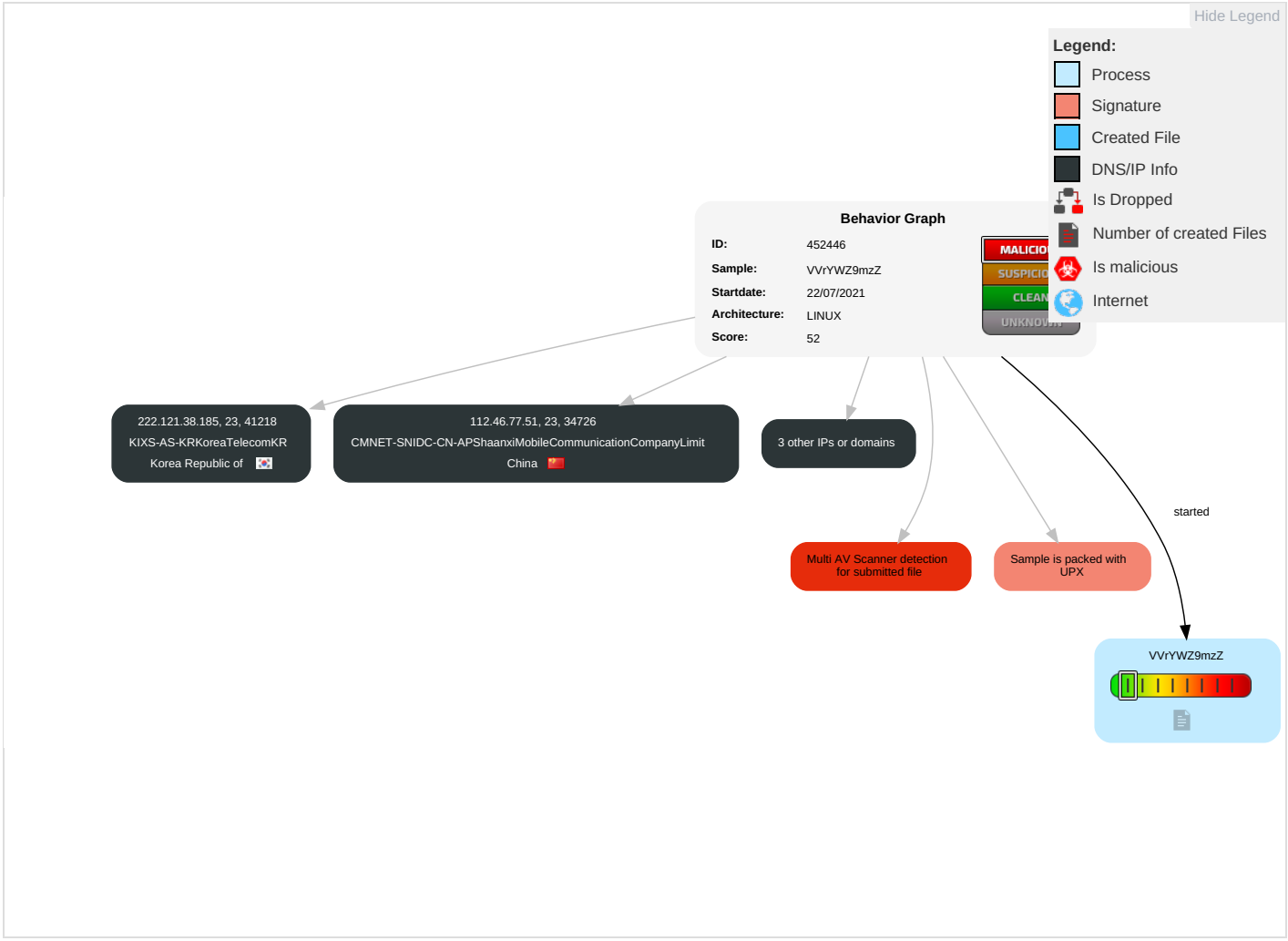
Mitre Att&ck Matrix

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	Obfuscated Files or Information 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
VVrYWZ9mzZ	26%	Virustotal		Browse
VVrYWZ9mzZ	33%	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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
97.102.228.248	unknown	United States		33363	BHN-33363US	false
112.46.77.51	unknown	China		140105	CMNET-SNIDC-CN-APShaanxiMobileCommunicationCompanyLimit	false
223.100.19.169	unknown	China		56044	CMNET-AS-LIAONINGChinaMobilecommunicationscorporationC	false
222.121.38.185	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
117.175.152.205	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false

Runtime Messages

Command:	/tmp/VVrYWZ9mzZ
Exit Code:	127
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BHN-33363US	sDwNKSpuhB	Get hash	malicious	Browse	• 72.31.223.26
	C4PozjQdGE	Get hash	malicious	Browse	• 72.187.13.255
	MD5OxTSc6i	Get hash	malicious	Browse	• 68.204.245.64
	AUFFFNSdKy	Get hash	malicious	Browse	• 68.205.212.145
	yZEHOt8K7X	Get hash	malicious	Browse	• 68.204.182.199
	ehn0f1d63M	Get hash	malicious	Browse	• 72.40.237.94
	v6clgzEGCb	Get hash	malicious	Browse	• 24.73.130.42
	dFwlxBbz2d	Get hash	malicious	Browse	• 97.103.226.137
	FawDB415Y0	Get hash	malicious	Browse	• 97.102.236.202
	395d6gwkWK	Get hash	malicious	Browse	• 71.43.252.141
	Xlojlgo2gb	Get hash	malicious	Browse	• 65.32.66.174
	b8oaj84zgz	Get hash	malicious	Browse	• 97.79.111.176
	Z7bNxhhS7y	Get hash	malicious	Browse	• 97.103.226.166
	AT9n7Bk0yE	Get hash	malicious	Browse	• 68.207.139.146
	PX7gd73hY6	Get hash	malicious	Browse	• 72.187.36.79
	khGshuibcr	Get hash	malicious	Browse	• 173.169.182.6
	qiJTsutSGd	Get hash	malicious	Browse	• 173.169.63.242
	Rb5g620lnp	Get hash	malicious	Browse	• 35.139.26.91
	DpuO7oic9y.exe	Get hash	malicious	Browse	• 142.196.11 8.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	boI88C399w.exe	Get hash	malicious	Browse	• 50.91.114.38
CMNET-AS-LIAONINGChinaMobilecommunicationscorporationC	Vk3A1yJJMg	Get hash	malicious	Browse	• 112.42.114.1
	jEbpttXKCa	Get hash	malicious	Browse	• 36.137.134.204
	Vs7Vm7J1TR	Get hash	malicious	Browse	• 39.135.127.180
	Af1Fnq4l4G	Get hash	malicious	Browse	• 36.132.150.41
	AT9n7Bk0yE	Get hash	malicious	Browse	• 112.41.179.126
	Rb5g620lnp	Get hash	malicious	Browse	• 39.153.45.252
	wEcncyxrEe	Get hash	malicious	Browse	• 36.128.104.41
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 39.152.130.11
KIXS-AS-KRKoreaTelecomKR	RzBo7FFhaM	Get hash	malicious	Browse	• 110.71.105.232
	d8dgn3wGJL	Get hash	malicious	Browse	• 175.252.45.55
	s54l0GKMh9	Get hash	malicious	Browse	• 183.105.180.39
	z0FwvGSnDF	Get hash	malicious	Browse	• 121.134.140.247
	D1dU3jQ1Il	Get hash	malicious	Browse	• 218.158.241.237
	RsEvjl1iTt.exe	Get hash	malicious	Browse	• 121.136.102.4
	A7X93JRxhp	Get hash	malicious	Browse	• 125.137.150.28
	8ZJ0cPowTy	Get hash	malicious	Browse	• 119.215.188.3
	92CRMNlBq8	Get hash	malicious	Browse	• 183.126.251.85
	XuQRPW44hi	Get hash	malicious	Browse	• 121.170.47.64
	Taf5zLti30	Get hash	malicious	Browse	• 175.198.110.50
	5qpsqg7U0G	Get hash	malicious	Browse	• 175.239.252.125
	U5q75RGCmQ	Get hash	malicious	Browse	• 222.96.223.234
	oEF7GAiRIg	Get hash	malicious	Browse	• 121.145.187.107
	GEso3CniSk	Get hash	malicious	Browse	• 121.177.185.16
	BTNNG17tlh	Get hash	malicious	Browse	• 121.152.147.6
	bPAMfuy9oa	Get hash	malicious	Browse	• 121.177.185.53
	apep.mips	Get hash	malicious	Browse	• 121.170.84.41
	CefN2XNyFi	Get hash	malicious	Browse	• 119.193.74.164
	7OAzOUL9cd	Get hash	malicious	Browse	• 118.41.209.66

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):	7.917436227483886
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	VVrYWZ9mzZ
File size:	22132
MD5:	28ae443f54fdb93adc756778ad76ef90
SHA1:	61c196c94b176f71a5748e5910c9db9c03927e9e
SHA256:	e00e03516a774d45197cbeac2e89b5d9a4df7849b6fd19e360ee72619ab6311d

General	
SHA512:	889bf93b674a86fd49f4fd9e06959272d553930cb623914b4babfddba66d5fca1c3baa41eb36c6ff4125a583042a88d9f122c70b441dd543f73550321a23498b
SSDEEP:	384:YAmog4c6L5i4+stlW01vhQIE2TQKMpI8QwxZVFjfPnSb9khymdGUop5hX0:Ypoh/DxCvhdR4IjWVFbSKs3UozJ0
File Content Preview:	.ELF...a.....(.....P...4.....4. ...(.....T...T.....?.....Q.td.....CvUPX!.....X...X.....q.....?.E.h;.}...^.....+P.f.qY@.....}6N.h.....X...|.?..E(...p....h..]

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0xc350
Flags:	0x2
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	0x8000	0x8000	0x54ff	0x54ff	4.0354	0x5	R E	0x8000		
LOAD	0x3fb0	0x1bfb0	0x1bfb0	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

TCP Packets

System Behavior

Analysis Process: VVrYWZ9mzZ PID: 4594 Parent PID: 4519

General

Start time:	11:22:28
Start date:	22/07/2021
Path:	/tmp/VVrYWZ9mzZ
Arguments:	/usr/bin/qemu-arm /tmp/VVrYWZ9mzZ
File size:	22132 bytes
MD5 hash:	28ae443f54fdb93adc756778ad76ef90

File Activities

File Read