

JOeSandbox Cloud BASIC



**ID:** 553488

**Sample Name:** gsf3z44v5s

**Cookbook:**

defaultlinuxfilecookbook.jbs

**Time:** 01:18:21

**Date:** 15/01/2022

**Version:** 34.0.0 Boulder Opal

## Table of Contents

Table of Contents	2
Linux Analysis Report gsf3z44v5s	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Analysis Advice	3
General Information	3
Process Tree	3
Yara Overview	4
Jbx Signature Overview	4
AV Detection:	4
Data Obfuscation:	4
Mitre Att&ck Matrix	4
Malware Configuration	4
Behavior Graph	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Domains	5
URLs	5
Domains and IPs	5
Contacted Domains	5
URLs from Memory and Binaries	5
Contacted IPs	6
Public	6
Runtime Messages	6
Joe Sandbox View / Context	6
IPs	6
Domains	6
ASN	6
JA3 Fingerprints	6
Dropped Files	6
Created / dropped Files	6
Static File Info	6
General	7
Static ELF Info	7
ELF header	7
Program Segments	7
Network Behavior	7
Network Port Distribution	7
TCP Packets	8
System Behavior	8
Analysis Process: gsf3z44v5s PID: 5212 Parent PID: 5110	8
General	8
File Activities	8
File Read	8
Analysis Process: dash PID: 5253 Parent PID: 4331	8
General	8
Analysis Process: rm PID: 5253 Parent PID: 4331	8
General	8
File Activities	9
File Deleted	9
File Read	9

# Linux Analysis Report gsf3z44v5s

## Overview

### General Information

Sample Name:	gsf3z44v5s
Analysis ID:	553488
MD5:	5502094e79b489..
SHA1:	3faad8451da16e6.
SHA256:	6f5dde695a158e.
Tags:	32 arm elf mirai
Infos:	

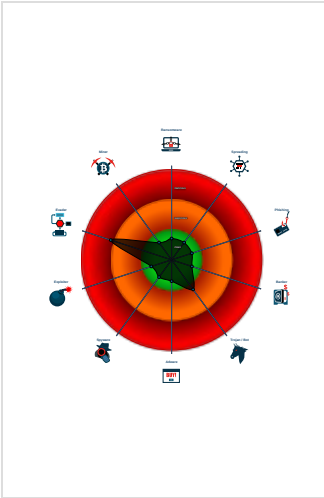
### Detection

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...
Tries to connect to HTTP servers, b...
Executes the "rm" command used to ...

### 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
- 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

## General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553488
Start date:	15.01.2022
Start time:	01:18:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gsf3z44v5s
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:	mal52.evad.lin@0/0@0/0

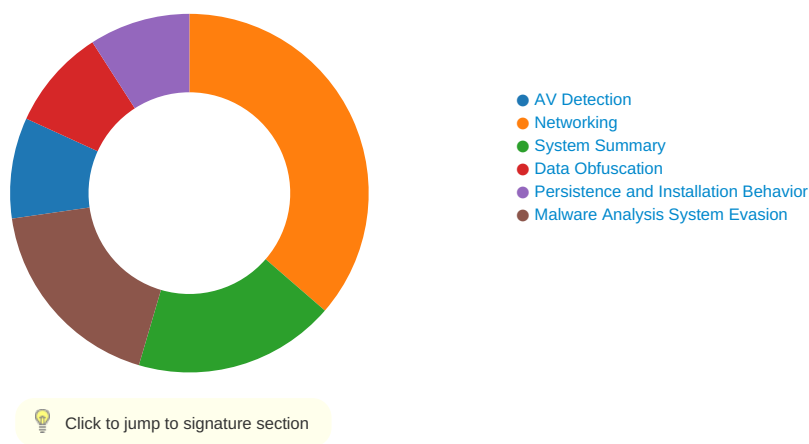
## Process Tree

- system is Inxubuntu20
  - gsf3z44v5s (PID: 5212, Parent: 5110, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/gsf3z44v5s
  - dash New Fork (PID: 5253, Parent: 4331)
  - rm (PID: 5253, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.gnhgFAVsJy /tmp/tmp.t3qRXe8EQV /tmp/tmp.wpv1yxnV4b
  - cleanup

## Yara Overview

No yara matches

## Jbx Signature Overview



### AV Detection:



Multi AV Scanner detection for submitted file

### Data Obfuscation:



Sample is packed with UPX

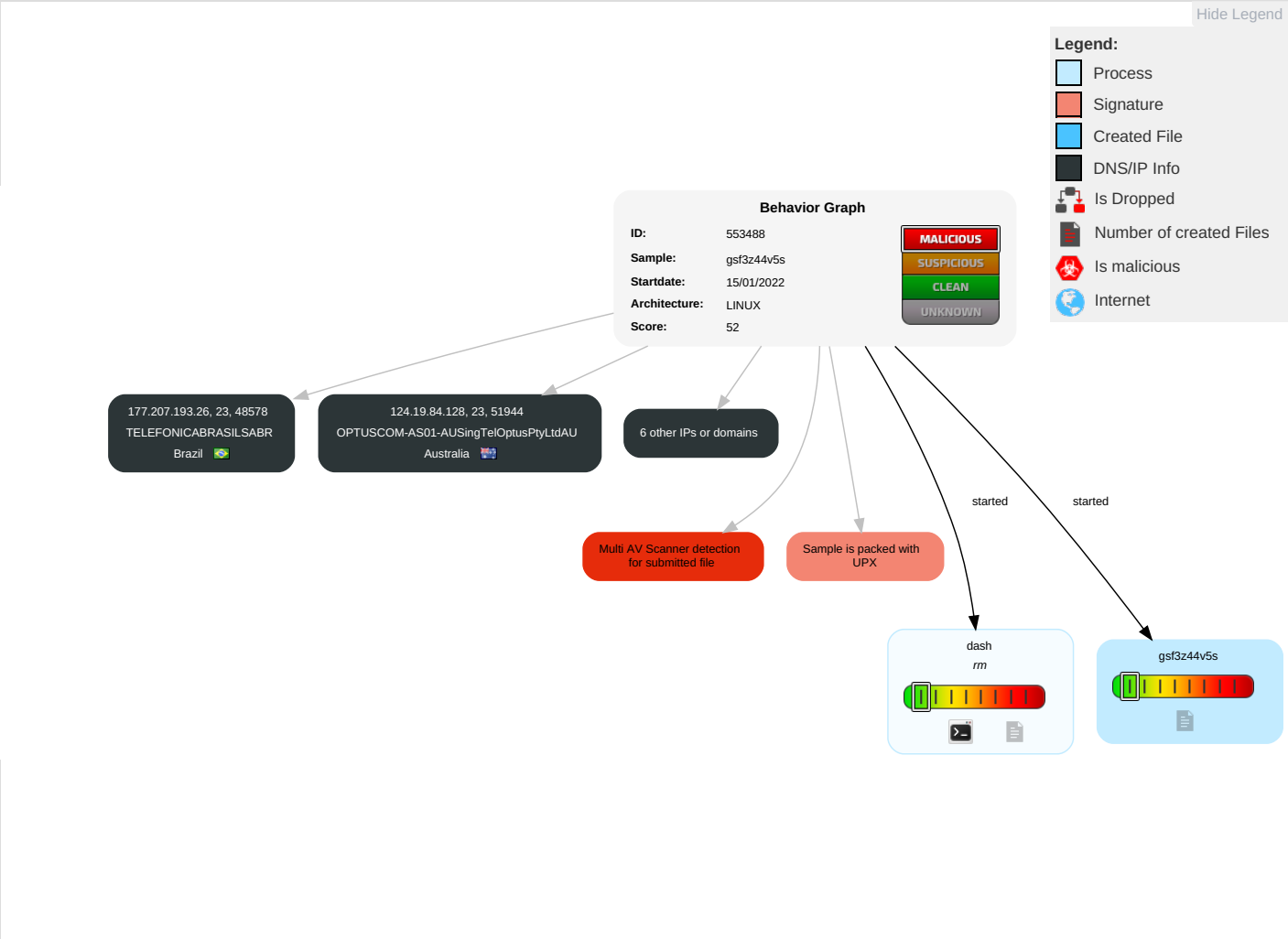
## Mitre Att&ck Matrix

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 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	File Deletion 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

## Malware Configuration









No configs have been found

## Behavior Graph



Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
183.5.95.66	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
34.249.145.219	unknown	United States		16509	AMAZON-02US	false
177.207.193.26	unknown	Brazil		18881	TELEFONICABRASILSABR	false
124.19.84.128	unknown	Australia		7474	OPTUSCOM-AS01-AUSingTelOptusPtyLtdAU	false
121.15.190.47	unknown	China		58466	CT-GUANGZHOU-IDCCHINANETGuangdongprovincenetworkCN	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/gsf3z44v5s
Exit Code:	127
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

Static File Info

General	
File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	7.915655038267032
TrID:	<ul style="list-style-type: none"><li>ELF Executable and Linkable format (generic) (4004/1) 100.00%</li></ul>
File name:	gsf3z44v5s
File size:	22124
MD5:	5502094e79b489ff942ebe314f34a34a
SHA1:	3faad8451da16e6ee0f003b9d0070710f42a1b90
SHA256:	6f5dde695a158e5028c3105754df18a00182db560288f37279da6143de73b84
SHA512:	bf80e4710e25abacde5eb845057ac89c900afa901dab74c5ac4523c3985b798db7d4b0c63b85d47b6608c6bb0eb07bf2ffe07e9ade057770a7c312ecf31dd166
SSDEEP:	384:pUOI4RRYAPzXj1WBxhsqAWPlizpZ5DFILLFIM1f4ybVeR80cU7SmkohymdGUop5v:pUOIMRY+zxYba9OJDFILoMZEC0qros3l
File Content Preview:	.ELF...a.....(....H..4.....4. ...(.T...T....?.....Q.td.....CvUPXl.....\.....q.....?.E.h;.}...^.....+P.f.k.@.....}6N.h.....X...].?.E(...p...i..]

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:	0xc348
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

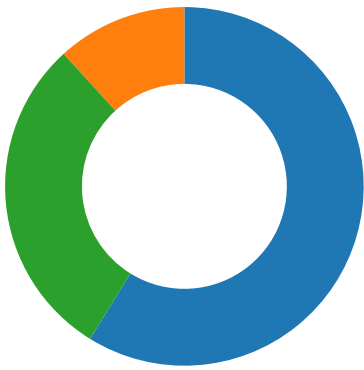
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x54f7	0x54f7	4.0623	0x5	R E	0x8000		
LOAD	0x3fb4	0x1bfb4	0x1bfb4	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution

● 23 (Telnet)  
● 80 (HTTP)  
● 443 (HTTPS)



## TCP Packets

## System Behavior

Analysis Process: gsf3z44v5s PID: 5212 Parent PID: 5110

### General

Start time:	01:19:03
Start date:	15/01/2022
Path:	/tmp/gsf3z44v5s
Arguments:	/tmp/gsf3z44v5s
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

### File Activities

#### File Read

Analysis Process: dash PID: 5253 Parent PID: 4331

### General

Start time:	01:20:27
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5253 Parent PID: 4331

### General

Start time:	01:20:27
Start date:	15/01/2022
Path:	/usr/bin/rm



Arguments:	rm -f /tmp/tmp.gnhgFAvsJy /tmp/tmp.t3qRXe8EQV /tmp/tmp.wpv1yxvV4b
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read