ID: 635053
Sample Name: KzUyRGzaDZ
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 11:51:08
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

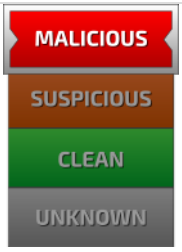
KzUyRGzaDZ

Overview

General Information

Sample Name:	KzUyRGzaDZ
Analysis ID:	635053
MD5:	9d8c6e23c4a6d5..
SHA1:	2995d242ea96d0.
SHA256:	13cdc7b6231e4d..
Tags:	64 elf gafgyt
Infos:	

Detection



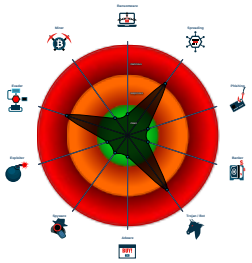
Mirai

Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Opens /proc/net/* files useful for fin…
- Sample is packed with UPX
- Sample contains only a LOAD segm…
- Tries to connect to HTTP servers, b…
- Yara signature match

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635053
Start date and time: 27/05/202211:51:08	2022-05-27 11:51:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KzUyRGzaDZ
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.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/KzUyRGzaDZ
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	echo zP
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- KzUyRGzaDZ (PID: 6230, Parent: 6131, MD5: 9d8c6e23c4a6d55edf8849401f32ca4c) Arguments: /tmp/KzUyRGzaDZ
  - KzUyRGzaDZ New Fork (PID: 6231, Parent: 6230)
  - KzUyRGzaDZ New Fork (PID: 6232, Parent: 6230)
    - KzUyRGzaDZ New Fork (PID: 6233, Parent: 6232)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
KzUyRGzaDZ	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x9e30:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x9e9f:$s2: $Id: UPX • 0x9e50:$s3: $Info: This file is packed with the UPX executable packer

Memory Dumps

Source	Rule	Description	Author	Strings
6230.1.00000000a0bbd638.00000000abc4abe9.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6232.1.00000000a0bbd638.00000000abc4abe9.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6231.1.00000000a0bbd638.00000000abc4abe9.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6233.1.00000000a0bbd638.00000000abc4abe9.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Spreading

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

Data Obfuscation

Sample is packed with UPX

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

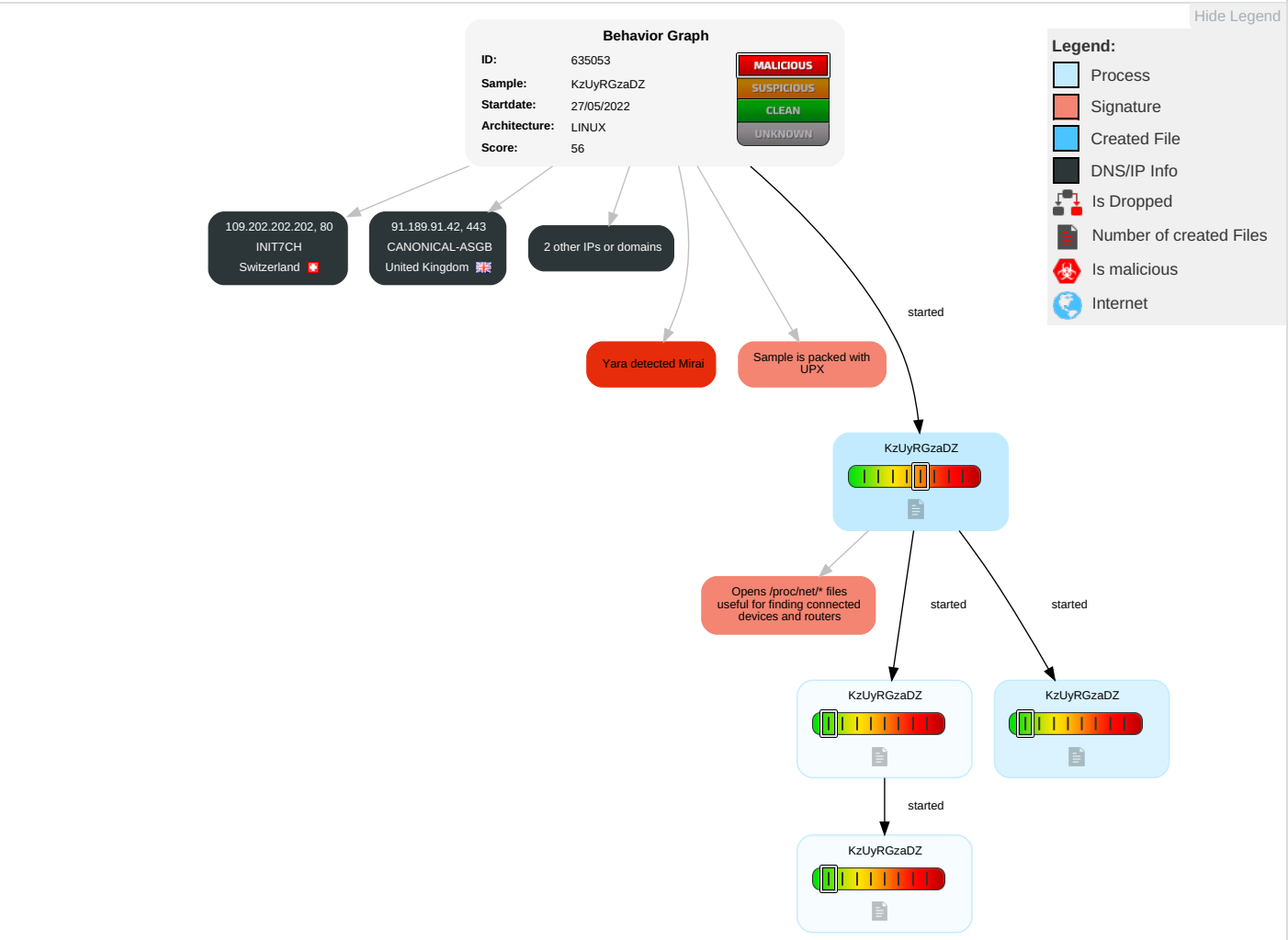
Mitre Att&ck Matrix

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	1 Obfuscated Files or Information	OS Credential Dumping	1 Remote System Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

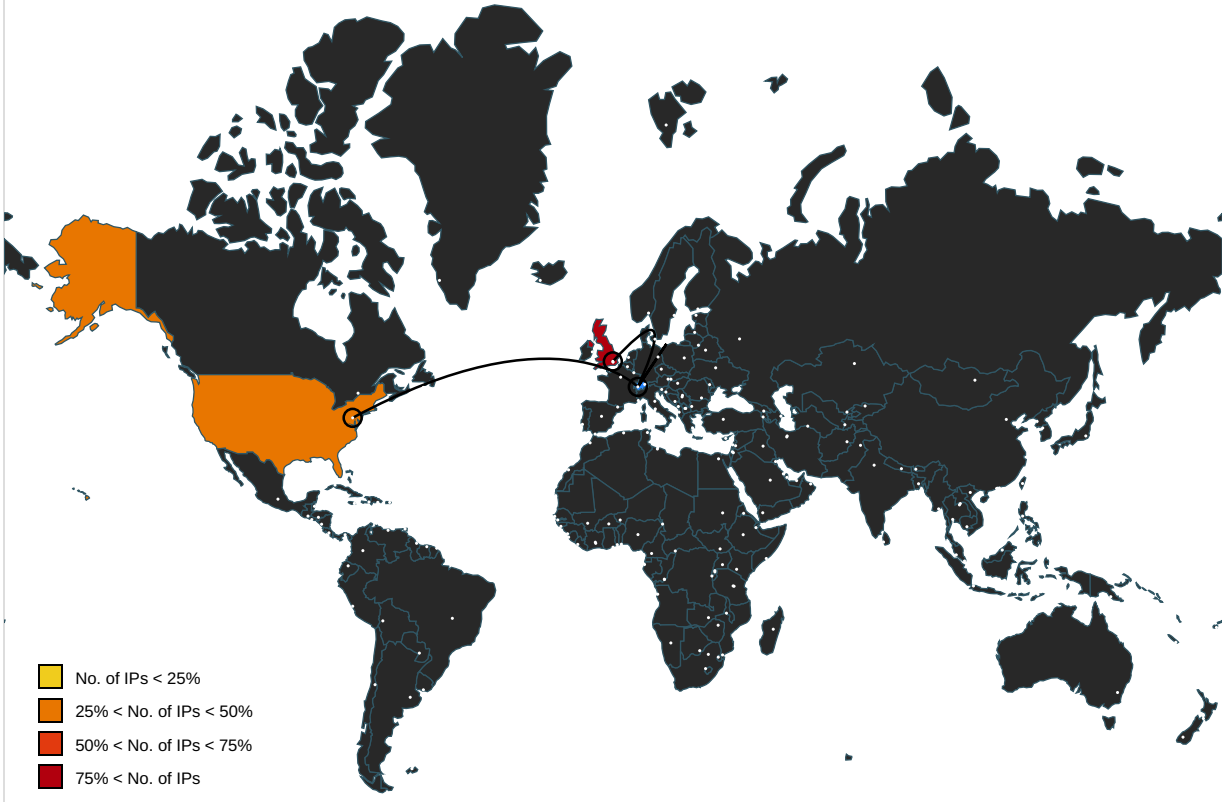
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.245.210.119	unknown	United States		36352	AS-COLOCROSSINGUS	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

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

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):	7.974934192282023
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	KzUyRGzaDZ
File size:	49804
MD5:	9d8c6e23c4a6d55edf8849401f32ca4c
SHA1:	2995d242ea96d0e0ee2980369e8d687e92e78e0a
SHA256:	13cdc7b6231e4ddb3f3e062def4919fde078d9751b007a1f4e105ed4d0961fe6
SHA512:	7101fac0d177effb6c590aa5a508402f812c70bd83d288cd2cb421e8bb28868bb669c5d4abdb0d5ffa0d8f1bfdb9a8376ffd90876d8cccbae7d538ec31300c6f
SSDEEP:	768:8Vlo1OeMMg27EbV3UkkgaI3+V/ATmxUiq7LPE/QfVjx00DCb0ARb:MlZMg27Skz219iqJBfUNRb
TLSH:	5D2302DFDD5274F6D0B0C17302992381B91BF1281B856B738661BADFCDB55420E4D7A2
File Content Preview:	.ELF.....>.....@.....@.8...@.....R.....R.....Q.td.....G.lUPX!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:	0x109398

ELF header

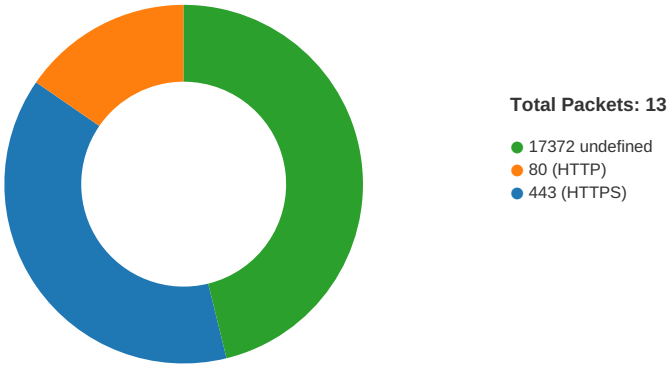
Flags:	0x0
ELF Header Size:	64
Program Header Offset:	64
Program Header Size:	56
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	64
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0xa4d4	0xa4d4	4.0598	0x5	R E	0x100000		
LOAD	0x810	0x520810	0x520810	0x0	0x0	0.0000	0x6	RW	0x1000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x8		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: KzUyRGzaDZ PID: 6230, Parent PID: 6131

General

Start time:	11:51:57
Start date:	27/05/2022
Path:	/tmp/KzUyRGzaDZ
Arguments:	/tmp/KzUyRGzaDZ
File size:	49804 bytes
MD5 hash:	9d8c6e23c4a6d55edf8849401f32ca4c

File Activities

File Deleted

File Read

Analysis Process: KzUyRGzaDZ PID: **6231**, Parent PID: **6230**

General

Start time:	11:51:57
Start date:	27/05/2022
Path:	/tmp/KzUyRGzaDZ
Arguments:	n/a
File size:	49804 bytes
MD5 hash:	9d8c6e23c4a6d55edf8849401f32ca4c

Analysis Process: KzUyRGzaDZ PID: **6232**, Parent PID: **6230**

General

Start time:	11:51:57
Start date:	27/05/2022
Path:	/tmp/KzUyRGzaDZ
Arguments:	n/a
File size:	49804 bytes
MD5 hash:	9d8c6e23c4a6d55edf8849401f32ca4c

Analysis Process: KzUyRGzaDZ PID: **6233**, Parent PID: **6232**

General

Start time:	11:51:57
Start date:	27/05/2022
Path:	/tmp/KzUyRGzaDZ
Arguments:	n/a
File size:	49804 bytes
MD5 hash:	9d8c6e23c4a6d55edf8849401f32ca4c