ID: 829689
Sample Name:
SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:31:06
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

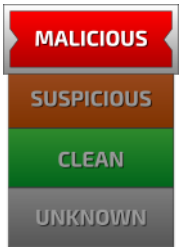
SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf

Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf
Analysis ID:	829689
MD5:	0d7a0d32ecf04..
SHA1:	d060eae88a98...
SHA256:	9da726d31cfec..
Tags:	elf
Infos:	

Detection

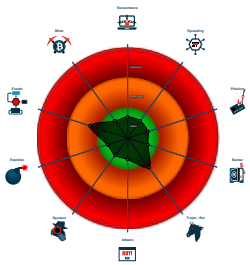


Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Sample contains only a LOAD segm…
- Yara signature match
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- ELF contains segments with high en…

Classification



Analysis Advice

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

Exit code information suggests that the sample terminated abnormally, try to lookup the sample's target architecture.

All HTTP servers contacted by the sample do not answer. The sample is likely 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 only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829689
Start date and time:	2023-03-18 21:31:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample file name:	SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf
Detection:	MAL
Classification:	mal56.linELF@0/0@0/0

Runtime Messages

Command:	/tmp/SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf
PID:	6223
Exit Code:	139
Exit Code Info:	SIGSEGV (11) Segmentation fault invalid memory reference
Killed:	False

Standard Output:	
Standard Error:	qemu: uncaught target signal 11 (Segmentation fault) - core dumped

Process Tree

- **system is lnxubuntu20**
  - SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf (PID: 6223, Parent: 6122, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf	Linux_Packer_Patched_UPX_62e11c64	unknown	unknown	• 0x78:$a: 55 50 58 21 0A 58 0D 89 00 00 00 00 00 00 00 00 00 00 00 00

Memory Dumps

Source	Rule	Description	Author	Strings
6223.1.00007f2e70400000.00007f2e70421000.r-x.sdmp	Linux_Packer_Patched_UPX_62e11c64	unknown	unknown	• 0x78:$a: 55 50 58 21 0A 58 0D 89 00 00 00 00 00 00 00 00 00 00 00 00

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

System Summary

Malicious sample detected (through community Yara rule)

Mitre Att&ck Matrix

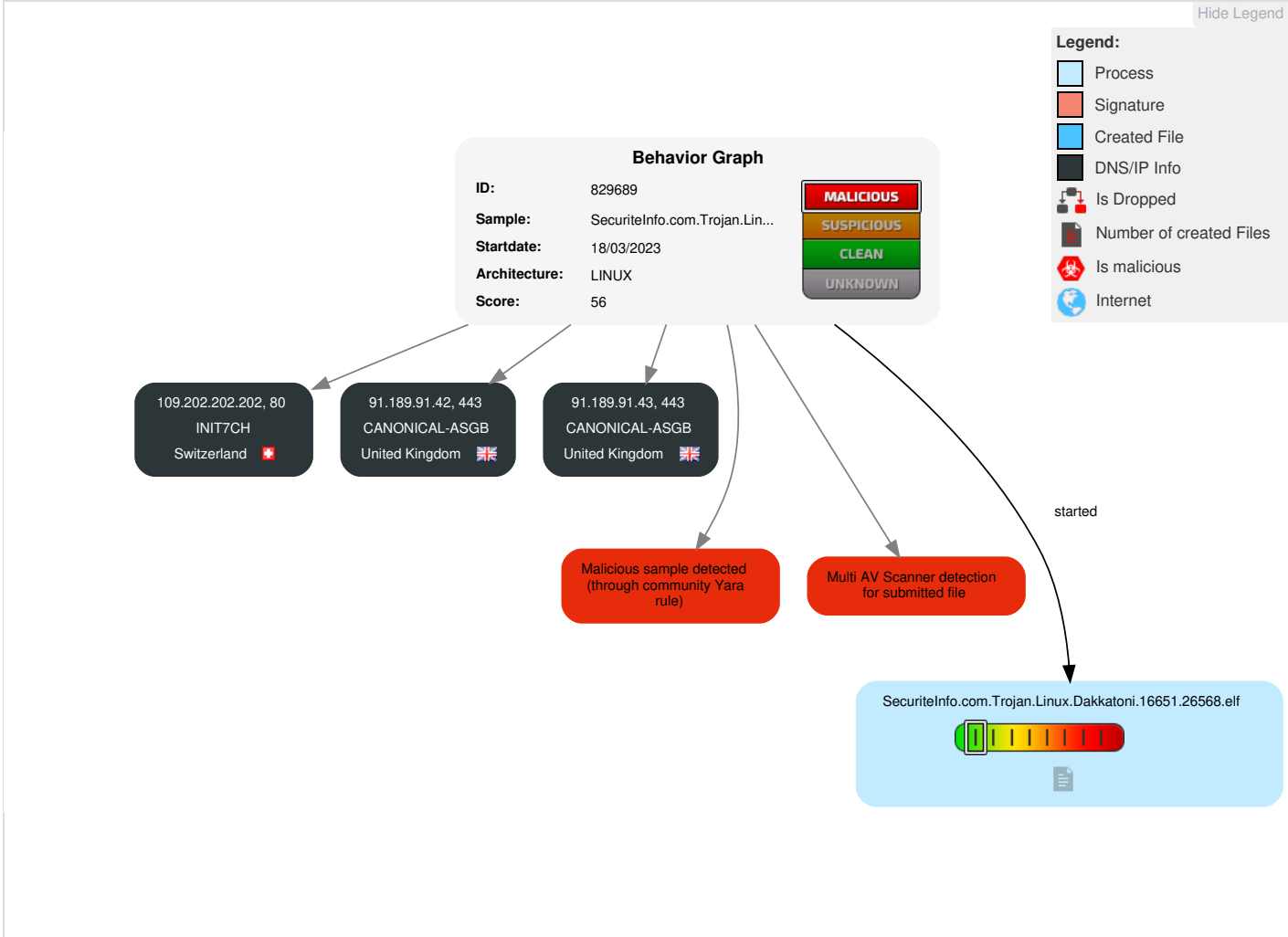
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Obfuscated Files or Information	OS Credential Dumping	1 1 Security Software 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf	5%	ReversingLabs		
SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf	12%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

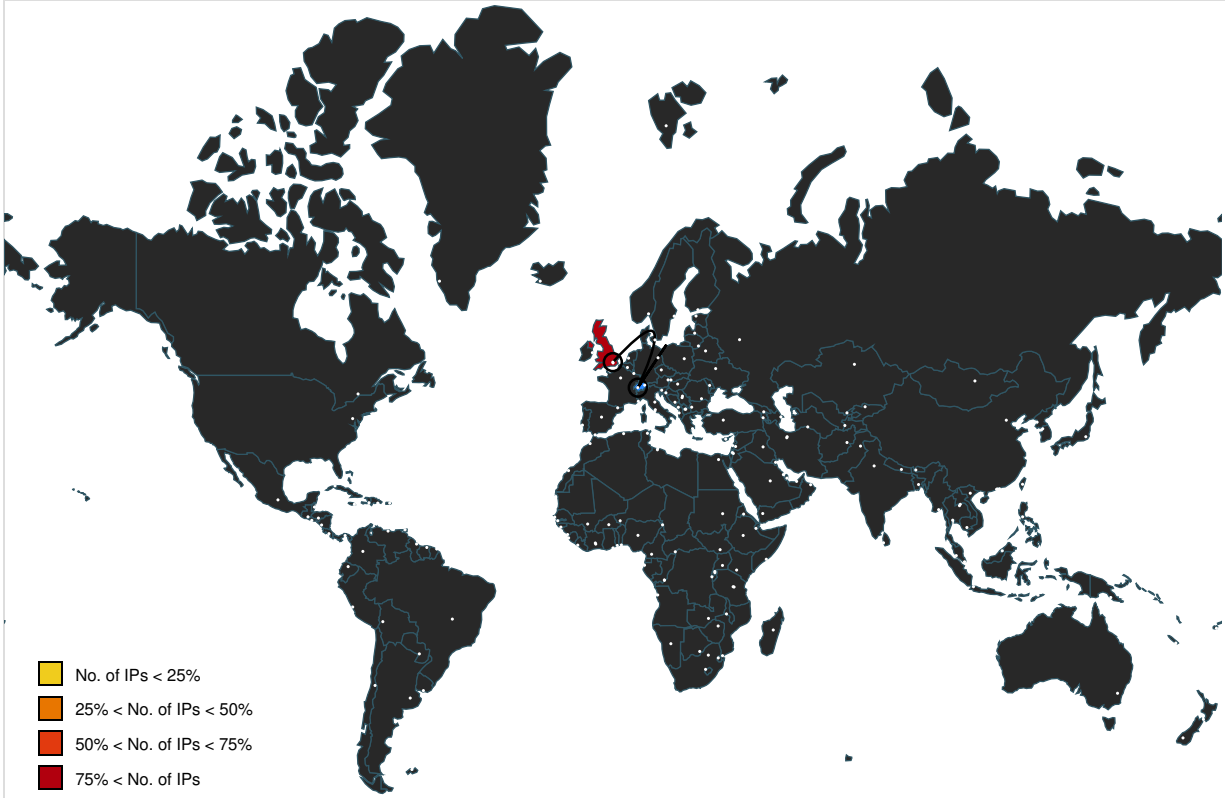
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, no section header
Entropy (8bit):	7.723190077963099
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf
File size:	10136
MD5:	0d7a0d32ecf0446189e05b0d96de705b
SHA1:	d060eae88a98939b04e0d39be16c072e66916018
SHA256:	9da726d31cfeceac5e5e360f14a4d1b823b97c620ebc62dbfcfa0750930e0d76
SHA512:	18837fab1e71522781decb6b90f55fa3046afb6df7c44abcbea99e1e0fa3dea1718baf4da6910f1f3de1ef5c2ea9b1561a441b057c166f8c7d375075c1f366d5
SSDEEP:	192:0JUo2TjiSlZwhEeoCg+8J/3s0IreBf1fp66NllOiaLpxmoJPvbvvABsAO:0Fin4W7Cg+A7DfnflQuAcBsAO
TLSH:	9222D09EEDE39F74DA715AB28B4B0E707CFF9B14ED1C5579D88434488B6A805501A38C
File Content Preview:	.ELF.....A.h...4.....4. ...(.....@...@.....C...C.....*.*UPX!.X.....\....|.$..ELF.....@.`....4..^h... ...(..... <...@.....ll.....H.W.`.t.d....dt.Q.....].M.....6...

Static ELF Info

ELF header

Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	

ELF header

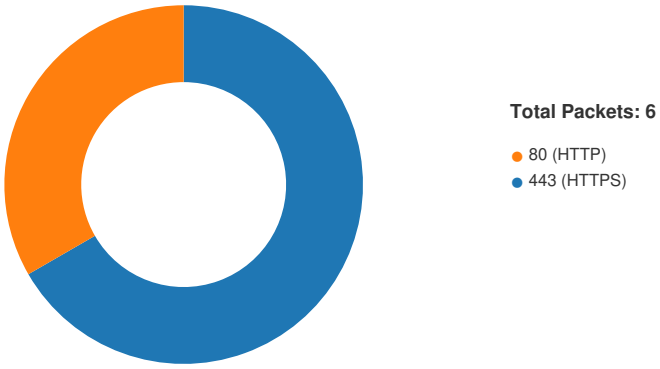
Header String Table Index:	

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	0x205b2	0x205b2	7.7232	0x5	R E	0x10000		
LOAD	0x0	0x430000	0x430000	0x0	0x8ac18	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf PID: 6223, Parent PID: 6122

General

Start time:	21:31:49
Start date:	18/03/2023
Path:	/tmp/SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf
Arguments:	/tmp/SecuriteInfo.com.Trojan.Linux.Dakkatoni.16651.26568.elf
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read