ID: 651260
Sample Name: loligang.x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 17:59:27
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

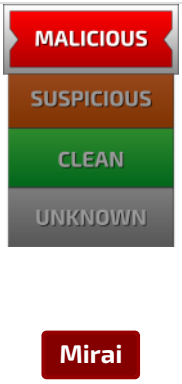
loligang.x86

Overview

General Information

Sample Name:	loligang.x86
Analysis ID:	651260
MD5:	626c4dc99eea6d..
SHA1:	51079f90726093..
SHA256:	68cb74c5325f29…
Infos:	

Detection



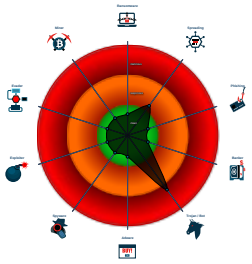
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Yara detected Mirai
- Machine Learning detection for sam…
- Enumerates processes within the "p…
- Yara signature match
- Sample tries to kill a process (SIGK…
- Sample has stripped symbol table

Classification



General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651260
Start date and time: 23/06/202217:59:27	2022-06-23 17:59:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	loligang.x86
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:	mal68.troj.linX86@0/0@0/0

Runtime Messages

Command:	/tmp/loligang.x86
PID:	6222
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	lzrd cock fest"/proc/"/exe
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- loligang.x86 (PID: 6222, Parent: 6123, MD5: 626c4dc99eea6d5e4df179086edc8a98) Arguments: /tmp/loligang.x86
  - loligang.x86 New Fork (PID: 6223, Parent: 6222)

- loligang.x86 New Fork (PID: 6224, Parent: 6222)
- loligang.x86 New Fork (PID: 6225, Parent: 6222)
  - loligang.x86 New Fork (PID: 6226, Parent: 6225)
  - loligang.x86 New Fork (PID: 6227, Parent: 6225)
  - loligang.x86 New Fork (PID: 6228, Parent: 6225)
  - loligang.x86 New Fork (PID: 6243, Parent: 6225)
    - loligang.x86 New Fork (PID: 6244, Parent: 6243)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
loligang.x86	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0xefc4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf034:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf0a4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf114:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf184:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf3f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf448:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf49c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf4f0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xf544:$xo1: oMXKNNC\x0D\x17\x0C\x12
loligang.x86	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	0xe9e0:$x1: POST /cdn-cgi/ 0xee2b:$s1: LCOGQGPTGP
loligang.x86	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6226.1.00000000622d5c71.00000000a6a40188.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x598:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x610:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x688:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x700:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x778:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xa08:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xa60:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xab8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb10:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb68:$xo1: oMXKNNC\x0D\x17\x0C\x12
6227.1.00000000622d5c71.00000000a6a40188.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x598:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x610:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x688:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x700:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x778:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xa08:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xa60:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xab8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb10:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb68:$xo1: oMXKNNC\x0D\x17\x0C\x12
6244.1.00000000622d5c71.00000000a6a40188.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	0x598:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x610:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x688:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x700:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x778:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xa08:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xa60:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xab8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb10:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xb68:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
6222.1.00000000622d5c71.00000000a6a40188.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x598:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x610:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x688:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x700:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x778:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa08:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa60:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xab8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb10:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb68:$xo1: oMXKNNC\x0D\x17\x0C\x12
6243.1.00000000622d5c71.00000000a6a40188.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x598:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x610:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x688:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x700:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x778:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa08:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa60:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xab8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb10:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb68:$xo1: oMXKNNC\x0D\x17\x0C\x12
Click to see the 19 entries				

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

Mitre Att&ck Matrix

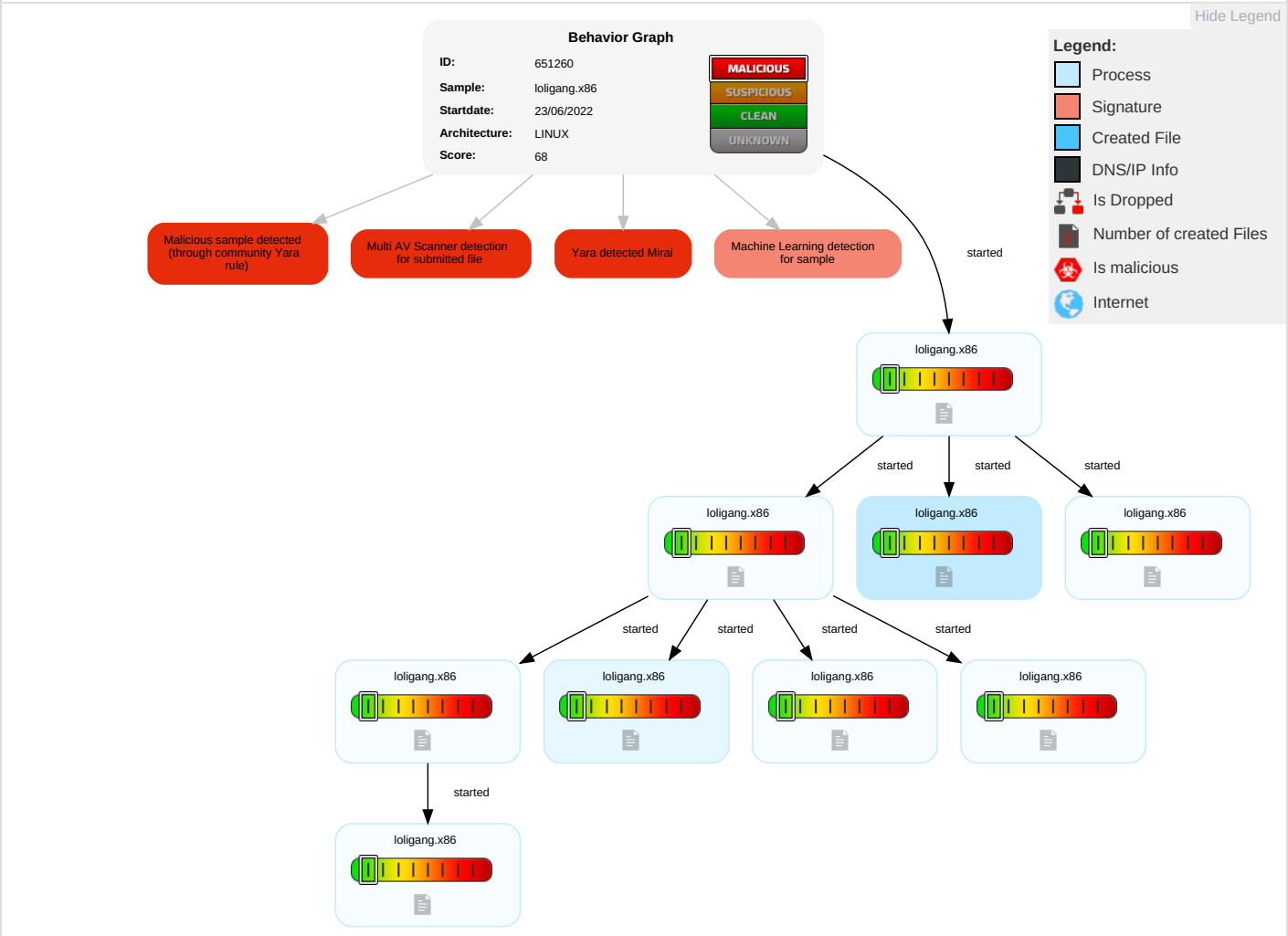
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

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	1 OS Credential Dumping	System Service Discovery	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
loligang.x86	61%	Virustotal		Browse
loligang.x86	100%	Joe Sandbox ML		

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

No contacted IP infos

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 LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.408338044451668

TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	loligang.x86
File size:	66136
MD5:	626c4dc99eea6d5e4df179086edc8a98
SHA1:	51079f907260930c3b991286ad11abb61d76b91d
SHA256:	68cb74c5325f29a74eae212973ea710b3a885a3866853e21b3bdaf9e262b0c23
SHA512:	bc203a473c19b41ea9f0a2e0487abd1fa853fd89b7bb7ec612014fd1f0e0787786416e31699244e5d22b3edd659bade57022b9433029689605bb6a740b46b676
SSDEEP:	1536:IoRC9170vwHbQXZ5+qXDEuXi90dSW7V/DjObeFt6PuQ4ZH:PC917iwHbQXZ5+qXA594SWZ/XObeb6G7
TLSH:	AB5329C8A593F8F5DC140978307ABB66AEB3F13B7135E99BC3D82927A841702D10669D
File Content Preview:	.ELF.....d...4.....4. ...(..... ... .Q.td.....U..S.....w....h.....[]...$.....U.....=.....t..5....$.....$.....u.....t....h {.....

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 - System V
ABI Version:	0
Entry Point Address:	0x8048164
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	65736
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0xe906	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x80569b6	0xe9b6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x80569e0	0xe9e0	0x1140	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8058000	0x10000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8058008	0x10008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8058020	0x10020	0x68	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80580a0	0x10088	0x860	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x10088	0x3e	0x0	0x0		0	0	1

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	0xfb20	0xfb20	6.5000	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x10000	0x8058000	0x8058000	0x88	0x900	1.7570	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

No network behavior found

System Behavior

Analysis Process: loligang.x86 PID: 6222, Parent PID: 6123

General

Start time:	18:00:14
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	/tmp/loligang.x86
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98

Analysis Process: loligang.x86 PID: 6223, Parent PID: 6222

General

Start time:	18:00:14
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	n/a
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98

File Activities

File Read

Directory Enumerated

Analysis Process: loligang.x86 PID: 6224, Parent PID: 6222

General

Start time:	18:00:14
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	n/a
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98

Analysis Process: loligang.x86 PID: 6225, Parent PID: 6222

General

Start time:	18:00:14
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	n/a
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98

Analysis Process: loligang.x86 PID: 6226, Parent PID: 6225

General

Start time:	18:00:14
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	n/a
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98

File Activities

File Read

Directory Enumerated

Analysis Process: loligang.x86 PID: **6227**, Parent PID: **6225**

General

Start time:	18:00:14
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	n/a
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98

Analysis Process: loligang.x86 PID: **6228**, Parent PID: **6225**

General

Start time:	18:00:14
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	n/a
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98

Analysis Process: loligang.x86 PID: **6243**, Parent PID: **6225**

General

Start time:	18:00:42
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	n/a
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98

Analysis Process: loligang.x86 PID: **6244**, Parent PID: **6243**

General

Start time:	18:00:42
Start date:	23/06/2022
Path:	/tmp/loligang.x86
Arguments:	n/a
File size:	66136 bytes
MD5 hash:	626c4dc99eea6d5e4df179086edc8a98