ID: 679631
Sample Name: RaNg2d7Qzo
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:31:01
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

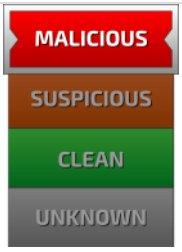
RaNg2d7Qzo

Overview

General Information

Sample Name:	RaNg2d7Qzo
Analysis ID:	679631
MD5:	8c33b327bc030e..
SHA1:	af6b7dabe6acf05..
SHA256:	1f732b672c0f0f1..
Tags:	32 elf mips mirai
Infos:	

Detection



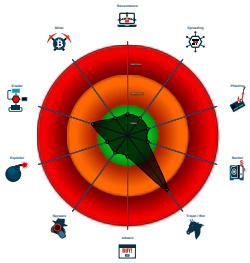
Mirai

Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Yara signature match
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Sample listens on a socket
- Sample contains strings indicative o…

Classification



Analysis Advice

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:	35.0.0 Citrine
Analysis ID:	679631
Start date and time: 06/08/202207:31:01	2022-08-06 07:31:01 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RaNg2d7Qzo
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:	mal64.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/RaNg2d7Qzo
PID:	6232
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- RaNg2d7Qzo (PID: 6232, Parent: 6122, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/RaNg2d7Qzo
  - RaNg2d7Qzo New Fork (PID: 6234, Parent: 6232)
  - RaNg2d7Qzo New Fork (PID: 6235, Parent: 6232)
  - RaNg2d7Qzo New Fork (PID: 6236, Parent: 6232)
    - RaNg2d7Qzo New Fork (PID: 6240, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6241, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6243, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6246, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6248, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6250, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6252, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6254, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6255, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6256, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6257, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6258, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6264, Parent: 6236)
    - RaNg2d7Qzo New Fork (PID: 6267, Parent: 6236)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
RaNg2d7Qzo	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	0x22e34:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22ea4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22f14:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22f84:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22ff4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x23264:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x232b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x2330c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x23360:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x233b4:$xo1: oMXKNNC\x0D\x17\x0C\x12
RaNg2d7Qzo	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6232.1.00007fd13c465000.00007fd13c467000.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	0x1584:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x15f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x166c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x16e0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1754:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x19d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a2c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a84:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1adc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1b34:$xo1: oMXKNNC\x0D\x17\x0C\x12
6232.1.00007fd13c400000.00007fd13c424000.r-x.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	0x22e34:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22ea4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22f14:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22f84:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22ff4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x23264:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x232b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x2330c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x23360:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x233b4:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
6232.1.00007fd13c400000.00007fd13c424000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6235.1.00007fd13c400000.00007fd13c424000.r-x.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	• 0x22e34:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22ea4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22f14:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22f84:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22ff4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x23264:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x232b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x2330c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x23360:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x233b4:$xo1: oMXKNNC\x0D\x17\x0C\x12
6235.1.00007fd13c400000.00007fd13c424000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 1 entries				

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

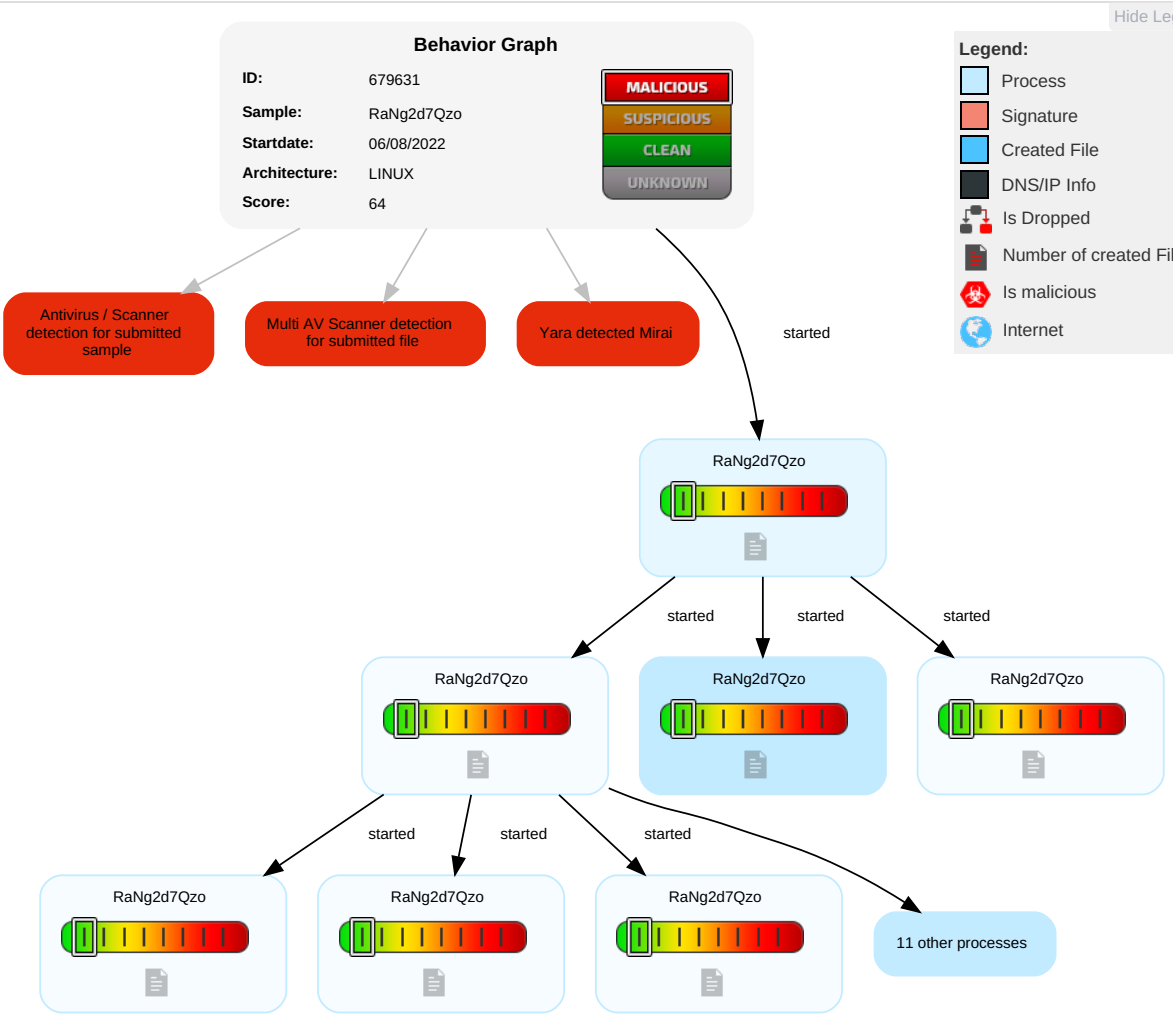
Mitre Att&ck Matrix

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	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software 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
RaNg2d7Qzo	60%	Virustotal		Browse
RaNg2d7Qzo	34%	Metadefender		Browse
RaNg2d7Qzo	69%	ReversingLabs	Linux.Trojan.Mirai	
RaNg2d7Qzo	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://46.23.109.47/Cloud/Gpon.sh	19%	Virustotal		Browse
http://46.23.109.47/Cloud/Gpon.sh	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.x86	18%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://46.23.109.47/Cloud/Cloud.x86	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Comtrend.sh%20-O%20-%3E%20/tmp/jno;sh%20/tmp/jno%27/&sessionKey=1039230114	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Netlink.sh%20-O%20-%3E%20/tmp/jno;sh%20/tmp/jno%27/&waninf=1_INTERNET_R_VI	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.mpsl;chmod	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.mips;	100%	Avira URL Cloud	malware	
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://0.0.0.0/Cloud/Cloud.x86	0%	Avira URL Cloud	safe	
http://46.23.109.47/Cloud/Dlink.sh%20-O%20-%3E%20/tmp/kh;sh%20/tmp/kh%27$	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.701630357525989
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	RaNg2d7Qzo
File size:	150284
MD5:	8c33b327bc030efedb88abee85efef14
SHA1:	af6b7dabe6acf0577663902ef127acadf7fa6168
SHA256:	1f732b672c0f0f1893f9515fa07dc655618beaeb8dd47f0ebeb00895f862ba4f
SHA512:	3c78a28b868a00dda9d7d2500af6ccc63d78201940c7abe7ee72954839f45324da3fa24e5e15cd68cec1136c3e52928657dc2f9fb4567efde2ef0ee8ab2afad6
SSDEEP:	1536:OMfjBhjBYB1yqYmQbB6+U8XKAgi1ALIAlw93AZPgMXNybTDK2QpOZqaBhIzWES2:OMf7Ms/lB6+uAgTYcXtpOm
TLSH:	73E3D54BAB710FFBE89FDD3700E91706159C591622B96FB1B670D818F28B24F29D3864
File Content Preview:	.ELF.....`.@.4....H.....4. ...(.....@...@.@>..@>.....@...@F..@F.x...8.....Q.td.....<L..'!.....'.....<(..'!... .....9'.. .....<...'!.....p.9

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	149724
Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x20ec0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x420fe0	0x20fe0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x421040	0x21040	0x2e00	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x464000	0x24000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x464008	0x24008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x464014	0x24014	0x10	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x464030	0x24030	0x2c0	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4642f0	0x242f0	0x588	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x464878	0x24878	0x24	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x4648a0	0x24878	0xa98	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x84c	0x24878	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x24878	0x64	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	0x400000	0x400000	0x23e40	0x23e40	5.7270	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x24000	0x464000	0x464000	0x878	0x1338	3.8923	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

No network behavior found

System Behavior

Analysis Process: RaNg2d7Qzo PID: 6232, Parent PID: 6122

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	/tmp/RaNg2d7Qzo
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: RaNg2d7Qzo PID: 6234, Parent PID: 6232

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: RaNg2d7Qzo PID: 6235, Parent PID: 6232

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: 6236, Parent PID: 6232

General

Start time:	07:31:48
Start date:	06/08/2022

Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6240**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6241**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6243**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6246**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6248**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6250**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022

Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6252**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6254**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6255**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6256**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6257**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6258**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022

Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6264**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: RaNg2d7Qzo PID: **6267**, Parent PID: **6236**

General

Start time:	07:31:48
Start date:	06/08/2022
Path:	/tmp/RaNg2d7Qzo
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9